Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

Contenido

Descripción general de Kaspersky Endpoint Security
Novedades de esta versión
Comparación de las funciones de Kaspersky Endpoint Security según la herramienta de administración Kaspersky Security Center
Instalar y desinstalar la aplicación
- Kit de distribución
- Requisitos de hardware y software
- Prepararse para la instalación
- Instalar Kaspersky Endpoint Security
- Preparación de la aplicación para su uso
- Desinstalar Kaspersky Endpoint Security

Iniciar la aplicación por primera vez
Interfaz de la aplicación Kaspersky Endpoint Security
- Ventana principal de la aplicación
- Icono de Kaspersky Endpoint Security
- Ventana de ajustes de la aplicación

Acerca de las notificaciones
Licencias de la aplicación Kaspersky Endpoint Security
- Acerca del Contrato de licencia de usuario final
- Acerca de la licencia
- Acerca de la suscripción
- Acerca del certificado de licencia
- Acerca de la clave
- Acerca del código de activación
- Acerca del archivo de claves
- Acerca de la provisión de datos
- Activar Kaspersky Endpoint Security
- Ver la información de la licencia
- Gestionar licencias y suscripciones
- Comparación de la funcionalidad de la aplicación según el tipo de licencia para estaciones de trabajo

Ejecutar tareas habituales
- Abrir la aplicación y salir de ella
- Ver el estado de protección del equipo
- Ver el estado operativo de los componentes instalados
- Desactivar y reanudar la protección del equipo
- Utilización del Centro de protección
- Ejecutar tareas de análisis
- Configurar el inicio automático de una tarea de análisis programada
- Actualizar las bases de datos de la aplicación
- Procedimiento si el acceso a un archivo está bloqueado
- Restauración de un archivo que la aplicación ha eliminado o desinfectado
- Visualización del informe acerca del funcionamiento de una aplicación
- Pasos que deben seguirse si aparecen ventanas de notificaciones

Configuración avanzada de la aplicación
- Cobertura de la protección del equipo
- Protección frente a amenazas en archivos
- Protección frente a amenazas web
- Protección frente a amenazas en el correo
- Protección frente a amenazas en la red
- Firewall
- Detección de comportamiento
- Análisis
- Tareas de actualización
- Tareas locales
  - Tarea de análisis de discos externos
- Depósito de copias de seguridad
- Informes
- Managed Detection and Response

- Endpoint Detection and Response (KATA)
- Endpoint Detection and Response Optimum
  - Integración con Endpoint Detection and Response Optimum
  - Análisis en busca de indicadores de peligro
  - Mover archivo a Cuarentena
  - Obtener archivo
  - Eliminar el archivo
  - Iniciar proceso
  - Terminar proceso
  - Prevención de ejecución
  - Aislamiento de la red informática
  - Sandbox en la nube
- Cifrado de disco de FileVault
- Protección con contraseña
- Prevención de exploits
- Motor de reparación
- Control web
- Control de dispositivos

Participación en Kaspersky Security Network

Comprobar la integridad de los componentes de la aplicación

Administración de la aplicación mediante la Consola de administración de Kaspersky Security Center

- Implementar Kaspersky Endpoint Security en una red corporativa
- Actualizar Kaspersky Endpoint Security versión 11.1 o posterior a la versión 12.2
- Prepárese para la instalación remota de Kaspersky Endpoint Security
  - Instalación del complemento de administración de Kaspersky Endpoint Security
  - Instalación del Agente de red de forma local
  - Instalación del Agente de red con Apple Remote Desktop
  - Instalación del Agente de red con Kaspersky Security Center
  - Instalación del Agente de red mediante el protocolo SSH
  - Desinstalación del Agente de red de forma local
- Gestionar el Agente de red desde la línea de comandos
  - Iniciar/detener el Agente de red en un equipo remoto
  - Comprobar manualmente la conexión entre un equipo cliente y el Servidor de administración. Utilidad Klnagchk
  - Conectar manualmente un equipo remoto al Servidor de administración. Utilidad Klmover
  - Desinstalar el Agente de red
- Instalar y desinstalar Kaspersky Endpoint Security
  - Instalación de la aplicación mediante el protocolo SSH
  - Instalación de la aplicación mediante Kaspersky Security Center
  - Creación de un paquete de instalación
  - Desinstalación de la aplicación con Kaspersky Security Center
- Iniciar y detener la aplicación a través de Kaspersky Security Center
- Crear y administrar tareas
  - Crear tareas
  - Iniciar y detener tareas manualmente
  - Importar y exportar tareas
  - Ver tareas
  - Gestionar la configuración de tareas específicas
- Crear y administrar directivas
  - Crear una directiva
  - Ver la lista de directivas
  - Configurar los ajustes de la directiva
  - Cambiar el estado de una directiva
  - Exportación de una directiva a un archivo KLP
  - Importar una directiva desde un archivo KLP
- Crear y administrar perfiles de directivas
- Generar un informe sobre objetos detectados
- Obtener una clave de recuperación para un disco cifrado

Administración remota de la aplicación a través de Kaspersky Security Center Web Console y Cloud Console

- Instalación del complemento web de Kaspersky Endpoint Security
- Crear directivas
  - Configure el ajuste de Protección frente a amenazas avanzadas
  - Configure el ajuste de Protección frente a amenazas básicas

Configure el ajuste de Protección frente a amenazas en archivos
Configure el ajuste de Protección frente a amenazas web
Configure el ajuste de Protección frente a amenazas en la red
Configure los Controles de seguridad
Configurar el cifrado de datos
Configurar los ajustes de Detection and Response
Configurar Managed Detection and Response
Configurar Endpoint Detection and Response
Configurar Endpoint Detection and Response (KATA)
Configurar los ajustes de actualización
Configurar los ajustes adicionales
Crear tareas
Configurar los ajustes de la tarea de análisis
Configurar los ajustes de la tarea Agregar clave
Configurar la tarea de actualización
Obtener una clave de recuperación para una unidad cifrada
Administrar la aplicación desde la línea de comandos
Ver la ayuda de la línea de comandos
Ejecutar análisis de software malicioso
Actualizar la aplicación
Anular la última actualización
Iniciar/detener un componente o una tarea
Ver el estado y las estadísticas de un componente o una tarea
Exportar configuración de protección
Activar la aplicación
Instalar la extensión de sistema
Configurar las conexiones de red
Eliminar claves de licencia
Devolver códigos de la línea de comandos
Salir de la aplicación
Desinstalar la aplicación
Comandos de administración de Detection and Response
Administrar Prevención de ejecución
Administrar Aislamiento de red
Ponerse en contacto con el Servicio de soporte técnico
Cómo obtener soporte técnico
Servicio de soporte técnico a través de Kaspersky CompanyAccount
Recopilar información para el Servicio de soporte técnico
Utilizar un archivo de rastreo
Crear un archivo de rastreo
Fuentes de información sobre la aplicación
Apéndices
Problemas conocidos y limitaciones
Lista de objetos analizados por extensión
Máscaras en rutas a archivos y carpetas
Requisitos del archivo de IOC
Intérpretes de scripts admitidos para Prevención de ejecución
Cómo añadir el certificado de Kaspersky Endpoint Security al almacenamiento de certificados de Mozilla Firefox
Información sobre código de terceros
Avisos sobre las marcas comerciales

Descripción general de Kaspersky Endpoint Security

La aplicación Kaspersky Endpoint Security protege los ordenadores con macOS contra el malware y otras amenazas de seguridad informática.

Protección frente a amenazas en archivos

El componente Protección frente a amenazas en archivos protege el sistema de archivos del ordenador en tiempo real interceptando y analizando los intentos de acceso a los archivos. Más información.

Protección frente a amenazas web

El componente Protección frente a amenazas web protege la información entrante y saliente del ordenador a través de los protocolos HTTP y HTTPS cuando utilice Safari, Google Chrome™ y Firefox™. Más información.

Protección frente a amenazas en el correo

La protección frente a amenazas en el correo analiza los archivos adjuntos de los mensajes de correo electrónico entrantes y salientes en busca de malware y otras amenazas. El componente proporciona protección al ordenador con la ayuda de bases de datos antimalware, el servicio en la nube de Kaspersky Security Network y el análisis heurístico. Más información.

Protección frente a amenazas en la red

El componente Protección frente a amenazas en la red evita intrusiones en el sistema operativo. Este componente protege contra ciberatacantes (quienes usan análisis de puertos y ataques por fuerza bruta) y el software malicioso que instalan (incluido el malware que trata de enviar datos personales a delincuentes). Más información.

Firewall

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

Detección de comportamiento

El componente Detección de comportamiento recibe información sobre las acciones de las aplicaciones en su ordenador y la proporciona a otros componentes de protección para mejorar su rendimiento. También realiza la acción seleccionada como respuesta a la actividad de malware. Más información.

Prevención de exploits

El componente Prevención de exploits detecta el código del programa que aprovecha las vulnerabilidades en el ordenador para explotar los privilegios de administrador o realizar actividades maliciosas. Más información.

Motor de reparación

El Motor de reparación permite que Kaspersky Endpoint Security revierta las acciones realizadas por malware en el sistema operativo. Más información.

Análisis

La aplicación Kaspersky Endpoint Security detecta y neutraliza malware y otras amenazas de seguridad informática bajo demanda en la cobertura del análisis especificada. Kaspersky Endpoint Security puede ejecutar un análisis completo del ordenador, un análisis rápido de las áreas más importantes y un análisis de la cobertura de análisis especificada. Más información.

Actualización

Kaspersky Endpoint Security actualiza las bases de datos y los módulos de la aplicación desde los servidores de actualización de Kaspersky, desde los puntos de distribución o desde otras fuentes especificadas por su administrador del sistema y crea copias de seguridad de todos los archivos actualizados para permitir una operación de deshacer de la última actualización. Más información.

Depósito de copias de seguridad

Kaspersky Endpoint Security crea una copia de seguridad de los archivos infectados antes de cualquier intento de desinfectarlos o eliminarlos, lo que posibilita que los restaure. Más información.

Informes

Kaspersky Endpoint Security genera informes sobre eventos y acciones relacionados con componentes de aplicaciones. Más información.

Notificaciones

Kaspersky Endpoint Security usa notificaciones para informarle sobre ciertos eventos en el funcionamiento de Kaspersky Endpoint Security. Las notificaciones pueden ir acompañadas por sonidos. Más información.

Centro de protección

Kaspersky Endpoint Security muestra mensajes sobre el estado de protección en el Centro de protección. Centro de protección muestra información sobre el estado de protección del ordenador y sobre cómo eliminar los problemas y las amenazas de seguridad informática. Más información.

Administración remota de la aplicación a través de Kaspersky Security Center

Kaspersky Endpoint Security le permite llevar a cabo una administración remota de la protección de ordenadores: recibir información sobre el estado actual de protección del ordenador, solucionar problemas y responder a amenazas de seguridad informática de forma remota, activar o desactivar componentes de protección (Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en la red, Detección de comportamiento), activar y desactivar el Control web, Managed Detection and Response y Endpoint Detection and Response (KATA), ejecutar tareas de análisis, actualizar las bases de datos de la aplicación, ejecutar cifrado del disco de inicio y administrar licencias y suscripciones de Kaspersky Endpoint Security. Puede usar las siguientes herramientas para administrar Kaspersky Endpoint Security:

- Consola de administración de Kaspersky Security Center. Más información.
- Kaspersky Security Center Web Console y Cloud Console. Más información.

Nota: La funcionalidad compatible con Kaspersky Endpoint Security depende de la herramienta de administración que use.

Cifrado de disco de FileVault

Kaspersky Endpoint Security permite la administración remota del cifrado de FileVault. El cifrado evita que otros usuarios tengan acceso no autorizado a datos confidenciales almacenados en el disco de inicio del ordenador del usuario.

Nota: La función de cifrado de disco de FileVault estará disponible en Kaspersky Security Center 10 SP3 Para obtener más información, póngase en contacto con el Servicio de soporte técnico de Kaspersky.

Control web

Puede administrar remotamente el acceso a sitios web que visitan los usuarios. Puede permitir o bloquear el acceso a direcciones web específicas o grupos de direcciones web. También puede permitir o bloquear el acceso a ciertas categorías de sitios web según el contenido. Más información.

Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a los dispositivos que están instalados o conectados al ordenador. Esto le permite proteger el ordenador de infecciones cuando dichos dispositivos están conectados y evitar pérdidas o fugas de datos. Más información.

Managed Detection and Response

El componente Managed Detection and Response facilita la interacción con el servicio de Kaspersky Managed Detection and Response, que detecta y elimina continuamente las amenazas de seguridad dirigidas a su organización. Más información.

Endpoint Detection and Response

El componente Endpoint Detection and Response facilita la interacción con la solución Kaspersky Endpoint Detection and Response. Esta solución combina la detección automática de amenazas con la capacidad de reaccionar a estas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. Más información.

Endpoint Detection and Response (KATA)

El componente Endpoint Detection and Response (KATA) facilita la interacción con la solución Kaspersky Anti Targeted Attack Platform. Esta solución detecta de inmediato amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas y ataques de día cero, entre otras. Más información.

Novedades de esta versión

Esta ayuda se aplica a Kaspersky Endpoint Security for Mac versión 12.2.

Kaspersky Endpoint Security ofrece las siguientes funciones nuevas y mejoras:

- El nuevo macOS 27 Golden Gate ahora es compatible.
- El nuevo macOS 26 Tahoe ahora es compatible.
- Añadimos los nuevos componentes Protección frente a amenazas en el correo, Control de dispositivos, Firewall, Motor de reparación y Prevención de exploits.
- Ahora puede activar el componente Managed Detection and Response desde la aplicación Kaspersky Endpoint Security.
- Se mejoró la visibilidad de las acciones de respuesta para los detalles de la alerta.
- Ahora puede administrar el componente Detección de comportamiento en Web Console.
- Añadimos resúmenes de alertas.
- Ahora se le notificará que un objeto es crítico del sistema antes de que se realice cualquier acción de respuesta.
- Ahora puede editar archivos IOC directamente en Web Console al crear o editar la configuración de la tarea de análisis de IOC.
- Ahora puede mover los objetos detectados a Cuarentena desde los detalles de la alerta.
- Añadimos advertencias para acciones restringidas para la tarea de Aislamiento de red.
- Correcciones de errores generales y mejoras.

Comparación de las funciones de Kaspersky Endpoint Security según la herramienta de administración Kaspersky Security Center

La funcionalidad compatible con Kaspersky Endpoint Security depende de la herramienta de administración que use (consulte la tabla siguiente).

Puede usar las siguientes herramientas para administrar Kaspersky Endpoint Security:

- Consola de administración de Kaspersky Security Center. Se ha instalado el complemento de Microsoft Management Console (MMC) en la estación de trabajo del administrador de Kaspersky Security Center.
- Kaspersky Security Center Web Console. Un componente de Kaspersky Security Center que se instala en el servidor de administración. Puede trabajar con la Web Console usando un navegador en cualquier equipo que tenga acceso al servidor de administración.
- Kaspersky Security Center Cloud Console. La versión en la nube de Kaspersky Security Center.

Comparación de las funciones de Kaspersky Endpoint Security

Función	Kaspersky Security Center		
	Consola de administración	Web Console	Cloud Console
Protección frente a amenazas avanzadas			
Kaspersky Security Network	✓	✓	✓
Detección de comportamiento	✓	✓	
Prevención de exploits	✓	✓	
Motor de reparación	✓	✓	
Protección frente a amenazas básicas			
Protección frente a amenazas en archivos	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓
Protección frente a amenazas en el correo	✓	✓	
Firewall	✓	✓	
Controles de seguridad			
Control web	✓	✓	✓
Control de dispositivos	✓	✓	
Cifrado de datos			

Cifrado de disco de FileVault	✓	✓	✓
Clave de recuperación	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	
Endpoint Detection and Response (KATA)	✓	✓	✓
Tareas			
Agregar clave	✓	✓	✓
Actualización	✓	✓	✓
Análisis rápido	✓	✓	
Deshacer	✓	✓	✓
Análisis	✓	✓	✓

Instalar y desinstalar la aplicación

Kit de distribución

El kit de distribución incluye el paquete de instalación de Kaspersky Endpoint Security, que contiene los siguientes archivos:

- Archivos necesarios para instalar la aplicación de cualquiera de las formas disponibles.
- El archivo license_<loc>.txt con el Contrato de licencia de usuario final.
  El Contrato de licencia de usuario final especifica las condiciones de uso de la aplicación.

Descomprima el paquete de instalación para acceder a los archivos.

Requisitos de hardware y software

Kaspersky Endpoint Security tiene los siguientes requisitos de hardware y software:

- Tipo de procesador: Intel, Apple Silicon
- 4 GB de memoria (RAM)
- 5 GB de espacio libre en disco
- Sistema operativo: macOS 13, 14, 15, 26, o 27
- Conexión a Internet

Navegadores compatibles:

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security es compatible con las siguientes herramientas de virtualización:

- Parallels Desktop 16 for Mac Business Edition o versión posterior
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

Los perfiles MDM se pueden implementar con los servidores Jamf y Apple. Si usa otros servidores, consulte el artículo en el sitio web del Servicio de soporte técnico (Base de conocimientos).

Kaspersky Endpoint Security puede administrarse remotamente a través de Kaspersky Security Center. Se requiere Kaspersky Security Center 14.2 o una versión posterior para administrar Kaspersky Endpoint Security mediante el complemento de administración para la Consola de administración de Kaspersky Security Center y el complemento web para Kaspersky Security Center Web Console.

Nota: Para administrar Kaspersky Endpoint Security for Mac 12.2 a través de Kaspersky Security Center, debe instalar el Agente de red versión 15 en los equipos remotos.

Prepararse para la instalación

Antes de instalar la aplicación en su equipo, se recomienda hacer lo siguiente:

- Asegúrese de que el equipo cumpla con los requisitos de hardware y software.
- Elimine Kaspersky Internet Security for Mac o cualquier otra aplicación antimalware para evitar conflictos de sistema y maximizar el rendimiento del sistema.

Nota: Antes de instalar Kaspersky Endpoint Security de forma remota, le recomendamos que descargue el archivo KES_for_macOS11_and_later.zip del sitio web de Soporte técnico de Kaspersky y aplique el perfil de configuración KES_for_macOS11_and_later_profile.mobileconfig en el equipo cliente con las herramientas de administración remota de Apple. Esto permitirá que Kaspersky Endpoint Security obtenga lo siguiente: permisos para instalar la extensión de kernel y la extensión de sistema, acceso total al disco y permisos para configurar las conexiones de red. Para obtener más información sobre el perfil de configuración y otras opciones, visite el sitio web de Servicio de soporte técnico.

Instalar Kaspersky Endpoint Security

Importante: Los especialistas de Kaspersky recomiendan instalar Kaspersky Endpoint Security únicamente de las formas descritas en esta ayuda.

Puede instalar Kaspersky Endpoint Security de una de las siguientes formas:

- Localmente, desde el kit de distribución descargado del sitio web de Kaspersky.
- Remotamente con Apple Remote Desktop.
- Remotamente, a través de la Consola de administración de Kaspersky Security Center.
- Remotamente, a través de Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

  Para obtener información detallada sobre el despliegue de las aplicaciones de Kaspersky mediante Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center. Para obtener información detallada sobre el despliegue de las aplicaciones de Kaspersky mediante Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Para realizar una instalación estándar de Kaspersky Endpoint Security

1. Descomprima el archivo ZIP del kit de distribución.
2. Abra el archivo .dmg que forma parte del contenido del archivo descomprimido.
3. En la ventana que se abre, haga doble clic en **Instalar Kaspersky Endpoint Security**.

   Se abre el asistente de instalación de Kaspersky Endpoint Security.
4. Haga clic en **Instalar**.
5. Siga los pasos del asistente de instalación para completar la instalación.

Cuando la instalación finalice, Kaspersky Endpoint Security se inicia automáticamente. No es necesario reiniciar el equipo.

Nota: Si se utiliza este método de instalación, no se instalarán los componentes Endpoint Detection and Response (KATA), Endpoint Detection and Response (Optimum) ni Sandbox en la nube.

Para realizar la instalación personalizada de Kaspersky Endpoint Security

1. Descomprima el archivo ZIP del kit de distribución.
2. Abra el archivo .dmg que forma parte del contenido del archivo descomprimido.

3. En la ventana que se abre, haga doble clic en **Instalar Kaspersky Endpoint Security**.

   Se abre el asistente de instalación de Kaspersky Endpoint Security.

4. Haga clic en **Personalizar**, desmarque las casillas junto a los componentes que no desea instalar y haga clic en **Continuar**.

5. Siga los pasos del asistente de instalación para completar la instalación.

Cuando la instalación finalice, Kaspersky Endpoint Security se inicia automáticamente. No es necesario reiniciar el equipo.

Instale Kaspersky Endpoint Security en remoto con Apple Remote Desktop

1. En su Mac, escoja **menú Apple** > **Ajustes del sistema** > **General** > **Compartir**.
2. Seleccione la casilla de verificación **Administración remota**.
3. En otra Mac que desee usar como servidor, instale Apple Remote Desktop. Para obtener más información sobre Apple Remote Desktop, consulte Soporte técnico de Apple.
4. Abra Apple Remote Desktop.
5. En la ventana de **Escritorio remoto**, haga clic en **Análisis** a la izquierda y seleccione los dispositivos en los que desea desinstalar Kaspersky Endpoint Security.
6. Haga clic en **Instalar**.
7. En la solicitud de credenciales de administrador, introduzca un nombre de administrador y una contraseña, y haga clic en **Añadir**.
8. Hacer clic en + y seleccione el archivo .dmg con el paquete de instalación de Kaspersky Endpoint Security.
9. Haga clic en **Instalar**.

La instalación de Kaspersky Endpoint Security se inicia en los dispositivos seleccionados.

Preparación de la aplicación para su uso

Una vez instalada la aplicación Kaspersky Endpoint Security, puede hacer lo siguiente:

- Activar Kaspersky Endpoint Security. Cuando se activa la aplicación, Kaspersky Endpoint Security comienza a proteger su equipo. Puede actualizar regularmente las bases de datos y los módulos de la aplicación, realizar tareas de análisis de software malicioso y enviar solicitudes al Soporte técnico.

  El componente Managed Detection and Response se activa por separado en la Consola de administración de Kaspersky Security Center o en Kaspersky Security Center Web Console.

  Si el componente Endpoint Detection and Response no es compatible con su licencia actual, debe activar Kaspersky Endpoint Detection and Response de manera independiente.

- Determinar el estado de protección del equipo.
- Actualizar Kaspersky Endpoint Security.
- Analizar el equipo en busca de software malicioso.

Desinstalar Kaspersky Endpoint Security

1. Abra el archivo DMG del kit de distribución de la aplicación.
2. En la ventana con el contenido del kit de distribución, haga doble clic en **Desinstalar Kaspersky Endpoint Security**.

   Se inicia el programa de desinstalación de Kaspersky Endpoint Security.

3. En la ventana de programa de desinstalación, haga clic en **Desinstalar**.
4. En la solicitud de las credenciales del administrador, introduzca un nombre de administrador y una contraseña, y confirme que desea desinstalar Kaspersky Endpoint Security.

   Se inicia la desinstalación de Kaspersky Endpoint Security.

5. En la ventana Finalización, lea la información acerca de la finalización de la desinstalación y haga clic en **Salir** para salir del programa de desinstalación.

Kaspersky Endpoint Security se ha desinstalado del equipo. No es necesario reiniciar el equipo después de desinstalar la aplicación.

Iniciar la aplicación por primera vez

Kaspersky Endpoint Security se inicia en su equipo justo después de la instalación. Para proteger su Mac de inmediato, la aplicación le solicita que realice la configuración básica:

- Otorgue los permisos necesarios a Kaspersky Endpoint Security para proteger su Mac contra software malicioso, ataques de red y amenazas de Internet.

  Para obtener más información sobre los permisos que otorga, haga clic en (?).

- Activar Kaspersky Endpoint Security.

Nota: Se requiere una conexión a Internet para la configuración básica de Kaspersky Endpoint Security.

Iniciar Kaspersky Endpoint Security por primera vez

1. En la ventana **Protección esencial**, realice las siguientes acciones para garantizar que la Protección frente a amenazas en archivos y la Protección frente a amenazas web funcionen correctamente:

   - Si desea que la aplicación Kaspersky Endpoint Security funcione correctamente, permita que la aplicación analice todos los archivos de su Mac. Para hacerlo, haga clic en **Permitir** junto al elemento **Acceso total al disco** y siga las instrucciones en pantalla.
   - Si desea que Kaspersky Endpoint Security inspeccione las URL y los paquetes de red antes de que puedan hacerle daño a la Mac, instale la extensión de sistema. Para hacerlo, haga clic en **Instalar** junto al elemento **Extensión de sistema** y siga las instrucciones en pantalla.
   - Si desea que la extensión de sistema funcione correctamente, permita el filtrado de contenido de red. Para hacerlo, haga clic en **Permitir** junto al elemento **Filtrado de contenido de red** y siga las instrucciones en pantalla.
   - Si desea que Kaspersky Endpoint Security busque software malicioso y amenazas de Internet en el tráfico HTTPS cifrado, instale el certificado de confianza. Para hacer esto, haga clic en **Instalar** junto al elemento **Certificado de confianza** y siga las instrucciones en pantalla.

   Importante: La aplicación Kaspersky Endpoint Security no funcionará correctamente si no se conceden estos permisos. Debe otorgar todos los permisos en la ventana **Protección esencial**.

2. Haga clic en **Continuar**.

Se abre la ventana principal de la aplicación.

Interfaz de la aplicación Kaspersky Endpoint Security

Ventana principal de la aplicación

Abrir la ventana principal de la aplicación

En la barra de menús, haga clic en el icono de la aplicación y elija **Kaspersky Endpoint Security**.

La ventana principal de la aplicación de Kaspersky Endpoint Security contiene elementos de la interfaz que proporcionan acceso a las funciones principales de la aplicación.

La ventana principal de la aplicación se divide en dos partes:

- La parte izquierda contiene la barra lateral, que le permite navegar por la aplicación y acceder rápidamente a sus funciones principales.
- La parte central muestra el contenido de la sección elegida en la barra lateral y le permite administrar los datos.

Barra lateral

La barra lateral de la ventana principal de la aplicación tiene las siguientes opciones:

Supervisión	Haga clic para abrir la página **Supervisión**, que proporciona información sobre lo que está haciendo Kaspersky Endpoint Security para proteger su equipo.

Centro de protección	Haga clic para ver el estado de protección de su equipo. Más información.
Seguridad	Haga clic para ver el estado operativo de los componentes instalados. Más información.
Análisis	Haga clic para administrar las tareas de análisis. Más información.
Actualizar	Haga clic para administrar las tareas de actualización. Más información.
Licencia	Haga clic para activar la aplicación o ver información sobre su licencia. Más información.

Controles de la página **Supervisión**

La página **Supervisión** muestra el indicador de estado de protección, proporciona información sobre lo que Kaspersky Endpoint Security está haciendo para proteger su equipo y contiene los siguientes controles.

Centro de protección	Le informa de los problemas de protección del equipo. Más información.
Informes	Le permite ver eventos que ocurrieron durante el funcionamiento de la aplicación, componentes individuales y tareas. Más información.
Copia de seguridad	Le permite ver una lista de copias guardadas de archivos infectados que la aplicación ha eliminado. Más información. Más información.
Detección de amenazas	Le permite ver información sobre las tecnologías de detección de amenazas aplicadas por Kaspersky Endpoint Security y la cantidad de amenazas detectadas por estas tecnologías.
Kaspersky Security Network	Muestra el estado de la conexión entre Kaspersky Endpoint Security y Kaspersky Security Network, así como las estadísticas globales de Kaspersky Security Network.

Icono de Kaspersky Endpoint Security

Inmediatamente después de instalar Kaspersky Endpoint Security, el icono de Kaspersky Endpoint Security aparecerá en la barra de menús. Cuando se activa la aplicación, el icono de la aplicación muestra su estado. Si el icono de la aplicación está activo ( ), significa que algunos o todos los componentes de protección están activados. Si el icono de la aplicación está inactivo ( ), significa que todos los componentes de protección están desactivados.

Abrir el menú del icono de la aplicación

En la barra de menús, haga clic en el icono de la aplicación.

De forma predeterminada, el icono de la aplicación se muestra siempre en la barra de menús. Puede eliminar el icono de la aplicación de la barra de menús.

Eliminar el icono de la aplicación de la barra de menús

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Interfaz** de la sección **Icono de aplicación**, desmarque la casilla **Mostrar en barra de menús**.

Cuando abre la ventana de la aplicación, el icono de la aplicación también aparece en el **Dock**.

Desde el menú del icono de la aplicación, puede acceder a la ventana principal de la aplicación y llevar a cabo las siguientes acciones:

- Desactivar la protección del equipo.
- Reanudar la protección del equipo.
- Abrir el Centro de protección.
- Comenzar Análisis rápido.
- Ejecutar una actualización.
- Abrir la ventana de ajustes de la aplicación.
- Salir de Kaspersky Endpoint Security.

Ventana de ajustes de la aplicación

Abrir la ventana de ajustes de la aplicación

Realice una de las siguientes acciones:

- En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
- En la barra de menús, haga clic en **Kaspersky Endpoint Security** > **Ajustes**.
- Si Kaspersky Endpoint Security se está ejecutando, haga clic en el icono de la aplicación en **Dock** y elija **Ajustes**.

Se puede acceder rápidamente a los ajustes de la aplicación utilizando las siguientes pestañas en la parte superior de la ventana de ajustes:

- **Protección**. En esta pestaña, puede activar o desactivar la protección del equipo y establecer la configuración de Protección frente a amenazas en archivos, Protección frente a amenazas web y Protección frente a amenazas en la red.
- **Análisis**. En esta pestaña, puede establecer la configuración de las tareas de análisis y el inicio planificado de las tareas de análisis.
- **Amenazas**. En esta pestaña, puede elegir las categorías de objetos a detectar, crear la Zona de confianza y establecer la configuración de Copia de seguridad.
- **Avanzado**. En esta pestaña, se puede unir a Kaspersky Security Network o abandonarlo.
- **Actualizar**. En esta pestaña, puede establecer la configuración de actualización de la aplicación o volver a la versión anterior de las bases de datos de la aplicación.
- **Interfaz**. En esta pestaña, puede establecer la configuración del icono de Kaspersky Endpoint Security, las notificaciones y los informes, y activar o desactivar el registro de información de depuración en un archivo de rastreo.

El botón  le permite bloquear usuarios sin derechos de administrador al editar la configuración de Kaspersky Endpoint Security. Dicho botón está situado en la parte inferior de la ventana de ajustes de la aplicación. Para editar la configuración, debe introducir las credenciales del administrador.

Al hacer clic en el botón (?), se abre la ayuda de Kaspersky Endpoint Security, que describe todos los ajustes en la ventana de la aplicación actual. También puede abrir el tema de ayuda de la ventana de la aplicación seleccionando la opción **Abrir la ayuda de esta ventana** del menú **Ayuda**.

Acerca de las notificaciones

Kaspersky Endpoint Security muestra notificaciones para informarle de los eventos de la aplicación. En función de la versión del sistema operativo instalado en el equipo, las notificaciones aparecen en el Centro de notificaciones del sistema operativo. La aparición de notificaciones depende de las opciones establecidas en la configuración de notificación del sistema operativo.

Los eventos de Kaspersky Endpoint Security se dividen en tres tipos según su importancia:

- *Críticos*: eventos que representan una amenaza peligrosa para la seguridad del equipo (detección de objetos maliciosos, vulnerabilidades, problemas con Kaspersky Endpoint Security). Los eventos críticos requieren su atención inmediata. Le recomendamos que no desactive las notificaciones sobre eventos críticos.
- *Importantes*: eventos que no precisan su atención inmediata, pero que más adelante pueden representar una amenaza para la seguridad del equipo.
- *Informativas:* eventos comunicados para su información.

Desactivar notificaciones

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Interfaz** de la sección **Notificaciones**, marque o desmarque la casilla de verificación **Activar notificaciones**.

Activar el registro de eventos no críticos

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Interfaz**, en la sección **Informes**, seleccione la casilla de verificación **Registrar eventos no críticos** para recibir notificaciones sobre eventos informativos de Kaspersky Endpoint Security.

Independientemente de si las notificaciones están activadas o desactivadas, los informes de la aplicación incluyen información sobre los eventos que ocurren mientras se ejecuta Kaspersky Endpoint Security.

Las notificaciones pueden ir acompañadas de sonidos (por ejemplo, las notificaciones sobre un software malicioso detectado). Puede desactivar la alerta de sonido.

La carga de eventos no críticos aumenta el tamaño total del archivo de informes de manera considerable. Tenga en cuenta que esta configuración se aplica solo a la Protección frente a amenazas en archivos.

Desactivar las alertas de sonido que acompañan a las notificaciones

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la sección **Interfaz** de la pestaña **Notificaciones**, desmarque la casilla de verificación **Activar sonidos de alerta cuando se detecte software malicioso**.

Si se requiere una acción en respuesta a un evento, Kaspersky Endpoint Security muestra una ventana de notificación. Por ejemplo, cuando la aplicación detecte un objeto malicioso, le solicitará que elimine el objeto o lo desinfecte. La ventana de notificación desaparece de la pantalla solo después de que se seleccione una de las acciones.

Licencias de la aplicación Kaspersky Endpoint Security

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* (Contrato de licencia) es un contrato vinculante entre usted y AO Kaspersky Lab en el que se estipulan las condiciones de uso de la aplicación.

Importante: Lea atentamente el Contrato de licencia antes de comenzar a utilizar la aplicación.

Puede consultar los términos del Contrato de licencia de usuario final de las siguientes maneras:

- Durante la instalación de Kaspersky Endpoint Security
- Al leer el documento license.txt de la carpeta de instalación de aplicación

Al instalar Kaspersky Endpoint Security, confirma que comprende y acepta los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, cancele la instalación de Kaspersky Endpoint Security y no use la aplicación.

Acerca de la licencia

Una *licencia* es el derecho a utilizar la aplicación durante un tiempo limitado, concedido bajo los términos del Contrato de licencia firmado (Contrato de licencia de usuario final).

La cobertura de servicios y el período de validez dependen de la licencia que se utilice para la aplicación.

Existen los siguientes tipos de licencia:

- *De prueba*

  Una licencia gratuita diseñada para probar la aplicación. La licencia de prueba suele durar poco tiempo.

  Cuando caduca una licencia de prueba, se desactivan todas las funciones de Kaspersky Endpoint Security. Si desea continuar utilizando la aplicación, deberá adquirir una licencia comercial.

  Puede usar la aplicación con una licencia de prueba durante solo un período de prueba.

- *Comercial*

  Una licencia de pago.

  Cuando caduca una licencia comercial, se desactivan las funciones clave de la aplicación. Para seguir utilizando Kaspersky Endpoint Security, debe renovar su licencia comercial. Una vez que caduca una licencia comercial, no puede seguir usando la aplicación y debe eliminarla del dispositivo.

  Recomendamos renovar la licencia antes de que caduque para garantizar la protección ininterrumpida contra todas las amenazas de seguridad.

Acerca de la suscripción

Una *suscripción a Kaspersky Endpoint Security* es un pedido de compra para utilizar la aplicación con unos parámetros específicos (fecha de caducidad y número de dispositivos protegidos). Puede solicitar la suscripción a Kaspersky Endpoint Security a su proveedor de servicios (por ejemplo, su proveedor de servicios de Internet). Puede administrar su suscripción en el área de miembros del sitio web del proveedor del servicio. Por ejemplo, puede renovar o cancelar su suscripción, reducir su vigencia o cambiar el número de dispositivos protegidos con su suscripción.

Una suscripción puede ser limitada, por ejemplo, de un año, o ilimitada, es decir, sin fecha de caducidad. Para continuar utilizando Kaspersky Endpoint Security después de un período de suscripción limitado, debe renovar la licencia manualmente. Una suscripción ilimitada se renueva automáticamente mientras haya pagado al proveedor de servicios de antemano.

Si usa la aplicación con una suscripción limitada, cuando esta caduque se le ofrecerá un período de gracia para renovarla. La aplicación permanece funcional durante el período de gracia.

Cuando caduque la suscripción para actualizaciones y finalice el período de gracia para la renovación de la suscripción, Kaspersky Endpoint Security permanecerá funcional, pero ya no actualizará las bases de datos de la aplicación.

Cuando caduque la suscripción para actualizaciones y protección y finalice el período de gracia para la renovación de la suscripción, Kaspersky Endpoint Security deja de proteger el equipo.

Para utilizar Kaspersky Endpoint Security con una suscripción, debe agregar el código de activación proporcionado por el proveedor de servicio. Si utiliza la aplicación con una suscripción, no puede usar un código de activación diferente para renovar su suscripción. Solo puede aplicar un código de activación diferente si la suscripción caduca o la cancela. Para cancelar la suscripción, póngase en contacto con el proveedor de servicio al que compró Kaspersky Endpoint Security.

Nota: Un código de activación de suscripción diferente solo se puede aplicar cuando se elimina la clave activa. La suscripción no tiene un archivo de claves. No puede agregar la suscripción como una clave de reserva. No se puede agregar una clave de reserva cuando se utiliza la suscripción.

Si ya está utilizando Kaspersky Endpoint Security con una licencia válida, pero en lugar de eso desea utilizar la aplicación con una suscripción, quite la clave activa actual para poder activar la aplicación usando una clave de suscripción. El código de activación que ha aplicado para activar la aplicación en este equipo se puede utilizar en otro equipo.

Nota: Las opciones de suscripción posibles pueden variar con cada proveedor de servicios. Algunos proveedores de servicios también pueden decidir no proporcionar un período de gracia para renovar suscripciones.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que recibe junto con un archivo de claves o un código de activación.

Un certificado de licencia contiene la siguiente información sobre la licencia proporcionada:

- Clave de licencia o número de pedido
- Información sobre el usuario al que se le ha concedido la licencia
- Información acerca de la aplicación que se puede activar con la licencia proporcionada
- Límite del número de equipos con licencia (es decir, dispositivos en los que puede utilizarse la aplicación con la licencia proporcionada)
- Fecha de inicio de validez de la licencia
- Fecha de caducidad o vigencia de la licencia
- Tipo de licencia

Acerca de la clave

Una *clave* es una secuencia de bits que puede aplicar para activar y utilizar la aplicación de acuerdo con lo establecido en las condiciones del Contrato de licencia de usuario final. Los especialistas de Kaspersky son los encargados de generar las claves.

Se puede agregar una clave a la aplicación mediante los siguientes métodos: aplicar un *archivo de claves* o introducir un *código de activación*. La clave se muestra en la interfaz de aplicación como una secuencia alfanumérica única después de agregarla a la aplicación.

Kaspersky puede bloquear la clave si se han infringido los términos del Contrato de licencia. Si la clave ha sido bloqueada, tiene que agregar otra para usar la aplicación.

Una clave puede ser activa o de reserva.

Una *clave activa* es una clave que utiliza actualmente la aplicación. Se puede agregar una clave activa para una licencia comercial o de prueba o para una suscripción. La aplicación solo puede utilizar una clave activa.

Una *clave de reserva* es aquella que permite al usuario utilizar la aplicación, pero que no se encuentra en uso. La clave de reserva se activa automáticamente cuando caduca la licencia asociada a la clave activa. Solo es posible agregar una clave de reserva si la clave activa ya se ha agregado.

Una clave de licencia de prueba se puede añadir como clave activa. Una clave para la licencia de prueba no puede agregarse como clave de reserva. No se puede agregar una clave de reserva cuando la clave de licencia de prueba está activa.

Acerca del código de activación

Un *código de activación* es una secuencia única de 20 letras y números. Debe introducir un código de activación para añadir una clave de licencia para activar Kaspersky Endpoint Security. Recibirá el código de activación en la dirección de correo electrónico que proporcionó al adquirir Kaspersky Endpoint Security o al solicitar la versión de prueba de la aplicación.

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

Si ha perdido su código de activación después de instalar la aplicación, póngase en contacto con el partner de Kaspersky a quien le compró la licencia.

Acerca del archivo de claves

Un *archivo de claves* es un archivo con la extensión .key que le proporciona Kaspersky. Los archivos clave están diseñados para activar la aplicación al agregar una clave de licencia.

Recibirá un archivo de claves en la dirección de correo electrónico que proporcionó al adquirir Kaspersky Endpoint Security o al solicitar la versión de prueba de la aplicación.

No será necesario conectarse con los servidores de activación de Kaspersky para activar la aplicación con un archivo de claves.

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

Para restaurar su archivo de claves, realice una de las siguientes acciones:

- Comuníquese con el vendedor de la licencia.
- Consiga un archivo de claves a través del sitio web de Kaspersky que corresponda a su código de activación disponible.

Acerca de la provisión de datos

Contrato de licencia de usuario final

Al activar Kaspersky Endpoint Security utilizando el código de activación, con objeto de verificar el uso legítimo de la aplicación y brindar información estadística sobre la distribución y el uso de los productos de Kaspersky, usted acepta facilitar automáticamente la siguiente información durante el uso de Kaspersky Endpoint Security:

- Tipo, versión y localización del Software instalado.
- Versiones de las actualizaciones instaladas.
- El identificador del equipo y el identificador de la instalación del software en el equipo.
- El código de activación y el identificador de activación único para la licencia actual.
- El tipo, versión y tamaño de la palabra del sistema operativo.
- Nombre del entorno virtual si el Software se instala en un entorno virtual.
- Identificadores de los componentes de Software activos al momento de proporcionar la información.
- El origen de datos compatible.
- Tiempo de espera.
- Fecha y hora del equipo del usuario.
- Versión del protocolo.
- Tipo de contenido del protocolo.
- Longitud de contenido del protocolo.
- Tipo de compresión de datos utilizado.
- Tipo de firma del resguardo de activación.
- Identificador del centro de activación regional.
- Hash del código de activación calculados con el algoritmo SHA1.
- Hash del cuerpo del resguardo calculados con el algoritmo SHA1.

- Fecha y la hora de creación del resguardo de la licencia.
- Identificador de activación de la licencia.
- Identificador del resguardo de la licencia actual.
- Identificador de la secuencia de ticket de la licencia.
- Fecha y la hora de activación de la licencia.
- Fecha y la hora de caducidad de la licencia.
- Estado de la licencia.
- Versión de la licencia.
- Identificador único del equipo del usuario.
- Versión del encabezado del resguardo de la licencia.
- Nombre de la aplicación.
- Tipo de datos transferidos.
- Versión del esquema de datos transferidos.
- Versión completa del sistema operativo.
- Descripción de la máquina virtual utilizada.
- Lista de Id. para aplicaciones compatibles.

Cuando usa los servidores de actualización de Kaspersky para descargar las actualizaciones, para aumentar la eficiencia del procedimiento de actualización, acepta brindar periódicamente la siguiente información para la identificación de la aplicación durante las actualizaciones de bases de datos y del módulo:

- ID de Software (AppID).
- ID de licencia activa.
- ID único de instalación del software (InstallationID).
- ID de inicio de tarea de actualización única (SessionID).
- Versión de la aplicación (BuildInfo).

Declaración de recopilación de datos de Kaspersky Security Network (KSN)

El uso de KSN puede aumentar la velocidad de reacción del Software a la información y a amenazas de seguridad de la red. El objetivo declarado se consigue al:

- La determinación de la reputación de los objetos analizados.
- La identificación de amenazas de seguridad informática que son nuevas y difíciles de detectar, y sus fuentes.
- Tomar medidas rápidas para mejorar la protección de los datos almacenados y procesados por un usuario con el equipo.
- La reducción de la probabilidad de falsos positivos.
- El aumento de la eficacia de los componentes de la aplicación.
- Investigar posibles infecciones en el equipo del usuario.
- La mejora del rendimiento de los productos de Kaspersky.
- La recepción de información de referencia sobre el número de objetos con reputación conocida.
- La identificación y corrección tempranas de errores relacionados con la instalación, la eliminación y la actualización del producto.

Durante el uso de KSN, Kaspersky recibirá y procesará automáticamente datos. Los datos transmitidos por el usuario dependen del tipo de licencia instalada y de la configuración de uso de Kaspersky Security Network especificada.

Si utiliza una licencia para 1 a 4 nodos, Kaspersky recibirá y procesará automáticamente los siguientes datos durante el uso de Kaspersky Security Network:

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Versión completa del software instalado; tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. de dispositivo único; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

Si utiliza una licencia para 5 o más nodos, Kaspersky recibirá y procesará automáticamente los siguientes datos durante el uso de Kaspersky Security Network:

- Información sobre la versión del sistema operativo (SO) y los paquetes de servicios instalados en el ordenador, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del sistema operativo y los parámetros del modo de ejecución del sistema operativo; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO; versión de Service Pack del SO; fecha y hora de inicio del SO; tiempo de demora del procesamiento del evento acerca de la acción del SO en el subsistema de análisis de comportamiento; cantidad de eventos de acción del tipo actual demorados del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactiva; cantidad de eventos de acciones del SO procesados; cantidad de eventos de acción sincrónicos procesados del SO; demora total de todos los eventos de acción del tipo actual del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento de eventos persistentes; demora total de todos los eventos de acción del SO; cantidad de eventos de acción sincrónicos del SO en espera; fecha y hora del evento recibido por una acción en el SO.

- Información sobre el último reinicio fallido del sistema operativo: número de reinicios fallidos.

- Información sobre la aplicación instalada del Titular de los derechos y el estado de la protección antivirus: id. de instalación del software (PCID); versión del registro de la base de datos del software; el identificador único de la instancia de la instalación de la aplicación en el ordenador, el tipo de aplicación, id. del tipo de aplicación, la versión completa de la aplicación instalada, el identificador de la versión de configuración de la aplicación, el identificador del tipo de ordenador, el identificador único del ordenador en el que está instalada la aplicación, el identificador de Usuario único en los servicios del Titular de los derechos, el idioma regional y el estado de funcionamiento, la versión de los componentes de Software instalados y su estado de funcionamiento, la versión del protocolo utilizado para conectarse con los servicios del Titular de los derechos; versión completa del software instalado; tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); cantidad de ciclos de actualizar y aplicar para bases de datos antivirus; fecha y hora de la última actualización y aplicación de las bases de datos antivirus; Fecha y hora de lanzamiento de las bases de datos del software; versión del componente del Software; id. de actualización de software; tipo del software instalado; fecha y hora de inicio de System Watcher; fecha y hora de instalación del software; probabilidad de enviar estadísticas por medio de System Watcher; código del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo máximo permitido para el procesamiento de un evento por parte de System watcher; tiempo de procesamiento del evento que tardó más tiempo del estándar en ser procesado por System Watcher; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por System Watcher.

- Información sobre todos los objetos y operaciones procesados: veredicto del software del objeto que se procesa; código de directorio; tamaño del objeto que se procesa; suma de control (SHA256) del objeto que se procesa; número del software detectado en el contexto de System Watcher; fecha y hora de detección de software por parte de System Watcher; detectar características; ID del registro activado en las bases de datos Antivirus del software; motivo de detección de software por System Watcher; suma de control (MD5) del objeto que se procesa; resultado de la comprobación de integridad del módulo; nombre del objeto que se procesa; tipo de registro en las bases de datos antivirus del software activado; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; la dirección URL y del referente desde las que se descargó; el tamaño de los archivos analizados y las rutas hasta ellos; la señal del archivo; la fecha y la hora de creación del archivo; el nombre, el tamaño y las sumas de control (MD5, SHA2-256) del compresor (si el archivo estaba comprimido); la entropía del archivo; el tipo de archivo; el código de tipo de archivo; la señal, el ID y el formato del archivo ejecutable; la suma de control del objeto (MD5, SHA2-256); el tipo y el valor de la suma de control complementaria del objeto; datos sobre la firma digital (certificado) del objeto: datos sobre el editor del certificado, número de inicios del objeto desde el envío de la última estadística, ID de la tarea de análisis de la aplicación, los medios para recibir información sobre la reputación del

objeto, el valor del filtro de destino, los parámetros técnicos de las tecnologías de detección aplicables; ruta hacia el objeto que se procesa; código de directorio.

- Para archivos ejecutables: la entropía de las secciones del archivo, la marca de verificación de reputación o la marca de la firma del archivo, el nombre, el tipo, el tipo de ID, la suma de comprobación (MD5) y el tamaño de la aplicación cargada por el objeto que se está validando, la ruta de la aplicación y las rutas de las plantillas, un atributo que indica la presencia de la lista de autoejecución, la fecha de entrada, la lista de atributos, el nombre del compresor e información sobre la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME y la fecha y hora de creación del archivo.

- Información sobre las aplicaciones iniciadas y sus módulos: sumas de comprobación (MD5, SHA2-256) de los archivos en ejecución, tamaño, atributos, fecha de creación, nombre del compresor (si el archivo estaba comprimido), nombres de los archivos, información sobre los procesos que se ejecutan en el sistema (identificación del proceso [PID]), nombre del proceso, información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, la ruta completa a los archivos del proceso y la línea de comandos de inicio, una descripción de la aplicación a la que pertenece el proceso (el nombre de la aplicación e información sobre el editor), así como los certificados digitales que se usan e información necesaria para verificar su autenticidad o información sobre la ausencia de firma digital de un archivo e información sobre los módulos cargados en los procesos: sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación (MD5, SHA2-256, SHA1); las rutas a ellos; la información del encabezado de archivo PE; los nombres de los compresores (si se comprimió el archivo); la información sobre la disponibilidad y validez de estas estadísticas y el identificador del modo para generar las estadísticas que se envían.

- En caso de detectar una amenaza o vulnerabilidad, además de la información sobre el objeto escaneado se deberá proporcionar información sobre el identificador, la versión y el tipo de registro en la base de datos del antivirus; el nombre de la amenaza según la clasificación de Kaspersky, la fecha y la hora de la última actualización de la base de datos del antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de aplicación que solicitó la URL y en la cual ocurrió la detección; la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador del tipo de tráfico en el cual fue detectada la amenaza, el identificador de vulnerabilidad y el nivel de la amenaza recibida, la dirección URL y de referencia de la página web en la cual fue detectada la vulnerabilidad.

- Si se detectase un objeto potencialmente malicioso, se proveerá información sobre los datos contenidos en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo que realiza el ataque y número del puerto del equipo del usuario víctima del ataque de red, ID del protocolo de ataque, y nombre y tipo de ataque.

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

- El URL y la dirección IP del sitio web en el cual fue detectado el contenido malicioso o sospechoso; nombre, dimensión y suma de chequeo del archivo que solicitó dicho URL; identificador, peso y grado de aplicación de la norma establecida para dar el veredicto y objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: el estado de finalización de la tarea de actualización, el tipo de error que podría haber ocurrido durante el proceso de actualización, el número de actualizaciones fallidas y el identificador del componente de la aplicación que realiza las actualizaciones.

- Información acerca del uso de Kaspersky Security Network (KSN): el identificador de KSN, el identificador de la aplicación, la versión completa de la aplicación, la dirección IP impersonal del dispositivo del usuario, indicadores del nivel de satisfacción de las solicitudes de KSN, indicadores de la calidad de procesamiento de paquetes de KSN, indicadores del número de solicitudes de KSN e información sobre los tipos de solicitudes de KSN, fecha y hora en que se inició el envío de estadísticas, fecha y hora en que finalizó el envío de estadísticas, información sobre actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida y código de error de la actualización de la configuración.

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se ha detectado el evento, tipo y categoría de evento, nombre de la fuente del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la cual se solicita la reputación y el Referente, la conexión del tipo de protocolo de la conexión, el identificador interno del tipo de aplicación, el número del puerto usado, el identificador del Usuario, la suma de comprobación del archivo escaneado (MD5), el tipo de amenaza detectada, información sobre el registro usado para detectar una amenaza (el identificador del registro para las bases de datos antivirus, el registro de la marca de tiempo y el tipo); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

- Datos sobre la distribución territorial de la aplicación: la fecha de la instalación y activación de la aplicación, el ID del partner que proporciona la licencia para la activación de la aplicación, el ID de la aplicación, el ID de localización de idioma de la aplicación, el número de serie de la licencia de activación de la aplicación y el indicio de participación en KSN.

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Información sobre el hardware instalado en el equipo: tipo, nombre, nombre del modelo, versión de firmware y parámetros de los dispositivos integrados y conectados.

- Información sobre el dispositivo: ID de dispositivo.

- Información sobre el funcionamiento del componente Control web: la versión del componente, el motivo de la categorización, información adicional sobre el motivo de la categorización, la URL categorizada y la dirección IP de host de objeto bloqueado/categorizado.

También, a fin de conseguir el objetivo declarado de aumentar la eficacia de la protección proporcionada por la aplicación, Kaspersky puede recibir objetos que podrían ser explotados por intrusos para hacer daño al equipo y crear amenazas de seguridad informática. Estos objetos son:

- Archivos ejecutables o no ejecutables, o algunas de sus partes
- Áreas de la RAM del equipo
- Sectores involucrados en el proceso de arranque del SO
- Paquetes de datos de tráfico de red
- Páginas web y correos electrónicos que contienen objetos sospechosos o maliciosos
- Descripción de clases e instancias de clases para el almacenamiento WMI
- Informes de actividad de la aplicación

Los informes de actividad de la aplicación contienen la siguiente información sobre los archivos y procesos:

- Nombre, tamaño y versión del archivo que se envía, su descripción y sumas de comprobación (MD5, SHA2-256, SHA1), ID del formato, el nombre de su fabricante, el nombre de la aplicación a la que pertenece el archivo, la ruta totalmente calificada al archivo en el equipo y el código de la ruta de la plantilla, fecha y hora de creación del archivo y la actualización.
- Fecha de inicio y finalización de la validez del certificado y las horas si el archivo enviado tiene una firma digital, fecha y hora en que se firmó el certificado, nombre del emisor del certificado, información sobre el titular del certificado, impresión y clave pública del certificado y los algoritmos usados para calcularlos, número de serie del certificado.
- El nombre de la cuenta que había ejecutado el proceso.
- Las sumas de comprobación (MD5, SHA2-256, SHA1) para el nombre del equipo que ejecuta el proceso.
- Los encabezados de las ventanas del proceso.
- ID para las bases de datos antivirus, nombre de la amenaza identificada según la clasificación de Kaspersky.
- La información sobre la licencia usada para la aplicación, ID de la licencia, su tipo y fecha de caducidad.
- La hora local del equipo del momento en que se proporcionó la información.
- Los nombres y las rutas de los archivos a los que accedió el proceso.
- Direcciones URL e IP a las que accedió el proceso.
- Direcciones URL e IP desde las que se descargó el archivo en ejecución.

Además, para lograr el objetivo declarado con respecto a la prevención de falsos positivos, el Titular de los derechos puede recibir archivos ejecutables y no ejecutables de confianza, o bien partes de estos.

Lea la Declaración de Kaspersky Security Network

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Avanzado**, haga clic en **Mostrar la Declaración de KSN**.

Kaspersky Endpoint Security guarda la siguiente información en un archivo de rastreo:

- Información sobre el dispositivo y el sistema operativo (ID exclusivo del dispositivo, tipo de dispositivo, direcciones MAC de dispositivos de red, tipo de sistema operativo, versión del sistema operativo).
- Información sobre la operación de la aplicación y sus módulos.
- Información sobre la suscripción (tipo de suscripción, región).
- Información sobre la configuración regional del idioma, ID de la aplicación, personalización de la aplicación, versión de la aplicación, ID exclusivo de instalación de la aplicación, ID exclusivo del equipo.

- Información sobre el estado de protección contra software malicioso del equipo, así como sobre todos los objetos detectados y procesados (el nombre del objeto detectado, la fecha y hora de la detección, la dirección web de descarga, los nombres y tamaños de los archivos infectados y sus rutas, la dirección IP del equipo atacante y el número de puerto del equipo al que se dirige el ataque de red, la lista de actividad de software malicioso y las direcciones web no deseadas) y las acciones relevantes y decisiones tomadas por la aplicación y el usuario.
- Información sobre las aplicaciones descargadas por el usuario (dirección web, cualidades, tamaño de archivo e información sobre el proceso de descarga del archivo).
- Información sobre las aplicaciones iniciadas y sus módulos (tamaño, tributos, fecha de creación, detalles del encabezado del PE, región, nombre, ubicación y compresores).
- Información sobre los errores de interfaz y el uso de la interfaz de la aplicación de Kaspersky instalada.
- Información sobre conexiones de red: la dirección IP del equipo remoto y del equipo del usuario, los números de puertos a través de los que se estableció la conexión y el protocolo de red de la conexión.
- Información sobre los paquetes de red recibidos y enviados por el equipo sobre las redes de TI y de telecomunicaciones.
- Información sobre los mensajes de correo electrónico e instantáneos enviados y recibidos.
- Información sobre las direcciones web visitadas: la hora en que se estableció la conexión con un protocolo abierto, los datos de inicio de sesión y la contraseña del sitio web, y el contenido de las cookies.
- Certificado público del servidor.

Los archivos de rastreo solo contienen la información necesaria para corregir defectos de la aplicación. Kaspersky utiliza los archivos de rastreo para investigar los incidentes asociados a errores en el funcionamiento de la aplicación Kaspersky Endpoint Security.

De forma predeterminada, la creación de archivos de rastreo está desactivada. Puede activar la generación de archivos de rastreo en los ajustes de la aplicación.

Los archivos de rastreo se pueden enviar a Kaspersky solo de forma manual. La aplicación no envía los archivos de rastreo a Kaspersky de manera automática.

Puede elegir cómo se envían los archivos de rastreo a Kaspersky.

Antes de enviar archivos de rastreo a Kaspersky, examine los datos que contienen.

Importante: Los archivos de rastreo pueden contener información personal o confidencial. Al enviar archivos de rastreo a Kaspersky, acepta proporcionarle a Kaspersky todos los datos almacenados en los archivos de rastreo que envía y también acepta el método usado para enviarlos.

Los archivos (o partes de estos) que los intrusos pueden aprovechar para dañar el equipo o los datos también se pueden enviar a Kaspersky para su análisis.

Kaspersky protege toda información recibida de acuerdo con la ley y las normas aplicables de Kaspersky. Los datos se transmiten a través de un canal seguro.

La participación en Kaspersky Security Network es voluntaria. La decisión de participar se toma al instalar la aplicación. No obstante, podrá cambiar de opinión más adelante en cualquier momento.

Activar Kaspersky Endpoint Security

Importante: Antes de activar Kaspersky Endpoint Security, asegúrese de que la fecha y hora establecidas en el equipo coincidan con la fecha y hora reales.

Para realizar la activación, se debe agregar una clave a la aplicación. El componente Managed Detection and Response se activa por separado. Para utilizar este componente, debe activar Kaspersky Managed Detection and Response en la Consola de administración de Kaspersky Security Center o en Kaspersky Security Center Web Console.

Si el componente Endpoint Detection and Response no es compatible con su licencia actual, debe activar Kaspersky Endpoint Detection and Response de manera independiente.

Nota: Se requiere una conexión a Internet para activar la aplicación.

Activar la versión de prueba

1. Abra la ventana principal de la aplicación.

2. En la barra lateral de la ventana principal de la aplicación, haga clic en **Licencia**.

   Se abre la ventana **Licencia**.

3. En la ventana **Licencia** que se abre, haga clic en **Activar**.

   Kaspersky Endpoint Security se conecta a los servidores de activación de Kaspersky y envía los datos para que se verifiquen. Si se supera esta verificación, la aplicación recibe y agrega una clave para la versión de prueba gratuita.

   Importante: Únicamente puede activar una versión de prueba de Kaspersky Endpoint Security si no se ha activado anteriormente la aplicación en el equipo.

Activar la aplicación mediante un código de activación

1. Abra la ventana principal de la aplicación.
2. En la barra lateral de la ventana principal de la aplicación, haga clic en **Licencia**.

   Se abre la ventana **Licencia**.

3. En la ventana **Licencia**, introduzca el código de activación que recibió al comprar Kaspersky Endpoint Security.
4. Haga clic en **Activar**.

   Nota: Un código de activación es una combinación única de veinte letras y números latinos agrupados de la siguiente manera: xxxxx-xxxxx-xxxxx-xxxxx.

   La aplicación se conecta a los servidores de activación de Kaspersky y envía el código de activación para verificar su autenticidad. Si se verifica el código de activación, se recibirá la clave de licencia en la aplicación y la agregará automáticamente.

   Nota: Según el código de activación que reciba, puede que deba completar un formulario de registro.

Si no se supera la verificación del código de activación, se mostrará la notificación correspondiente. En ese caso, póngase en contacto con el proveedor de software que le haya facilitado este código de activación.

Después de activar la aplicación con el código de activación, puede ver la siguiente información en la ventana **Licencia**:

- Estado de la licencia o suscripción
- Claves activas
- Claves de reserva (si existen)
- El tipo de licencia y el número de equipos en los que puede utilizar la aplicación con la licencia o la suscripción actuales
- Funciones de la aplicación que están disponibles con la licencia o suscripción actuales
- Fecha y hora de vencimiento de la licencia
- Número de días hasta la caducidad de la licencia

Ver la información de la licencia

Ver la información de la licencia

1. Abra la ventana principal de la aplicación.
2. En la barra lateral de la ventana principal de la aplicación, haga clic en **Licencia**.

   Se abre la ventana **Licencia**.

La ventana **Licencia** puede contener la siguiente información:

- Estado de la licencia o suscripción

- Claves activas
- Claves de reserva (si existen)
- El tipo de licencia y el número de equipos en los que puede utilizar la aplicación con la licencia o la suscripción actuales
- Funciones de la aplicación que están disponibles con la licencia o suscripción actuales
- Fecha y hora de vencimiento de la licencia
- Número de días hasta la caducidad de la licencia

Gestionar licencias y suscripciones

Deberá renovar la licencia si ha caducado la licencia asociada a la clave activa y no ha agregado ninguna clave de reserva. Cuando la licencia caduca, la aplicación continúa funcionando con una funcionalidad limitada (las actualizaciones, Kaspersky Security Network, Control Web y el cifrado de disco de FileVault a través de Kaspersky Security Center dejan de estar disponibles). Aún podrá utilizar todos los componentes de la aplicación y ejecutar análisis de software malicioso, aunque únicamente con las bases de datos antimalware que se hubieran instalado antes del vencimiento de la licencia.

Importante: Cuando sus bases de datos antimalware quedan desactualizadas, el equipo se expone a un riesgo mayor de infección.

Renovar una licencia

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Centro de protección**.
   La ventana **Centro de protección** se abre.
2. En la ventana **Centro de protección**, haga clic en **Renovar**.

Se abre una página web con información sobre cómo renovar su licencia a través de la tienda en línea de Kaspersky o las empresas asociadas de Kaspersky. Al renovar una licencia a través de una tienda en línea y tras realizar el pago, se enviará un código de activación para Kaspersky Endpoint Security a la dirección de correo electrónico especificada en el formulario de pedido.

Al utilizar la aplicación con una suscripción, Kaspersky Endpoint Security se pone en contacto automáticamente con el servidor de activación en intervalos concretos hasta el momento del vencimiento de la suscripción.

Si utiliza la aplicación con una suscripción ilimitada, Kaspersky Endpoint Security renovará su suscripción sin que tenga que hacer nada.

Si usa la aplicación con una suscripción limitada y el período de gracia para renovar la suscripción ha terminado, Kaspersky Endpoint Security se lo notifica y deja de intentar renovar la suscripción y actualizar las bases de datos de la aplicación automáticamente.

Puede renovar manualmente su suscripción poniéndose en contacto con el proveedor al que compró Kaspersky Endpoint Security.

Renovar su suscripción

1. Abra la ventana principal de la aplicación.
2. En la barra lateral de la ventana principal de la aplicación, haga clic en **Licencia**.
   Se abre la ventana **Licencia**.
3. En la ventana **Licencia**, haga clic en **Visitar el sitio web del proveedor de servicios**.

Se abre el sitio web de su proveedor de servicios.

El estado de su suscripción puede desactualizarse. En ese caso, deberá actualizar el estado de la suscripción de forma manual. Si no tiene una suscripción actual, Kaspersky Endpoint Security deja de actualizar las bases de datos de la aplicación (si tiene suscripción a actualizaciones) o deja de proteger el equipo (si tiene una suscripción a actualizaciones y protección).

Actualizar el estado de la suscripción

1. Abra la ventana principal de la aplicación.
2. En la barra lateral de la ventana principal de la aplicación, haga clic en **Licencia**.
   Se abre la ventana **Licencia**.

3. En la ventana **Licencia**, haga clic en el botón .

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

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

Comparación de las funciones de Kaspersky Endpoint Security

Función	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Protección frente a amenazas avanzadas						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓
Motor de reparación	✓	✓	✓	✓	✓	✓
Protección frente a amenazas básicas						
Protección frente a amenazas en archivos	✓	✓	✓	✓	✓	✓
Protección frente a amenazas web	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en el correo	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Protección frente a amenazas en la red	✓	✓	✓	✓	✓	✓
Controles de seguridad						
Control de dispositivos	✓	✓	✓	✓	✓	✓
Control web	✓	✓	✓	✓	✓	✓
Cifrado de datos						
Cifrado de disco de FileVault	–	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *(La licencia de Kaspersky Sandbox se debe comprar por separado)*	✓	✓	✓	✓	✓	✓

Ejecutar tareas habituales

Abrir la aplicación y salir de ella

Expandir todo | Contraer todo

En cuanto termine la instalación, la aplicación se iniciará automáticamente y aparecerá el icono de la aplicación en la barra de menús.

Abrir la aplicación

En la barra de menús, haga clic en el icono de la aplicación y elija **Kaspersky Endpoint Security**.

Salir de la aplicación

En la barra de menús, haga clic en el icono de la aplicación y elija **Salir**.

Cuando sale de la aplicación, el proceso de la aplicación se elimina de la memoria del equipo.

Importante: Después de salir de la aplicación Kaspersky Endpoint Security, el equipo deja de estar protegido y puede infectarse, lo que supone un riesgo de pérdida de datos.

Ver el estado de protección del equipo

El indicador del estado de protección, que tiene forma de escudo y está situado en la ventana principal de la aplicación, le informa sobre los problemas de protección de su equipo. Según el estado de protección del equipo, el color del indicador puede cambiar. Si Kaspersky Endpoint Security descubre alguna amenaza de seguridad, aparece un mensaje sobre amenazas en la ventana principal de la aplicación y el indicador cambia de color.

El color del indicador puede cambiar de los siguientes modos:

- **Verde**. Su equipo está protegido de forma apropiada.

  Un indicador verde significa que las bases de datos antimalware están actualizadas y que todos los componentes de la aplicación se han configurado siguiendo las recomendaciones de Kaspersky. No se han detectado objetos maliciosos o todos los objetos maliciosos detectados se han neutralizado.

- **Amarillo**. Se reduce el nivel de la protección del equipo.

  Un indicador amarillo significa que Kaspersky Endpoint Security ha detectado un problema. Estos problemas incluyen pequeñas desviaciones de la configuración de protección recomendada o las bases de datos de aplicaciones ligeramente obsoletas.

- **Rojo**. Su equipo tiene un riesgo de infección.

  Un indicador rojo significa que hay problemas peligrosos que pueden resultar en la infección del equipo y la pérdida de datos. Por ejemplo, las bases de datos antimalware de la aplicación son muy obsoletas, la aplicación no está activada o se han detectado objetos maliciosos.

  Recomendamos que solucione cualquier problema y resuelva las amenazas de la seguridad cuanto antes.

Ver el estado operativo de los componentes instalados

Kaspersky Endpoint Security le permite verificar el estado de los componentes de la aplicación instalados en la ventana **Seguridad**. El indicador que aparece junto al nombre de cada componente refleja su estado.

Ver el estado del componente

1. Abra la ventana principal de la aplicación.
2. En la barra lateral de la ventana principal de la aplicación, haga clic en **Seguridad**.

   Se abre la ventana **Seguridad**.

Es posible que se muestren los siguientes indicadores de estado:


El componente se está ejecutando.


El componente se está ejecutando y es administrado por una directiva de seguridad.


El componente no funciona correctamente.


El componente ha presentado un error de funcionamiento y es administrado por una directiva de seguridad.

El componente está desactivado.

El componente está desactivado y es administrado por una directiva de seguridad.


El componente está en pausa.


El componente no es compatible con la licencia actual.

Nota: Para algunos componentes, también puede usar el menú de 3 puntos junto al nombre del componente para abrir un informe o configurar los ajustes del componente.

Desactivar y reanudar la protección del equipo

De forma predeterminada, Kaspersky Endpoint Security se inicia cuando se carga el sistema operativo y protege su equipo hasta que se apaga. Todos los componentes de protección (Protección frente a amenazas en archivos, Protección frente a amenazas web y Protección frente a amenazas en la red) se activan y ejecución.

Puede desactivar completamente la protección o solo unos componentes específicos de esta.

Importante: Kaspersky recomienda que no desactive la protección o los componentes de protección, ya que esto puede hacer que su equipo se infecte y que se pierdan datos.

Cuando la protección del equipo está desactivada, se producen las siguientes situaciones:

- El icono de la aplicación de la barra de menús está inactivo.
- El indicador de estado de protección de la ventana principal de la aplicación se muestra de color rojo.

Cuando uno o varios componentes de protección se desactivan, el indicador de estado de protección del equipo se muestra de color rojo o amarillo.

Nota: La desactivación o la suspensión de los componentes de protección no afecta a las tareas de análisis ni a la tarea de actualización.

Puede desactivar/reanudar la protección del equipo mediante uno de los siguientes métodos:

- Desde el icono de la aplicación
- Desde la ventana de ajustes de la aplicación
- Desde el menú **Protección**

Desactivar/reanudar la protección del equipo desde el icono de la aplicación

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Desactivar protección/Activar protección**.
   Cuando desactiva la protección, aparece un mensaje que solicita las credenciales del administrador.
2. En la solicitud de las credenciales del administrador, introduzca un nombre de administrador y una contraseña, y confirme que desea desactivar la protección.

Deshabilitar/reanudar la protección del equipo desde la ventana de ajustes de la aplicación

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Protección**, en la sección **General**, active/desactive la casilla **Activar protección**.

Desactivar/reanudar la protección del equipo desde la barra de menús

En la barra de menús, haga clic en **Protección** > **Desactivar protección/Activar protección**.

Importante: Si desactiva la protección del equipo, esta no volverá a activarse automáticamente cuando Kaspersky Endpoint Security se inicie de nuevo. Debe volver a activar la protección del equipo manualmente.

Desactivar un componente de protección

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la sección **<nombre del componente>** de la pestaña **Protección**, desmarque la casilla **Activar <nombre del componente>**.

Importante: Si ha desactivado un componente de protección, este no volverá a activarse automáticamente cuando Kaspersky Endpoint Security se inicie de nuevo. Debe volver a activar el componente de protección manualmente.

Activar un componente de protección

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la sección **<nombre del componente>** de la pestaña **Protección**, marque la casilla **Activar <nombre del componente>**.

Para activar la protección del equipo o los componentes de protección, también puede utilizar el Centro de protección. La desactivación de la protección del equipo o de componentes de protección pone a su equipo en un riesgo mucho mayor de infección. Por eso, el Centro de protección informa cuando la protección de su equipo está desactivada.

Utilización del Centro de protección

Centro de protección es una función de Kaspersky Endpoint Security que le ayuda a analizar y corregir problemas y amenazas de seguridad informática.

Abrir el Centro de protección

En la barra lateral de la ventana principal de la aplicación, haga clic en **Centro de protección**.

En Centro de protección, puede encontrar información sobre amenazas activas, ver el estado de las bases de datos de la aplicación y averiguar si algún componente de protección está desactivado.

Nota: Si el administrador del sistema de su organización activa el Control Web para bloquear el acceso a recursos web peligrosos, Kaspersky Endpoint Security muestra la notificación **Control web está activado** en el Centro de protección.

Para cada problema o amenaza, Kaspersky Endpoint Security sugiere acciones que puede realizar para resolver el problema o la amenaza. Por ejemplo, si Kaspersky Endpoint Security descubre archivos infectados en el equipo, puede hacer clic en **Desinfectar**. Si las bases de datos antimalware están desactualizadas, puede hacer clic en el botón **Actualizar**. Puede corregir un problema o neutralizar una amenaza de inmediato o hacerlo más tarde.

Corregir un problema o neutralizar una amenaza inmediatamente

Haga clic en el botón que lleva el nombre de la acción recomendada para corregir el problema o neutralizar la amenaza.

La aplicación realiza la acción seleccionada.

Si ha cerrado el Centro de protección sin neutralizar las amenazas peligrosas, el indicador de estado de protección que aparece en la ventana principal de la aplicación continuará en color rojo para recordarle estas amenazas.

Ejecutar tareas de análisis

La tarea Análisis completo predeterminada está incluida en Kaspersky Endpoint Security. Durante la ejecución de esta tarea, la aplicación analiza la memoria, los objetos de inicio y todas las unidades internas del equipo en busca de virus y otro software malicioso.

Realizar un análisis completo del equipo

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.

   Se abre la ventana **Análisis**.

2. Haga clic en el botón **Análisis completo**.

Se iniciará un análisis completo del equipo.

La tarea Análisis rápido predeterminada está incluida en Kaspersky Endpoint Security. Durante la ejecución de esta tarea, la aplicación analiza las áreas críticas del equipo (memoria, objetos de inicio y carpetas del sistema) en busca de virus y otro software malicioso.

Realizar un análisis rápido del equipo

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.
   Se abre la ventana **Análisis**.
2. Haga clic en el botón **Análisis rápido**.

Se iniciará un análisis rápido del equipo.

Si desea analizar objetos concretos (como un disco interno, una carpeta, un archivo o un disco extraíble) en busca de virus y otros tipos de software malicioso, puede utilizar la tarea de Análisis personalizado.

Analizar un archivo seleccionado

Realice una de las siguientes acciones:

- Haga clic con el botón derecho del ratón en un elemento seleccionado y elija **Analizar en busca de software malicioso**.
- Arrastre el elemento seleccionado al icono de la aplicación en el Dock.
- Arrastre un elemento seleccionado en la ventana **Análisis**.

Puede ver los resultados de las tareas de análisis completadas en la ventana **Informes**.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Configurar el inicio automático de una tarea de análisis programada

Puede crear la programación de inicio de las tareas Análisis rápido y Análisis completo. Kaspersky Endpoint Security analiza automáticamente todo el equipo o las áreas especificadas de este de acuerdo con la programación configurada.

Programar una tarea de análisis desde la ventana Análisis

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.
   Se abre la ventana **Análisis**.
2. Haga clic en **Planificar análisis**.
   Se abre un cuadro de diálogo donde podrá definir el análisis.
3. Seleccione la casilla **Análisis completo** o **Análisis rápido**.
4. Especifique la frecuencia y hora de inicio del análisis.
5. Haga clic en **Aceptar**.

Planificar una tarea de análisis desde la ventana de Ajustes

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Análisis**, haga clic en **Planificar**.
3. En la ventana que se abre, seleccione la casilla de verificación al lado del nombre de la tarea de análisis que desea iniciar en una programación.
4. Configure la hora y la frecuencia de la tarea de análisis.
5. Haga clic en **Aceptar** para guardar los cambios realizados en la programación de tareas de análisis.

Puede ver los resultados de la tarea de análisis en la ventana **Informes**.

Actualizar las bases de datos de la aplicación

Los servidores de actualización específicos de Kaspersky son el origen principal de las actualizaciones de Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede usar los puertos de distribución, las carpetas locales u otros servidores web como un *origen de actualizaciones*.

Nota: Para descargar las actualizaciones de los servidores es necesario disponer de conexión a Internet.

De forma predeterminada, Kaspersky Endpoint Security comprueba periódicamente la existencia de actualizaciones en los servidores de actualización de Kaspersky. Si existen actualizaciones nuevas en un servidor, Kaspersky Endpoint Security las descarga en segundo plano y las instala en su equipo.

Iniciar manualmente una actualización de Kaspersky Endpoint Security

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Actualizar**.
   Se abre la ventana **Actualizar**.
2. Haga clic en **Actualizar**.

La aplicación comprobará si hay actualizaciones. Si las actualizaciones están disponibles, la aplicación las descarga e instala en su equipo.

También puede iniciar una tarea de actualización mediante una de las siguientes formas:

- Haga clic en el icono de la aplicación y elija **Actualizar**.
- En la barra de menús, elija **Protección** > **Actualizar**.

Puede cambiar la forma en que Kaspersky Endpoint Security actualiza las bases de datos de la aplicación. De forma predeterminada, la aplicación actualiza las bases de datos automáticamente.

Activar/desactivar las descargas automáticas de las actualizaciones de bases de datos de Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la sección **Actualizar** de la pestaña **Bases de datos**, marque o desmarque la casilla **Descargar actualizaciones automáticamente**.

Puede ver los resultados de las tareas de actualización realizadas en la ventana **Informes**.

Nota: La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y las actualizaciones de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Procedimiento si el acceso a un archivo está bloqueado

Expandir todo | Contraer todo

La aplicación Kaspersky Endpoint Security bloquea el acceso a archivos y aplicaciones infectados. Si un archivo está infectado, debe desinfectarse antes de poder acceder a él.

Desinfectar un objeto detectado

1. En la barra de menús, elija **Protección** > **Objetos detectados**.

Se abre la ventana **Objetos detectados**.

2. En la sección **Objetos detectados**, haga clic en ••• al lado del archivo requerido y elija **Desinfectar**.

   La aplicación inicia la desinfección del objeto seleccionado. Mientras la desinfección esté en curso, la aplicación muestra un cuadro de diálogo en el que puede elegir la acción que llevar a cabo con el objeto.

Desinfectar todos los objetos detectados

1. En la barra de menús, elija **Protección** > **Objetos detectados**.

   Se abre la ventana **Objetos detectados**.

2. En la sección **Objetos detectados**, haga clic en **Desinfectar todo**.

   La aplicación inicia la desinfección de los objetos detectados. Mientras la desinfección esté en curso, la aplicación muestra una ventana de notificación en la que puede elegir la acción que llevar a cabo con el objeto. Si selecciona la casilla de verificación **Aplicar a todo** en la ventana de notificación al elegir una acción, la aplicación realizará la misma acción con todos los archivos de este tipo.

Si sabe con seguridad que los archivos que el componente Protección frente a amenazas en archivos está bloqueando son seguros, puede incluirlos en una zona de confianza.

Restauración de un archivo que la aplicación ha eliminado o desinfectado

En ocasiones no es posible guardar archivos enteros durante el proceso de desinfección. Si un archivo desinfectado contenía información importante a la que no se puede acceder total o parcialmente después de la desinfección, puede intentar restaurar el archivo original a partir de la copia de seguridad.

Restaurar un archivo que la aplicación ha eliminado o modificado durante la desinfección

1. En la barra de menús, elija **Protección** > **Objetos detectados**.

   Se abre la ventana **Objetos detectados**.

2. En la sección **Copia de seguridad**, haga clic en ••• al lado del archivo que quiere restaurar.

   El menú emergente se abre.

3. Elija **Restaurar archivo**.

   Se abre una ventana en la que tiene que especificar el nombre de archivo, la etiqueta y la carpeta en la que el archivo será restaurado. De forma predeterminada, el nombre de archivo original y la ubicación ya están especificados.

4. Especificar el nombre de archivo y la carpeta en la que el archivo será restaurado.

5. Haga clic en **Guardar**.

La aplicación restaura el archivo a la ubicación especificada con el nombre especificado.

Tiene que analizar el archivo en busca de software malicioso inmediatamente después de restaurarlo. Es posible que el objeto pueda desinfectarse mediante las bases de datos actualizadas sin dañarse.

Importante: Recomendamos que no restaure copias de seguridad de archivos a menos que sea absolutamente necesario, porque podría causar una infección del equipo.

Visualización del informe acerca del funcionamiento de una aplicación

Puede consultar el informe de Kaspersky Endpoint Security en el que se muestran todos los objetos detectados en la pestaña **Objetos procesados**. Los eventos del sistema se muestran en la pestaña **Eventos del sistema**. Además, se crea un informe detallado separado para cada uno de los siguientes componentes de la aplicación: Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en la red, Detección de comportamiento y análisis y tareas de actualización.

Abrir la ventana Informes

En la barra de menús, elija **Protección** > **Informes**.

Pasos que deben seguirse si aparecen ventanas de notificaciones

Las notificaciones de la aplicación, que se muestran como ventanas de notificación, le informan de eventos de aplicación que requieren su atención.

Si este tipo de notificación aparece en la pantalla, seleccione una de las opciones que se sugieren. La mejor opción es la que los expertos de Kaspersky establecen como predeterminada.

Configuración avanzada de la aplicación

Cobertura de la protección del equipo

Los objetos que detecta Kaspersky Endpoint Security se dividen en categorías en función de diversos atributos. La aplicación siempre realiza búsquedas de virus, gusanos, troyanos y herramientas maliciosas. Estos programas pueden causar daños significativos al equipo. Para garantizar una protección más fiable del equipo, puede ampliar la lista de objetos que se deben detectar permitiendo a la aplicación que compruebe el software legítimo que un intruso podría aprovechar para dañar su equipo o datos personales.

Kaspersky Endpoint Security protege contra los siguientes grupos de objetos:

- **Virus, gusanos, programas troyanos, herramientas maliciosas, software publicitario y automarcadores**.

  Esta categoría incluye:

  - Todos los tipos de software malicioso.
  - Software que puede molestarle al mostrar anuncios (como banners) en su equipo o al sustituir los resultados de búsqueda de su navegador por sitios web de publicidad.
  - Aplicaciones que establecen conexiones telefónicas ocultas mediante un módem.

  La protección contra cualquier tipo de software malicioso asegura el mínimo nivel de seguridad requerido. De acuerdo con las recomendaciones de los expertos de Kaspersky, Kaspersky Endpoint Security siempre supervisa los objetos que pertenecen a esta categoría.

- **Los intrusos pueden utilizar software legítimo para dañar su equipo o sus datos personales**. En esta categoría se incluye el software legítimo que los intrusos pueden utilizar para dañar su equipo o sus datos personales, como las aplicaciones de administración remota.

Selección de las categorías de objetos que se deben detectar

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Amenazas**, en la sección **Objetos a detectar**, seleccione las casillas que se encuentran junto a las categorías de objetos que se deben detectar.

   Nota: Kaspersky Endpoint Security siempre protege su equipo de virus, gusanos, programas troyanos, herramientas maliciosas, software publicitario y automarcadores. Por tanto, no se puede borrar la marca de selección de la casilla de verificación de esta categoría.

Según las categorías seleccionadas de objetos que se deben detectar, Kaspersky Endpoint Security utilizará algunas o todas sus bases de datos antimalware cuando se ejecuten Protección frente a amenazas en archivos, Protección frente a amenazas web y tareas de análisis.

Nota: Si Kaspersky Endpoint Security clasifica una aplicación como software malicioso, pero usted cree que es segura, puede agregarla a la Zona de confianza.

La *Zona de confianza* es una lista de objetos que Kaspersky Endpoint Security no analiza ni supervisa. Puede que necesite agregar objetos a la Zona de confianza si, por ejemplo, Kaspersky Endpoint Security bloquea el acceso a un objeto, una aplicación o un sitio web, aunque usted esté totalmente seguro de que dichos objetos, aplicaciones o direcciones web sean inocuos.

Al agregar una aplicación a la zona de confianza, dejarán de supervisarse sus actividades en los archivos y la red (incluidas las sospechosas). Sin embargo, Kaspersky Endpoint Security continúa analizando el archivo ejecutable y el proceso de la aplicación de confianza.

Nota: Cuando un administrador configura la directiva para prohibir la edición de la Zona de confianza, los usuarios no pueden acceder a los ajustes de la Zona de confianza.

Agregue/elimine un archivo o carpeta en/de la lista de archivos y carpetas de confianza

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Amenazas**, en la sección **Exclusiones**, haga clic en **Zona de confianza**.
   Se abre la ventana de configuración de Zona de confianza.
3. En la pestaña **Archivos y carpetas**, modifique la lista de archivos y carpetas de confianza:
   - Para agregar un archivo o carpeta a la lista:
     a. Haga clic en +.
     Se abre un cuadro de diálogo donde puede seleccionar un archivo o una carpeta.
     b. Seleccione el archivo o la carpeta que desee agregar.
     c. Haga clic en **Abrir**.
   - Para eliminar un archivo o una carpeta de la lista:
     a. Seleccione un archivo o carpeta que desee eliminar de la lista de carpetas y archivos de confianza.
     b. Haga clic en −.
4. Haga clic en **Aceptar**.

Añada/elimine una dirección web de confianza a/de la lista de direcciones web de confianza

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Amenazas**, en la sección **Exclusiones**, haga clic en **Zona de confianza**.
   Se abre la ventana de configuración de Zona de confianza.
   También puede abrir esta ventana si hace clic en el botón **Zona de confianza** en la sección **General** de la pestaña **Protección**.
3. En la pestaña **Direcciones web**, edite la lista de direcciones web de confianza:
   - Para agregar una dirección web a la lista:
     a. Haga clic en +.
     b. Introduzca la dirección web que desea agregar a la lista.
     c. Haga clic en **Aceptar**.
   - Para eliminar una dirección web de la lista:
     a. Seleccione una dirección web que quiera eliminar.
     b. Haga clic en −.
4. Haga clic en **Aceptar**.

Por defecto, la lista de direcciones web de confianza está vacía.

Añadir una aplicación de confianza a la lista de aplicaciones de confianza o eliminar una desde ella

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Amenazas**, en la sección **Exclusiones**, haga clic en **Zona de confianza**.
   Se abre la ventana de configuración de Zona de confianza.
   También puede abrir esta ventana si hace clic en el botón **Zona de confianza** en la sección **General** de la pestaña **Protección**.
3. En la pestaña **Aplicaciones de confianza**, edite la lista de aplicaciones de confianza:
   - Para añadir una aplicación a la lista, siga estos pasos:

a. Haga clic en +.

Se abre una ventana donde puede especificar los parámetros de la aplicación requerida.

b. Especifique los siguientes parámetros de la aplicación que desea añadir:

- **Ruta**
- **Requisito de firma de código**

> **Nota:** Puede introducir los valores de estos dos parámetros manualmente o hacer clic en el botón **Seleccionar** y seleccionar la aplicación que desea añadir en la ventana que se abre. En este caso, los valores de estos parámetros se insertan automáticamente.

c. En la sección **Opciones**, seleccione al menos un tipo de actividad que no desea que la aplicación Kaspersky Endpoint Security supervise:

- **No supervisar la actividad de archivos**
- **No supervisar la actividad de red**

d. Haga clic en **Aceptar**.

- Para eliminar una aplicación de la lista, siga estos pasos:

a. Seleccione la aplicación que desea eliminar.

b. Haga clic en −.

De forma predeterminada, la lista de aplicaciones de confianza está vacía.

Editar una aplicación de confianza

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Amenazas**, en la sección **Exclusiones**, haga clic en **Zona de confianza**.
   Se abre la ventana de configuración de Zona de confianza.
   También puede abrir esta ventana si hace clic en el botón **Zona de confianza** en la sección **General** de la pestaña **Protección**.
3. En la pestaña **Aplicaciones de confianza**, seleccione la aplicación que desee editar.
4. Haga clic en **Editar**.
5. Edite los parámetros de la aplicación en la ventana que se abre:
6. Haga clic en **Aceptar**.

Habilite la supervisión de una dirección web de confianza.

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Amenazas**, en la sección **Exclusiones**, haga clic en **Zona de confianza**.
   Se abre la ventana de configuración de Zona de confianza.
3. En la pestaña **Direcciones web**, desactive la casilla situada junto a una dirección web que desee que la aplicación Kaspersky Endpoint Security supervise.
4. Haga clic en **Aceptar**.

Protección frente a amenazas en archivos

El componente Protección frente a amenazas en archivos impide que se infecte el sistema de archivos del equipo. El componente se ejecuta durante el inicio del sistema operativo, permanece en la memoria del equipo y analiza todos los archivos que se abren, guardan o ejecutan en su equipo y en todos los discos conectados a este en busca de software malicioso. Si desactiva el componente Protección frente a amenazas en archivos, no se iniciará al iniciarse el sistema operativo. Tendrá que volver a activar el componente Protección frente a amenazas en archivos manualmente.

Activar/desactivar el componente Protección frente a amenazas en archivos

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en archivos**, active/desactive la casilla **Activar Protección frente a amenazas en archivos**.

   También puede activar el componente Protección frente a amenazas en archivos en Centro de protección. La desactivación de la protección del equipo o de componentes de protección pone a su equipo en un riesgo mucho mayor de infección. Por eso, el Centro de protección le informa cuando la protección está desactivada.

Puede crear una cobertura de protección para el componente Protección frente a amenazas en archivos.

Agregue/elimine un archivo o carpeta en/de la cobertura de protección

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en archivos**, haga clic en **Cobertura de protección**.

   Se abre una ventana con una lista de objetos que analizará el componente Protección frente a amenazas en archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza todos los objetos ubicados en los discos internos, extraíbles y de red conectados al equipo.

   Nota: Puede omitir el análisis del volumen de sistema de solo lectura para reducir considerablemente el tiempo de análisis. De forma predeterminada, la Protección frente a amenazas en archivos no analiza el volumen de sistema de solo lectura.

3. En la sección **Cobertura de protección**, añada los objetos a la Cobertura de protección o elimínelos de ella:

   - Para agregar un archivo o una carpeta a la cobertura de la protección:

     a. Haga clic en +.

     Se abre un menú emergente donde puede seleccionar objetos para agregar a la cobertura de protección.

     b. En este menú, seleccione el elemento **Archivos y carpetas**.

     Se abre un cuadro de diálogo donde puede seleccionar un archivo o una carpeta.

     c. Seleccione el archivo o la carpeta que quiera agregar a la cobertura de protección.

     d. Haga clic en **Abrir**.

   - Para eliminar un archivo o carpeta de la cobertura de protección:

     a. Seleccione un objeto en la lista de objetos de la cobertura de protección.

     b. Arrastre el objeto seleccionado desde la ventana o haga clic en –.

4. Si desea analizar el volumen de sistema de solo lectura, en la sección **Optimización**, desactive la casilla **Omitir el análisis del volumen de sistema de solo lectura**.

   Importante: Es posible que la optimización esté desactivada por motivos de seguridad.

5. Haga clic en **Guardar**.

Agregar/eliminar un objeto en la lista de objetos predeterminados a la cobertura de protección o eliminarlos de ella

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en archivos**, haga clic en **Cobertura de protección**.

   Se abre una ventana con una lista de objetos que analizará el componente Protección frente a amenazas en archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza todos los objetos ubicados en los discos internos, extraíbles y de red conectados al equipo.

   Nota: Puede omitir el análisis del volumen de sistema de solo lectura para reducir considerablemente el tiempo de análisis. De forma predeterminada, la Protección frente a amenazas en archivos no analiza el volumen de sistema de solo lectura.

3. En la sección **Cobertura de protección**, añada objetos de la lista de objetos predeterminados a la Cobertura de protección, o elimínelos de ella:

   - Para agregar un objeto de la lista de objetos predeterminados a la cobertura de protección, siga estos pasos:

     a. Haga clic en +.

     Se abre un menú emergente donde puede seleccionar objetos para agregar a la cobertura de protección.

     b. En el menú desplegable, seleccione un objeto que quiera añadir a la cobertura de protección (por ejemplo, **Todos los discos internos**).

   - Para eliminar un objeto de la lista de objetos predeterminados de la cobertura de la protección, siga estos pasos:

     a. Seleccione un objeto en la lista de objetos de la cobertura de protección.

     b. Arrastre el objeto seleccionado desde la ventana o haga clic en −.

4. Si desea analizar el volumen de sistema de solo lectura, en la sección **Optimización**, desactive la casilla **Omitir el análisis del volumen de sistema de solo lectura**.

   Importante: Es posible que la optimización esté desactivada por motivos de seguridad.

5. Haga clic en **Guardar**.

Desactive la protección de un objeto en la cobertura de protección

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en archivos**, haga clic en **Cobertura de protección**.

   Se abre una ventana con una lista de objetos que analizará el componente Protección frente a amenazas en archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza todos los objetos ubicados en los discos internos, extraíbles y de red conectados al equipo.

   Nota: Puede omitir el análisis del volumen de sistema de solo lectura para reducir considerablemente el tiempo de análisis. De forma predeterminada, la Protección frente a amenazas en archivos no analiza el volumen de sistema de solo lectura.

3. Desmarque la casilla de verificación situada al lado de un objeto en la lista de objetos de la cobertura de protección.

4. Haga clic en **Guardar**.

Activar el análisis del volumen de sistema de solo lectura

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en archivos**, haga clic en **Cobertura de protección**.

   Se abre una ventana con una lista de objetos que analizará el componente Protección frente a amenazas en archivos. De forma predeterminada, el componente Protección frente a amenazas en archivos analiza todos los objetos ubicados en los discos internos, extraíbles y de red conectados al equipo.

Nota: Puede omitir el análisis del volumen de sistema de solo lectura para reducir considerablemente el tiempo de análisis. De forma predeterminada, la Protección frente a amenazas en archivos no analiza el volumen de sistema de solo lectura.

3. En la sección **Optimización**, desactive la casilla **Omitir el análisis del volumen de sistema de solo lectura**.

Importante: Es posible que la optimización esté desactivada por motivos de seguridad.

4. Haga clic en **Guardar**.

Cuando el usuario o una aplicación intentan acceder a un archivo incluido en la cobertura de protección, el componente Protección frente a amenazas en archivos comprueba si las bases de datos de iSwift contienen información sobre el archivo y usa esta información para decidir si analizarlo o no.

Es posible reconocer los objetos maliciosos gracias al *análisis de firmas*, un modo de búsqueda de amenazas basado en descripciones de amenazas incluidas en las bases de datos antimalware. Además del análisis de firmas, el componente Protección frente a amenazas en archivos utiliza el análisis heurístico y otras tecnologías de análisis.

Si se detecta una amenaza en un archivo, Kaspersky Endpoint Security identifica el tipo de software malicioso detectado (por ejemplo, *virus* o *programa troyano*). Después, la aplicación muestra una notificación sobre el objeto detectado y realiza una acción sobre el objeto sobre la base de la configuración de la Protección frente a amenazas en archivos.

Seleccione la acción que debe realizar el componente Protección frente a amenazas en archivos tras detectar un archivo infectado

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en archivos**, seleccione la acción que esta protección debe realizar después de descubrir un archivo infectado.

Antes de intentar desinfectar o eliminar un archivo, Kaspersky Endpoint Security crea una copia de seguridad para una posterior restauración o desinfección.

La información acerca del componente Protección frente a amenazas en archivos y de todos los objetos detectados se registra en un informe.

Nota: Si el componente Protección frente a amenazas en archivos deja de funcionar por un error, puede ver el informe e intentar iniciar el componente de nuevo. Si el problema no se soluciona, puede comunicarse con el Servicio de soporte técnico de Kaspersky.

Ver el informe de Protección frente a amenazas en archivos

1. En la barra de menús, elija **Protección** > **Informes**.
   Se abre la ventana **Informes**.
2. Abrir la pestaña **Amenazas en archivos**.

Protección frente a amenazas web

Cada vez que utiliza Internet, su equipo se expone a un riesgo de infección por software malicioso y a otro tipo de amenazas de seguridad informática. Las amenazas de seguridad de su equipo pueden introducirse en él al descargar programas gratuitos o visitar sitios web que hayan sufrido ataques de piratas. Además, los gusanos de red pueden atacar su equipo en cuanto este se conecta a Internet, antes incluso de que abra una dirección web o descargue un archivo.

Kaspersky Endpoint Security protege la información entrante y saliente de su equipo a través de los protocolos HTTP y HTTPS en Safari, Chrome o Firefox.

Nota: Kaspersky Endpoint Security supervisa el tráfico web en los puertos que más se utilizan para la transferencia de datos HTTP y HTTPS. Kaspersky Endpoint Security analiza las conexiones cifradas (HTTPS) solo si está seleccionada la casilla de verificación **Comprobar conexiones seguras (HTTPS)** en la sección **General**.

Activar o desactivar el componente Protección frente a amenazas web

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas web**, active/desactive la casilla **Activar Protección frente a amenazas web**.

También puede activar el componente Protección frente a amenazas web en Centro de protección. La desactivación de la protección del equipo o de componentes de protección pone a su equipo en un riesgo mucho mayor de infección. Por eso, el Centro de protección le informa cuando la protección está desactivada.

Importante: Si ha desactivado el componente Protección frente a amenazas web, este no volverá a activarse automáticamente cuando se reinicie Kaspersky Endpoint Security o el sistema operativo. Deberá volver a activarla de forma manual.

La Protección frente a amenazas web analiza el tráfico web sobre la base de la configuración recomendada por Kaspersky. Los objetos maliciosos se reconocen mediante los análisis de firmas, el análisis heurístico y los datos de Kaspersky Security Network.

La comprobación de los vínculos de los sitios web en busca de direcciones web phishing y maliciosas permite impedir los *ataques phishing*. Los *ataques de phishing* suelen realizarse mediante mensajes de correo electrónico enviados por delincuentes que se hacen pasar por instituciones financieras (como bancos) y que envían vínculos a sitios web fraudulentos. En estos correos electrónicos, los criminales tratan de engañar al usuario para que visiten un sitio web phishing e introduzcan datos confidenciales (como su número de tarjeta bancaria o el nombre y contraseña para su cuenta bancaria en línea). Un intento de ataque phishing puede disfrazarse, por ejemplo, como un mensaje de su banco con un vínculo a su sitio web oficial, pero, en realidad, el enlace lleva a una copia exacta del sitio web oficial del banco creada por impostores.

Protección frente a amenazas web supervisa su tráfico web en busca de intentos de visitar un sitio web phishing y bloquea el acceso a esos sitios web. A fin de comprobar los enlaces de los sitios web en busca de direcciones web phishing y maliciosas, Kaspersky Endpoint Security utiliza las bases de datos de la aplicación, los análisis heurísticos y los datos de Kaspersky Security Network.

Algoritmo de análisis del tráfico web

Protección frente a amenazas web intercepta cada sitio web o archivo a los que accede usted o una aplicación a través de los protocolos HTTP y HTTPS, y los analiza en busca de código malicioso:

- Si un sitio web o un archivo contienen código malicioso, Kaspersky Endpoint Security puede bloquearlo y mostrar una notificación para informarle que el archivo solicitado o el sitio web están infectados.
- Si el archivo o el sitio web no contienen código malicioso, puede acceder a ellos de inmediato.

Seleccione la acción que realiza el componente Protección frente a amenazas web después de descubrir un objeto de tráfico web peligroso

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas web**, seleccione la acción que debe realizar el componente Protección frente a amenazas web después de descubrir un objeto de tráfico web peligroso.

La información acerca de Protección frente a amenazas web y de todos los objetos de tráfico web peligrosos detectados se registra en un informe.

Nota: Si el componente Protección frente a amenazas web deja de funcionar por un error, puede ver el informe e intentar reiniciar el componente. Si el problema no se soluciona, puede comunicarse con el Servicio de soporte técnico de Kaspersky.

Ver el informe de Protección frente a amenazas web

1. En la barra de menús, elija **Protección** > **Informes**.

   Se abre la ventana **Informes**.

2. Abra la pestaña **Amenazas web**.

Protección frente a amenazas en el correo

El componente Protección frente a amenazas en el correo analiza los archivos adjuntos de los mensajes de correo electrónico entrantes y salientes en busca de malware y otras amenazas. El componente proporciona protección al ordenador con la ayuda de bases de datos antimalware, el servicio en la nube de Kaspersky Security Network y el análisis heurístico.

La aplicación es compatible con los siguientes clientes de correo: Apple Mail, Microsoft Outlook, Mozilla Thunderbird, Canary Mail, Spark, Mimestream, Airmail, Post Box, Boxy Suite 2, Twobird, Shift, Clean Email, eM Client, Superhuman, Polymail, HEY, Mail+ para Gmail, Spike mail.

El componente Protección frente a amenazas en el correo está activado de manera predeterminada. Puede desactivar la Protección frente a amenazas en el correo si es necesario.

Activar/desactivar la Protección frente a amenazas en el correo mediante Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas básicas** > **Protección frente a amenazas en el correo**.
5. Active/desactive el interruptor de **Protección frente a amenazas en el correo**.
6. Si la Protección frente a amenazas en el correo está activada, elija la acción que realizará la aplicación cuando se detecte malware:
   - **Eliminar**
   - **Bloquear**
7. Si es necesario, en la sección **Configuración avanzada**, configure el límite de tiempo para analizar los archivos o el tamaño máximo del archivo para su análisis.
8. Guarde los cambios.

Activar/desactivar la Protección frente a amenazas en el correo mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, elija la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, elija **Protección frente a amenazas básica** > **Protección frente a amenazas en el correo**.
7. Active o desactive la selección de la casilla **Activar Protección frente a amenazas en el correo**.
8. En la sección **Acción al detectar una amenaza**, elija la acción que se realizará cuando Kaspersky Endpoint Security detecte una amenaza.
9. Si es necesario, en la sección **Configuración de Protección frente a amenazas en el correo**, configure el límite de tiempo para analizar los archivos o el tamaño máximo del archivo para su análisis.
10. Haga clic en **Aceptar** para guardar los cambios.
11. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
    - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
    - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.

Activar/desactivar la Protección frente a amenazas en el correo mediante la aplicación Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en el correo**, active/desactive la casilla **Activar Protección frente a amenazas en el correo**.

3. Si la casilla **Activar Protección frente a amenazas en el correo** está seleccionada, elija la acción que se realizará cuando Kaspersky Endpoint Security detecte una amenaza.

4. Si es necesario, configure el límite de tiempo para analizar los archivos o el tamaño máximo del archivo para su análisis.

Ver el informe de Protección frente a amenazas en el correo

1. En la barra de menús, elija **Protección** > **Informes**.

   Se abre la ventana **Informes**.

2. Abra la pestaña **Protección frente a amenazas en el correo**.

Protección frente a amenazas en la red

Kaspersky Endpoint Security protege su equipo frente a ataques de red.

Un *ataque de red* es un intento de irrumpir en el sistema operativo de un equipo remoto. Los delincuentes intentan llevar a cabo ataques de red para hacerse con el control del sistema operativo, provocar la denegación de servicio del sistema operativo o acceder a información confidencial. Para conseguir estos objetivos, los delincuentes llevan a cabo ataques directos, como el análisis de puertos y los ataques por fuerza bruta, o bien utilizan software malicioso instalado en el equipo atacado.

Los ataques de red se pueden dividir en los siguientes tipos:

- *Análisis de puertos*. Este tipo de ataque de red se realiza generalmente como preparación para un ataque de red más peligroso. Un intruso analiza los puertos UDP y TCP que utilizan los servicios de red del equipo de destino y determina la vulnerabilidad de los equipos objetivo ante otros tipos de ataques de red más peligrosos. El análisis de puertos también permite al intruso determinar el sistema operativo del equipo de destino y seleccionar los ataques de red más apropiados.

- *Ataques de denegación del servicio* o ataques de red que provocan la negación del servicio. Dichos ataques de red hacen que el sistema operativo de destino se vuelva inestable o totalmente inoperable.

  Existen los siguientes principales tipos de ataques DoS:

  - La transmisión de paquetes de red especialmente diseñados que el equipo de destino no se espera y que, por lo tanto, hacen que el sistema operativo de destino funcione mal o se bloquee.

  - El envío de un gran número de paquetes de red a un equipo remoto en un corto período. Todos los recursos del equipo de destino se usan para procesar los paquetes de red que envía el intruso. Como resultado, el equipo deja de realizar sus funciones.

- *Ataques de intrusión de red*. Esos ataques de red están diseñados para "secuestrar" el sistema operativo del equipo objetivo. Este es el tipo de ataque de red más peligroso porque, si sale bien, el intruso consigue un control total del sistema operativo.

  Este tipo de ataque de red se usa cuando el intruso quiere obtener datos confidenciales de un equipo remoto (como números de tarjetas bancarias o contraseñas) o utilizar secretamente el equipo remoto para sus propios fines (por ejemplo, para atacar otros equipos desde este equipo).

Activar o desactivar el componente Protección frente a amenazas en la red

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Protección** de la sección **Protección frente a amenazas en la red**, active/desactive la casilla de verificación **Activar Protección frente a amenazas en la red**.

También puede activar el componente Protección frente a amenazas en la red en Centro de protección. La desactivación de la protección del equipo o de componentes de protección pone a su equipo en un riesgo mucho mayor de infección. Por eso, el Centro de protección le informa cuando la protección está desactivada.

Importante: Si ha desactivado el componente Protección frente a amenazas en la red, no volverá a activarse automáticamente cuando Kaspersky Endpoint Security o el sistema operativo se vuelva a iniciar. Tiene que volver a activar el componente Protección frente a amenazas en la red manualmente.

Cuando la aplicación detecta actividad de red peligrosa, Kaspersky Endpoint Security agrega automáticamente la dirección IP del equipo atacante a la lista de equipos bloqueados, a menos que el equipo atacante esté en la lista de equipos de confianza.

Editar la lista de equipos bloqueados

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en la red**, seleccione la casilla de verificación **Activar Protección frente a amenazas en la red**.
3. Haga clic en **Ajustes**.
   Se abre una ventana con una lista de equipos de confianza y una lista de equipos bloqueados.
4. Abra la pestaña **Equipos bloqueados**.
5. Si está seguro de que el equipo bloqueado no es una amenaza, seleccione la dirección IP del equipo en la lista y haga clic en **Desbloquear**.
   Se abre un diálogo de confirmación.
6. En el cuadro de diálogo de confirmación, realice una de las siguientes acciones:
   - Si desea desbloquear el equipo, haga clic en **Desbloquear**.
     Kaspersky Endpoint Security desbloquea la dirección IP.
   - Si no quiere que Kaspersky Endpoint Security bloquee la dirección IP seleccionada en ningún momento, haga clic en **Desbloquear y excluir**.
     Kaspersky Endpoint Security desbloquea la dirección IP y la agrega a la lista de equipos de confianza.
7. Haga clic en **Guardar**.

Puede crear y editar una lista de equipos de confianza. La aplicación Kaspersky Endpoint Security no bloquea de manera automática las direcciones IP de estos equipos, ni siquiera cuando se detecta actividad de red peligrosa en estos.

Editar la lista de equipos de confianza

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Protección**, en la sección **Protección frente a amenazas en la red**, seleccione la casilla de verificación **Activar Protección frente a amenazas en la red**.
3. Haga clic en **Ajustes**.
   Se abre una ventana con una lista de equipos de confianza y una lista de equipos bloqueados.
4. Abra la pestaña **Equipos de confianza**.
5. Editar la lista de equipos de confianza:
   - Para agregar una dirección IP a la lista de equipos de confianza:
     a. Haga clic en +.
     b. En el campo que aparece, introduzca la dirección IP del equipo en el que confía.
   - Para eliminar una dirección IP de la lista de equipos de confianza:
     a. Seleccione una dirección IP de la lista.
     b. Haga clic en −.
   - Para editar una dirección IP en la lista de equipos de confianza:
     a. Seleccione una dirección IP de la lista.
     b. Haga clic en **Editar**.
     c. Cambie la dirección IP.

6. Haga clic en **Guardar**.

Cuando se detecta un ataque de red, Kaspersky Endpoint Security registra información sobre el ataque en un informe.

Nota: Si el componente Protección frente a amenazas en la red deja de funcionar cuando detecta un error, consulte el informe e intente reiniciar el componente. Si el problema no se soluciona, puede comunicarse con el Servicio de soporte técnico de Kaspersky.

Ver el informe de Protección frente a amenazas en la red

1. En la barra de menús, elija **Protección** > **Informes**.
   Se abre la ventana **Informes**.
2. Abra la pestaña **Protección frente a amenazas en la red**.

Firewall

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

Prioridades de regla de red

Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. Si la actividad de la red se añade a varias reglas, Firewall regula la actividad de la red de acuerdo con la regla con la mayor prioridad.

Tipos de conexión de red

Firewall le permite controlar la actividad de la red según el tipo de conexión de red. Puede cambiar el tipo de conexión de red en la configuración de Kaspersky Endpoint Security.

Están disponibles los siguientes tipos de conexión de red:

- **Red pública**. La red no está protegida por aplicaciones antimalware, firewalls ni filtros (como Wi-Fi en un café). Cuando el usuario opera un ordenador que está conectado a dicha red, Firewall bloquea el acceso a los archivos y las impresoras de este ordenador. Los usuarios externos tampoco pueden acceder a los datos a través de carpetas compartidas y acceso remoto al escritorio de este ordenador. Firewall asigna el tipo de red pública a Internet de manera predeterminada. No puede cambiar el tipo de Internet.
- **Red local**. Red para usuarios con acceso restringido a archivos e impresoras en este ordenador (por ejemplo, para una LAN corporativa o una red doméstica).
- **Red de confianza**. Red segura en la que el ordenador no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de las redes con este estado.

Administrar el componente Firewall en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, elija la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, elija **Protección frente a amenazas básica** > **Firewall**.
7. Active o desactive la selección de la casilla **Activar Firewall**.
8. En la sección **Configuración del Firewall**, haga clic en el botón **Ajustes** y añada, edite o elimine reglas, o cambie su prioridad.
9. En la sección **Redes disponibles**, haga clic en el botón **Ajustes** y añada, edite, elimine o cambie el tipo de redes.
10. Haga clic en **Aceptar** para guardar los cambios.

11. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
    - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
    - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.

Administrar el componente Firewall en Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas básicas** > **Firewall**.
5. Active/desactive el interruptor **Firewall**.
6. En la sección **Configuración del Firewall**, haga clic en el **Reglas de paquetes de red** y añada, edite o elimine reglas, o cambie su prioridad.
7. En la sección **Redes disponibles**, haga clic en el **Configuración de red** y añada, edite o cambie el tipo de redes.
8. Guarde los cambios.

Administrar el componente Firewall en la aplicación de Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Protección**, en la sección **Firewall**, active o desactive la selección de la casilla **Activar Firewall**.
3. En caso de ser necesario, haga clic en el botón **Ajustes** y configure los ajustes de Firewall:
    - En la pestaña **Reglas de paquete de red**, puede añadir, editar o eliminar reglas, o cambiar su prioridad.
    - En la pestaña **Redes disponibles**, puede añadir, editar o cambiar el tipo de redes.

Como resultado, si Firewall está activado, Kaspersky Endpoint Security controla la actividad de la red y bloquea las conexiones de red no autorizadas al ordenador.

Ver el informe de Firewall

1. En la barra de menús, elija **Protección** > **Informes**.
   Se abre la ventana **Informes**.
2. Abra la pestaña **Firewall**.

Detección de comportamiento

El componente Detección de comportamiento recibe datos sobre las acciones de las aplicaciones en su ordenador y proporciona esta información a otros componentes de protección para mejorar su rendimiento. El componente Detección de comportamiento utiliza las firmas de flujo de comportamiento (BSS) de las aplicaciones. Si la actividad de una aplicación coincide con una firma de flujo de comportamiento, Kaspersky Endpoint Security realiza la acción de respuesta seleccionada. La funcionalidad de Kaspersky Endpoint Security basada en firmas de flujo de comportamiento proporciona una defensa proactiva para el ordenador.

De forma predeterminada, la Detección de comportamiento está activada y se ejecuta en el modo recomendado por los expertos de Kaspersky. Puede desactivar la Detección de comportamiento si es necesario.

Activar/desactivar la Detección de comportamiento mediante Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.

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

   Se abre la ventana de propiedades de la directiva.

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

4. Vaya a **Protección frente a amenazas avanzadas** > **Detección de comportamiento**.

5. Active/desactive el interruptor de **Detección de comportamiento**.

6. Si la Detección de comportamiento está activada, seleccione una de las siguientes acciones que se realizarán cuando se detecte actividad de software malicioso:

   - **Bloquear**

     Si se selecciona esta opción, Kaspersky Endpoint Security cierra la aplicación al detectar actividad maliciosa.

   - **Eliminar**

     Si se selecciona esta opción, cuando se detecta actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de una aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.

   - **Preguntar al usuario**

     Si se selecciona esta opción, cuando se detecta actividad de malware, la aplicación Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el objeto malicioso y solicita al usuario que elija la acción que debe realizar la aplicación Kaspersky Endpoint Security. Las acciones disponibles pueden variar en función del estado del objeto.

7. Si la detección de comportamiento y la protección de carpetas compartidas contra el cifrado externo están activadas, seleccione una de las siguientes acciones que se realizarán al detectar un cifrado externo:

   - **Informar**

     Si se selecciona esta opción, al detectar un intento de modificar archivos en carpetas compartidas, Kaspersky Endpoint Security añade información sobre este intento a la lista de amenazas activas, añade una entrada a los informes de la aplicación local y envía información sobre la actividad maliciosa detectada a Kaspersky Security Center.

   - **Bloquear dispositivo atacante para**

     Si se selecciona esta opción, cuando la aplicación Kaspersky Endpoint Security detecta un intento de modificar archivos en carpetas compartidas, bloquea el acceso a la modificación del archivo (solo lectura) para la sesión que inició la actividad maliciosa y crea copias de seguridad de los archivos modificados.

8. Guarde los cambios.

Activar/desactivar la Detección de comportamiento mediante la Consola de administración

1. Inicie la Consola de administración.

2. Maximice el nodo **Servidor de administración <nombre del servidor>**.

3. En el árbol de la consola, haga clic en **Dispositivos administrados**.

4. En el espacio de trabajo, seleccione la pestaña **Directivas**.

5. Haga clic derecho en la directiva que desea configurar y seleccione **Propiedades**.

6. En la ventana **Propiedades**, seleccione **Protección frente a amenazas avanzada** > **Detección de comportamiento**

7. Seleccione o anule la selección de la casilla **Detección de comportamiento**.

8. Si es necesario, en la sección **Acción al detectar actividad de software malicioso**, seleccione la acción que se realizará cuando se detecte actividad de malware.

9. Haga clic en **Aceptar** para guardar los cambios.

10. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:

- Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
- Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** tras guardar los cambios.

Activar/desactivar la Detección de comportamiento mediante la aplicación Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Avanzado**, en la sección **Detección de comportamiento**, seleccione o anule la selección de la casilla Activar Detección de comportamiento.

3. Si la casilla Activar Detección de comportamiento está seleccionada, seleccione una de las siguientes acciones que se realizarán cuando se detecte actividad de software malicioso:

   - Bloquear

     Si se selecciona esta opción, Kaspersky Endpoint Security cierra la aplicación al detectar actividad maliciosa.

   - Eliminar

     Si se selecciona esta opción, cuando se detecta actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de una aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.

   - Preguntar al usuario

     Si se selecciona esta opción, cuando se detecta actividad de malware, la aplicación Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el objeto malicioso y solicita al usuario que elija la acción que debe realizar la aplicación Kaspersky Endpoint Security. Las acciones disponibles pueden variar en función del estado del objeto.

Como resultado, si la Detección de comportamiento está activada, Kaspersky Endpoint Security utiliza firmas de flujo de comportamiento para analizar la actividad de las aplicaciones en el sistema operativo.

Importante: No recomendamos desactivar la Detección de comportamiento a menos que sea absolutamente necesario, ya que al hacerlo se reducirá la eficacia de los componentes de protección. Para detectar amenazas, los componentes de protección pueden solicitar datos recopilados por el componente Detección de comportamiento.

Análisis

Protección frente a amenazas en archivos y Protección frente a amenazas web proporcionan protección en tiempo real para el equipo, aunque también le recomendamos que analice su equipo con regularidad en busca de software malicioso y otras amenazas a la seguridad del equipo. Estos análisis son necesarios para evitar la propagación de software malicioso no detectado por los componentes de la protección.

Kaspersky Endpoint Security contiene las siguientes tareas integradas de análisis:

- **Análisis completo**.

  Un análisis de software malicioso de la memoria del equipo, de los objetos de inicio y de todos los discos internos del equipo.

- **Análisis rápido**.

  Un análisis de software malicioso solamente de áreas críticas del equipo: memoria, objetos de inicio y carpetas de sistema.

- **Análisis personalizado**.

  Análisis de software malicioso de un objeto específico (archivo, carpeta, disco interno o extraíble).

- **Análisis de discos externos**

  Un análisis de software malicioso de los discos externos que se realiza al conectar un disco externo al ordenador.

Cuando la aplicación realiza una tarea de análisis, los objetos maliciosos se reconocen mediante el análisis de firmas. Además del análisis de firmas, Kaspersky Endpoint Security utiliza el análisis heurístico y otras tecnologías de análisis.

La ventana **Análisis** muestra información sobre el progreso de cada tarea de análisis en ejecución (porcentaje completado y tiempo restante), así como el historial de análisis (las 100 tareas de análisis más recientes).

Iniciar las tareas de Análisis Completo y Análisis Rápido

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.
   Se abre la ventana **Análisis**.
2. En la ventana **Análisis**, haga clic en el botón **Análisis completo** o **Análisis rápido**.

La tarea de análisis comienza.

Iniciar una tarea de Análisis personalizado

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.
   Se abre la ventana **Análisis**.
2. Para iniciar la tarea de **Análisis personalizado**, realice una de las siguientes opciones:
   - Agregue un archivo o una carpeta en la ventana.
   - Haga clic en **Seleccionar** y abra un archivo o carpeta.

La tarea de análisis comienza.

Detener una tarea de análisis

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.
   Se abre la ventana **Análisis**.
2. En la ventana **Análisis**, haga clic en el botón ( ) al lado de la tarea de análisis que desea detener.
   Se abre un diálogo de confirmación.
3. En el cuadro de diálogo de confirmación, haga clic en **Detener**.

La tarea de análisis se detiene.

Puede planificar la tarea de Análisis completo o Análisis rápido.

Programar una tarea de análisis desde la ventana Análisis

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Análisis**.
   Se abre la ventana **Análisis**.
2. Haga clic en **Planificar análisis**.
   Se abre un cuadro de diálogo donde podrá definir el análisis.
3. Seleccione la casilla **Análisis completo** o **Análisis rápido**.
4. Especifique la frecuencia y hora de inicio del análisis.
5. Haga clic en **Aceptar**.

Planificar una tarea de análisis desde la ventana de Ajustes

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, haga clic en **Planificar**.
3. En la ventana que se abre, seleccione la casilla de verificación al lado del nombre de la tarea de análisis que desea iniciar en una programación.

4. Configure la hora y la frecuencia de la tarea de análisis.
5. Haga clic en **Aceptar** para guardar los cambios realizados en la programación de tareas de análisis.

Cuando se conecta un disco externo al ordenador, la aplicación de Kaspersky Endpoint Security puede comenzar a analizar el disco automáticamente, preguntar si se desea analizar o no realizar ninguna acción. Puede seleccionar una de las opciones en los ajustes de la tarea Análisis de discos externos.

Seleccionar la acción que desea que realice la aplicación de Kaspersky Endpoint Security cuando se conecta un disco externo al ordenador

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, seleccione **Análisis de discos externos** en la lista de la izquierda.
3. En la sección **Cuando un disco externo se conecta**, seleccione la acción que desea que Kaspersky Endpoint Security realice cuando se conecta un disco externo.

Las tareas Análisis completo y Análisis rápido ya incluyen coberturas de análisis. Al realizar la tarea de Análisis completo, la aplicación Kaspersky Endpoint Security analiza la memoria del equipo, los objetos de inicio y todos los discos internos. Al realizar la tarea de Análisis rápido, la aplicación analiza la memoria del equipo, los objetos de inicio y las carpetas del sistema. Puede cambiar la cobertura del análisis para la tarea de Análisis rápido.

Nota: Puede omitir el análisis del volumen de sistema de solo lectura para reducir considerablemente el tiempo de análisis. De forma predeterminada, Kaspersky Endpoint Security no analiza el volumen de sistema de solo lectura cuando realiza una tarea de Análisis rápido, pero sí cuando realiza una tarea de Análisis completo.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Activar o desactivar el análisis del volumen de sistema de solo lectura

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, seleccione la tarea de **Análisis completo** o **Análisis rápido** en la lista de la izquierda.
3. En la sección **Optimización**, active o desactive la casilla **Omitir el análisis del volumen de sistema de solo lectura**.

   Importante: Es posible que la optimización esté desactivada por motivos de seguridad.

Agregar un archivo o carpeta a la cobertura del análisis para la tarea de Análisis rápido o eliminarlos de dicha cobertura

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, seleccione la tarea de **Análisis rápido** en la lista de la izquierda.
3. En la sección **Cobertura del análisis**, haga clic en **Editar**.
   Se abre una ventana con la lista de objetos incluidos en la cobertura del análisis de la tarea de análisis rápido.
4. Edite la lista de objetos de la cobertura del análisis:
   - Para agregar un archivo o carpeta a la cobertura del análisis para la tarea de Análisis rápido:
     a. Haga clic en **+**.
        Aparece un menú emergente donde puede seleccionar objetos para agregar a la cobertura del análisis.
     b. Elija el elemento **Archivos y carpetas**.

Se abre un cuadro de diálogo donde puede seleccionar un archivo o una carpeta.

c. Seleccione un archivo o carpeta que quiera agregar a la cobertura del análisis para la tarea de Análisis rápido.

d. Haga clic en **Abrir**.

- Para eliminar un archivo o carpeta de la cobertura del análisis para la tarea de Análisis rápido:

a. Seleccione un objeto que desee eliminar.

b. Arrastre el objeto seleccionado desde la ventana o haga clic en −.

5. Haga clic en **Guardar**.

Agregar un objeto de la lista predeterminada de Análisis rápido a la cobertura del análisis para la tarea de Análisis rápido

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, seleccione la tarea de **Análisis rápido** en la lista de la izquierda.
3. En la sección **Cobertura del análisis**, haga clic en **Editar**.
   Se abre una ventana con la lista de objetos incluidos en la cobertura del análisis.
4. Haga clic en +.
   Aparece un menú emergente donde puede seleccionar objetos para agregar a la cobertura del análisis.
5. En el menú emergente, seleccione un objeto que quiera agregar a la cobertura del análisis (por ejemplo, **Memoria**).
6. Haga clic en **Aceptar**.

Desactive la protección de un objeto en la cobertura del análisis para la tarea de Análisis rápido

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, seleccione la tarea de **Análisis rápido** en la lista de la izquierda.
3. En la sección **Cobertura del análisis**, haga clic en **Editar**.
   Se abre una ventana con la lista de objetos de la cobertura del análisis.
4. Desmarque la casilla de verificación situada al lado del objeto en la lista de objetos de la cobertura del análisis.
5. Haga clic en **Aceptar**.

Si se detecta una amenaza en un archivo, la aplicación muestra una notificación y realiza la acción especificada sobre el objeto. Puede cambiar la acción que se debe realizar al detectar un objeto.

Seleccione la acción que Kaspersky Endpoint Security debe ejecutar al detectar archivos infectados

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Análisis**, seleccione una tarea en la lista de la tarea.
3. En la sección **Acción**, seleccione la acción que realiza la aplicación después de detectar los archivos infectados.

Antes de desinfectar o eliminar un archivo infectado, Kaspersky Endpoint Security guarda una copia de este en el Depósito de copias de seguridad para que pueda restaurar el archivo original si fuera necesario.

La información de los resultados de las tareas de análisis y de todos los objetos detectados se registra en un informe.

Nota: Si se producen errores durante la ejecución de una tarea de análisis de software malicioso, reinicie la tarea. Si el nuevo intento de ejecutar el análisis también devuelve un error, póngase en contacto con el Servicio de soporte técnico de Kaspersky.

Ver el informe de las tareas de análisis

1. En la barra de menús, elija **Protección** > **Informes**.
   Se abre la ventana **Informes**.
2. Abra la pestaña **Análisis**.

Tareas de actualización

Actualizar en el momento adecuado las bases de datos de la aplicación asegura la protección continua del equipo. Protección frente a amenazas en archivos, Protección frente a amenazas web y las tareas de análisis utilizan bases de datos de la aplicación para detectar y neutralizar software malicioso en el equipo. Las bases de datos de la aplicación se actualizan regularmente con diferentes tipos de amenazas y sus correspondientes formas de neutralizarlas, por lo que es importante actualizarlas con regularidad.

Kaspersky Endpoint Security descarga bases de datos y módulos nuevos de la aplicación de los servidores de actualización de Kaspersky y los instala en el equipo. Kaspersky Endpoint Security también puede usar los puntos de distribución, las carpetas locales u otros servidores web.

Nota: Es necesario tener acceso a Internet para que su equipo se pueda conectar a los servidores de actualización y descargar las actualizaciones. Si se conecta a Internet a través de un servidor proxy, es posible que tenga que establecer la configuración de red.

Puede descargar actualizaciones de bases de datos de aplicaciones de una de estas maneras:

- **Automático**. Kaspersky Endpoint Security comprueba regularmente la existencia de actualizaciones en los servidores de actualización de Kaspersky. Si hay una nueva actualización disponible en el servidor de actualización, Kaspersky Endpoint Security la descarga en segundo plano y la instala en su equipo. Esta opción está habilitada de forma predeterminada.
- **Manual**. Puede comprobar manualmente las actualizaciones de Kaspersky Endpoint Security en cualquier momento.

Activar/desactivar las descargas automáticas de las actualizaciones de bases de datos de Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la sección **Actualizar** de la pestaña **Bases de datos**, marque o desmarque la casilla **Descargar actualizaciones automáticamente**.

Comprobar actualizaciones de la base de datos de Kaspersky Endpoint Security

1. En la barra lateral de la ventana principal de la aplicación, haga clic en **Actualizar**.
   Se abre la ventana **Actualizar**.
2. Haga clic en **Actualizar**.

La aplicación comienza a actualizar las bases de datos.

También puede iniciar una tarea de actualización mediante una de las siguientes formas:

- Haga clic en el icono de la aplicación y elija **Actualizar**.
- En la barra de menús, elija **Protección** > **Actualizar**.

Durante una actualización, las bases de datos y los módulos de la aplicación se comparan con los que están disponibles en los servidores de actualización. Si el equipo cuenta con la versión más reciente de las bases de datos, la ventana **Actualizar** mostrará un mensaje para informarle de que las bases de datos de la aplicación están actualizadas. Si la versión y las bases de datos de la aplicación difieren de las que están disponibles actualmente en los servidores de actualizaciones, solo se descargarán e instalarán en su equipo los componentes de la actualización que falten. Las actualizaciones incrementales de las bases de datos de la aplicación tardan menos tiempo y requieren menos tráfico web.

Si se conecta a Internet a través de un servidor proxy, puede establecer la configuración de conexión del servidor proxy. Kaspersky Endpoint Security utiliza esta configuración para actualizar las bases de datos de las aplicaciones y descargar las actualizaciones de los módulos de las aplicaciones.

Configurar una conexión a un servidor proxy

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. Seleccione la pestaña **Actualizar**.
3. En la sección **Proxy**, seleccione la casilla **Utilizar servidor proxy** y haga clic en **Ajustes**.
   Se abre una ventana en la que puede establecer la configuración de conexión del servidor proxy.
4. Configuración de la conexión a un servidor proxy.
5. Haga clic en **Guardar** para guardar los cambios realizados en la configuración de conexión del servidor proxy.

Antes de actualizar las bases de datos de la aplicación, Kaspersky Endpoint Security crea copias de seguridad de ellas para que pueda realizarse una operación de deshacer, si fuera necesario. La función deshacer resulta útil en caso de que una nueva versión de las bases de datos de la aplicación contenga una firma incorrecta que provoque que Kaspersky Endpoint Security bloquee una aplicación segura.

Nota: Si las bases de datos de Kaspersky Endpoint Security se dañan, se recomienda iniciar una actualización para descargar e instalar la versión más reciente de las bases de datos de la aplicación.

Anular la última actualización

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. Seleccione la pestaña **Actualizar**.
3. En la sección **Deshacer**, haga clic en **Deshacer actualización**.

Kaspersky Endpoint Security proporciona un informe detallado de los resultados de las tareas de actualización en la ventana **Informes**.

Ver un informe de tareas de actualización

1. En la barra de menús, elija **Protección** > **Informes**.
2. Se abre la ventana **Informes**.
3. Abra la pestaña **Actualización**.

Nota: La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y las actualizaciones de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Tareas locales

Tarea de análisis de discos externos

Kaspersky Endpoint Security puede analizar todos los archivos que ejecuta o copia, incluso si el archivo está ubicado en un disco externo. Para evitar la propagación de software malicioso, puede configurar análisis automáticos de los discos externos cuando están conectados al dispositivo.

Se puede establecer la siguiente configuración en Análisis de discos externos:

- La acción que realiza Kaspersky Endpoint Security cuando se conecta un disco externo.

  Análisis

  Si se selecciona esta opción, Kaspersky Endpoint Security inicia una tarea de análisis de software malicioso para el disco externo conectado.

Esta opción está seleccionada de forma predeterminada.

No hacer nada

Si se selecciona esta opción, Kaspersky Endpoint Security no analiza el disco externo que se conecta.

- **La acción que realiza Kaspersky Endpoint Security cuando detecta un objeto malicioso.**

  Desinfectar; eliminar si la desinfección falla

  Si se selecciona esta opción, Kaspersky Endpoint Security bloquea el acceso al objeto infectado e intenta desinfectarlo sin solicitar la confirmación del usuario.

  Si el objeto está desinfectado, Kaspersky Endpoint Security lo guarda en su ubicación original con el nombre del archivo original. Si la desinfección no funciona, Kaspersky Endpoint Security elimina los objetos infectados que no se pudieron desinfectar.

  Esta opción está seleccionada de forma predeterminada.

  Preguntar al usuario

  Si se selecciona esta opción, se muestra una ventana de notificación con información sobre el objeto malicioso y se le solicita al usuario que escoja la acción que Kaspersky Endpoint Security debe realizar. Las acciones disponibles pueden variar en función del estado del objeto.

Puede configurar el Análisis de discos externos en la Consola de administración, Web Console o en la aplicación Kaspersky Endpoint Security.

Cómo configurar el Análisis de discos externos en la Consola de administración (MMC)

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, seleccione la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y seleccione **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Tareas locales** > **Análisis de discos externos**.
7. Defina la configuración de la tarea.
8. Haga clic en **Aceptar** para guardar los cambios.

Cómo configurar la ejecución del Análisis de discos externos en Web Console y Cloud Console

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Tareas locales** > **Análisis de discos externos**.
5. Defina la configuración de la tarea.
6. Haga clic en Aceptar para guardar los cambios.

Cómo configurar la ejecución del Análisis de discos externos en la interfaz de la aplicación

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Análisis**, seleccione **Análisis de discos externos** en la lista de la izquierda.

3. En la sección **Cuando un disco externo se conecta**, seleccione la acción que desea que Kaspersky Endpoint Security realice cuando se conecta un disco externo.

Depósito de copias de seguridad

En ocasiones, no es posible conservar la integridad de los archivos infectados durante el proceso de desinfección. Si un archivo desinfectado contenía información importante a la que no se puede acceder total o parcialmente después de la desinfección, puede restaurar el archivo original desde el Depósito de copias de seguridad.

Una *copia de seguridad* es una copia de un archivo peligroso que se crea cuando dicho archivo se elimina o se desinfecta. Esta copia se almacena en el Depósito de copias de seguridad.

El *Depósito de copias de seguridad* es una zona especial de almacenamiento que contiene copias de seguridad de archivos que se han eliminado o modificado durante la desinfección. La función principal del Depósito de copias de seguridad es la de permitir al usuario restaurar un archivo original en cualquier momento. Los archivos del Depósito de copias de seguridad se guardan en un formato especial y no son peligrosos para el equipo.

Visualizar el contenido del Depósito de copias de seguridad

1. En la barra de menús, elija **Protección** > **Objetos detectados**.

   Se abre la ventana **Objetos detectados**.

2. En la sección **Copia de seguridad**, vea la lista de archivos con copias de seguridad.

Puede restaurar o eliminar copias de seguridad de los archivos desde el Depósito de copias de seguridad.

Restaurar una copia de seguridad de un archivo desde el Depósito de copias de seguridad

1. En la barra de menús, elija **Protección** > **Objetos detectados**.

   Se abre la ventana **Objetos detectados**.

2. En la sección **Copia de seguridad**, haga clic en ••• al lado del archivo que quiere restaurar.

   El menú emergente se abre.

3. Elija **Restaurar archivo**.

   Se abre una ventana en la que tiene que especificar el nombre de archivo, la etiqueta y la carpeta en la que el archivo será restaurado. De forma predeterminada, el nombre de archivo original y la ubicación ya están especificados.

4. Especificar el nombre de archivo y la carpeta en la que el archivo será restaurado.

5. Haga clic en **Guardar**.

La aplicación restaura el archivo a la ubicación especificada con el nombre especificado.

Tiene que analizar el archivo en busca de software malicioso inmediatamente después de restaurarlo. Es posible que el objeto pueda desinfectarse mediante las bases de datos actualizadas sin dañarse.

Importante: Recomendamos que no restaure copias de seguridad de archivos a menos que sea absolutamente necesario, porque podría causar una infección del equipo.

Eliminar una copia de seguridad de un archivo desde el Depósito de copias de seguridad

1. En la barra de menús, elija **Protección** > **Objetos detectados**.

   Se abre la ventana **Objetos detectados**.

2. En la sección **Copia de seguridad**, haga lo siguiente:

   - Para eliminar todas las copias de seguridad de archivos, haga clic en **Eliminar todo**.
   - Para eliminar la copia de seguridad seleccionada, haga clic en ••• al lado de esta y elija **Eliminar copia de seguridad**.

De forma predeterminada, el período de almacenamiento de archivos en el Depósito de copias de seguridad es de 30 días. Pasado este período, los archivos se eliminan. Puede cambiar la duración del período máximo de almacenamiento de los archivos en el Depósito de copias de seguridad o quitar el límite de duración.

Configurar el período de almacenamiento de los archivos en el Depósito de copias de seguridad

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Amenazas**, en la sección **Copia de seguridad**, seleccione la casilla de verificación **Eliminar copias de seguridad de los objetos luego de <número> días** y especifique el período tras el cual los archivos almacenados en el Depósito de copias de seguridad se eliminan automáticamente.

Informes

Puede consultar el informe de Kaspersky Endpoint Security en el que se muestran todos los objetos detectados en la pestaña **Objetos procesados**. Los eventos del sistema se muestran en la pestaña **Eventos del sistema**. Además, se crea un informe detallado separado para cada uno de los siguientes componentes de la aplicación: Protección frente a amenazas en archivos, Protección frente a amenazas web, Protección frente a amenazas en la red, Detección de comportamiento y análisis y tareas de actualización.

Abrir la ventana Informes

En la barra de menús, elija **Protección** > **Informes**.

Kaspersky Endpoint Security le permite guardar informes en formato de texto. Esta funcionalidad puede resultar útil si se producen errores en tareas de análisis o componentes de la aplicación que no puede reparar por sí mismo y, por lo tanto, necesita obtener asistencia del Servicio de soporte técnico de Kaspersky. En ese caso, envíe el informe de texto al Servicio de soporte técnico de Kaspersky para que nuestros especialistas puedan analizar el problema y resolverlo lo antes posible.

Exportar un informe del componente Kaspersky Endpoint Security o informe de tarea a un archivo de texto

1. En la barra de menús, elija **Protección** > **Informes**.

   Se abre la ventana **Informes**.

2. En el panel izquierdo, seleccione la pestaña con el informe requerido.
3. En la esquina derecha superior, haga clic en .
4. En la ventana que se abre, especifique el nombre de fichero, las etiquetas y la carpeta del destino para el informe.
5. Haga clic en **Guardar**.

Por defecto, Kaspersky Endpoint Security no registra eventos informativos en informes. Puede permitir el registro de eventos informativos.

Permita el registro de eventos informativos en informes

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Informes**, seleccione la casilla de verificación **Registrar eventos no críticos** para recibir notificaciones sobre eventos informativos de Kaspersky Endpoint Security.

Managed Detection and Response

El componente Managed Detection and Response se agregó a Kaspersky Endpoint Security en la versión 11.2. Este componente interactúa con una solución llamada Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* busca, detecta y elimina amenazas dirigidas a su organización de forma ininterrumpida. Para obtener más información sobre cómo funciona la solución, consulte la *Ayuda de Kaspersky Managed Detection and Response*.

Al interactuar con Kaspersky Managed Detection and Response, la aplicación le permite realizar las siguientes funciones:

- Activar Managed Detection and Response a partir de un archivo de configuración BLOB.
- Ejecutar comandos desde Kaspersky Managed Detection and Response.
- Enviar datos telemétricos a Kaspersky Managed Detection and Response para la detección de amenazas.

El componente Managed Detection and Response tiene los siguientes requisitos adicionales:

- macOS 12 o versiones posteriores
- Mac basado en Intel, Apple Silicon
- Licencia de Kaspersky Endpoint Security activa

Integración con Kaspersky Managed Detection and Response

La integración con Kaspersky Managed Detection and Response consta de los siguientes pasos:

1. **Configurar el servidor proxy de Kaspersky Security Network**

   El servidor proxy de Kaspersky Security Network facilita el intercambio de datos entre equipos y la infraestructura de servicio en la nube de Kaspersky Security Network a través del Servidor de administración, en lugar de realizar un intercambio directo.

   Cargue el archivo de configuración de Kaspersky Security Network en las propiedades del Servidor de administración. El archivo de configuración de Kaspersky Security Network se encuentra en el archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en la consola de Kaspersky Managed Detection and Response. Para obtener más información sobre cómo configurar el servidor proxy de Kaspersky Security Network, consulte la *Ayuda de Kaspersky Security Center*.

   Como resultado, Kaspersky Endpoint Security utilizará KSN privada para determinar la reputación de archivos, aplicaciones y sitios web. El estado de funcionamiento *"Infraestructura: Kaspersky Private Security Network"* se indicará en la configuración de la directiva, en la sección Kaspersky Security Network.

   El uso de KSN privada con Kaspersky Managed Detection and Response asegura que la telemetría se envíe a servidores que cumplen con el RGPD (Reglamento General de Protección de Datos). Si no se utiliza KSN privada, la telemetría se puede enviar a KSN Global. Esto puede violar las leyes de su país.

   Importante: Debe activar el modo KSN extendido para que Managed Detection and Response funcione.

2. **Activar Managed Detection and Response**

   Cargue el archivo de configuración BLOB en la directiva de Kaspersky Endpoint Security (ver las instrucciones a continuación). El archivo BLOB contiene la ID del cliente e información acerca de la licencia para Kaspersky Managed Detection and Response. El archivo BLOB está ubicado en el archivo comprimido ZIP del archivo de configuración MDR. Puede obtener el archivo comprimido ZIP en la consola de Kaspersky Managed Detection and Response. Para obtener información detallada sobre el archivo BLOB, consulte la *Ayuda de Kaspersky Managed Detection and Response*.

   Activar Managed Detection and Response en la Consola de administración (MMC)

   1. Inicie la Consola de administración de Kaspersky Security Center.
   2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
   3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
   4. En el espacio de trabajo, elija la pestaña **Directivas**.
   5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
   6. En la ventana **Propiedades**, seleccione **Detection and Response** > **Managed Detection and Response**.
   7. Seleccione la casilla de verificación **Managed Detection and Response**.
   8. En el bloque del **Archivo de configuración MDR**, haga clic en **Importar** y seleccione el archivo BLOB recibido en la consola de Kaspersky Managed Detection and Response. El archivo tiene la extensión .P7.
   9. Haga clic en **Aceptar** para guardar los cambios.

Activar Managed Detection and Response en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
3. Se abre la ventana de propiedades de la directiva.
4. Elija la pestaña **Configuración de la aplicación**.
5. Seleccione **Detection and Response** > **Managed Detection and Response**.
6. Active el interruptor de **Managed Detection and Response**.
7. Haga clic en **Importar** y seleccione el archivo BLOB obtenido en la consola de Kaspersky Managed Detection and Response. El archivo tiene la extensión .P7.
8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security verifica el archivo BLOB. La verificación del archivo BLOB incluye una revisión de la firma digital y del período de validez de la licencia. Si el archivo BLOB se verifica correctamente, Kaspersky Endpoint Security carga y envía el archivo al equipo durante la siguiente sincronización con Kaspersky Security Center.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security admite la integración con el componente Kaspersky Endpoint Detection and Response como parte de la solución Kaspersky Anti Targeted Attack Platform. Esta solución está diseñada para detectar rápidamente amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas, ataques de día cero y otras. Para obtener más información sobre cómo funciona la solución, consulte la *Ayuda de Kaspersky Anti Targeted Attack Platform*.

Cuando se configura la integración con Endpoint Detection and Response (KATA), el servidor KATA recibe información sobre los eventos que se producen en el funcionamiento de Kaspersky Endpoint Security y las amenazas detectadas por la aplicación, así como información sobre el procesamiento de estas amenazas. Para reaccionar a las amenazas detectadas, Kaspersky Endpoint Security puede realizar las tareas iniciadas en la interfaz web de Kaspersky Anti Targeted Attack Platform.

El componente Endpoint Detection and Response (KATA) tiene los siguientes requisitos adicionales:

- Kaspersky Anti Targeted Attack Platform 6.0 o posterior.
- Kaspersky Security Center 14.2 o versiones posteriores.
- La integración con Endpoint Detection and Response (KATA) se puede configurar en la Consola de administración de Kaspersky Security Center (MMC), en Web Console o Cloud Console.

Integración con Kaspersky Endpoint Detection and Response (KATA)

La integración con Kaspersky Managed Detection and Response (KATA) consta de los siguientes pasos:

1. **Instalar el componente Endpoint Detection and Response**

   Puede elegir el componente Endpoint Detection and Response durante la instalación de Kaspersky Endpoint Security.

2. **Activar Endpoint Detection and Response**

   Si el componente Endpoint Detection and Response no es compatible con su licencia actual, debe activar Kaspersky Endpoint Detection and Response de manera independiente.

   Puede comprobar si la funcionalidad de Endpoint Detection and Response es compatible con la licencia actual en la ventana **Licencia**.

3. **Conectarse a un servidor KATA.**

   Kaspersky Anti Targeted Attack Platform requiere establecer una conexión de confianza entre Kaspersky Endpoint Security y un servidor KATA. Para configurar una conexión de confianza, debe usar un certificado TLS. Puede descargar un certificado TLS en la interfaz web de Kaspersky Anti Targeted Attack Platform. Para obtener información detallada sobre la descarga de un certificado, consulte la *Ayuda de Kaspersky Anti Targeted Attack Platform*.

   De manera predeterminada, Kaspersky Endpoint Security verifica el certificado TLS solo del servidor KATA. Para que la conexión sea más segura, puede activar la verificación bidireccional. Para activar la verificación bidireccional, debe usar un contenedor de cifrado protegido por contraseña. Para obtener información detallada sobre la descarga de un contenedor de cifrado, consulte la *Ayuda de Kaspersky Anti Targeted Attack Platform*.

   Conectar equipos con Kaspersky Endpoint Security a un servidor KATA mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, elija la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, elija **Detection and Response** > **Endpoint Detection and Response (KATA)**.
7. Elija la casilla de verificación **Endpoint Detection and Response (KATA)**.
8. Haga clic en **Configuración de conexión a servidor**.
9. En la ventana **Configuración de conexión a servidor** que se abre, configure los siguientes ajustes:
   - Haga clic en **Añadir certificado TLS** para elegir un certificado TLS que se utilizará para establecer una conexión de confianza con un servidor KATA.
   - Si desea cambiar el tiempo de espera de respuesta del servidor KATA, especifique el tiempo de espera en el campo **Tiempo de espera (s)**. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor KATA.
   - Si desea utilizar la verificación bidireccional, elija la casilla de verificación **Utilizar verificación bidireccional**. Haga clic en **Cargar criptocontenedor** para elegir un archivo de contenedor de cifrado e introduzca la contraseña en el campo **Contraseña de criptocontenedor**.
10. Haga clic en **Guardar**.
11. Para añadir un servidor KATA, haga clic en **Añadir**.
12. En la ventana del **Servidor KATA** que se abre, especifique la dirección y el puerto del servidor y haga clic en **Guardar**.
13. Haga clic en **Aceptar** para guardar los cambios.

Conecte equipos con Kaspersky Endpoint Security a un servidor KATA mediante Web Console

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.
4. Elija **Detection and Response** > **Endpoint Detection and Response (KATA)**.
5. Active el interruptor de **Endpoint Detection and Response (KATA)**.
6. Haga clic en **Configuración de conexión a servidor**.
7. En el cuadro de diálogo **Configuración de conexión a servidor** que se abre, configure lo siguiente:
   - Haga clic en **Añadir certificado TLS** para elegir un certificado TLS que se utilizará para establecer una conexión de confianza con un servidor KATA.
   - Si desea cambiar el tiempo de espera de respuesta del servidor KATA, especifique el tiempo de espera en el campo **Tiempo de espera (s)**. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor KATA.
   - Si desea utilizar la verificación bidireccional, elija la casilla de verificación **Utilizar verificación bidireccional**. Haga clic en **Cargar criptocontenedor** para elegir un archivo de contenedor de cifrado e introduzca la contraseña en el campo **Contraseña de criptocontenedor**.
8. Haga clic en **Aceptar**.
9. Para añadir un servidor KATA, haga clic en **Añadir**.
10. En el cuadro de diálogo que se abre, especifique la dirección y el puerto del servidor y haga clic en **Aceptar**.

11. Guarde los cambios.

Como resultado, los equipos aparecerán en la interfaz web de Kaspersky Anti Targeted Attack Platform.

Endpoint Detection and Response Optimum

A partir de la versión 12.1, Kaspersky Endpoint Security for Mac incluye un agente integrado para la solución Kaspersky Endpoint Detection and Response Optimum (en adelante, también "EDR Optimum"). Esta solución está diseñada para proteger la infraestructura de TI corporativa frente a las ciberamenazas avanzadas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos, así como métodos que utilizan herramientas legítimas del sistema. Para obtener detalles sobre la solución, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

Kaspersky Endpoint Detection and Response revisa y analiza el desarrollo de amenazas y proporciona al *personal de seguridad* o al *Administrador* información sobre el posible ataque que es necesaria para una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana separada. *Detalles de alerta* es una herramienta para ver toda la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, por ejemplo, el historial de archivos que aparecen en el ordenador. Para obtener más información sobre la administración de los detalles de las alertas, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

Nota: Puede configurar el componente EDR Optimum en Web Console.

Ajustes de Endpoint Detection and Response

Parámetro	Descripción
Aislamiento de red	Aislamiento automático del ordenador de la red en respuesta a amenazas detectadas. Cuando el aislamiento de red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones nuevas de TCP/IP en el ordenador. La aplicación solo deja activas las siguientes conexiones: • Conexiones enumeradas en Exclusiones de Aislamiento de red. • Conexiones iniciadas por los servicios de Kaspersky Endpoint Security. • Conexiones iniciadas por el Agente de red de Kaspersky Security Center.
Desbloquear automáticamente el equipo aislado en N horas	El aislamiento de red se puede desactivar de forma automática después de un tiempo especificado o manualmente. De manera predeterminada, Kaspersky Endpoint Security desactiva el aislamiento de red 8 horas después del inicio del aislamiento.
Exclusiones de aislamiento de red	Lista de reglas para las exclusiones del aislamiento de red. Las conexiones de red que coinciden con las reglas no se bloquean en los ordenadores cuando el aislamiento de red está activado. Para configurar las exclusiones de Aislamiento de red, puede utilizar una lista de perfiles de red estándar. De manera predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y las funciones de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones manualmente. **Importante:** Las exclusiones especificadas en las propiedades de la directiva se aplican solo si Aislamiento de red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del ordenador se aplican solo si el aislamiento de red se activa manualmente en las propiedades del ordenador de la consola de Kaspersky Security Center o en los detalles de la alerta.
Prevención de ejecución	Prevención de ejecución permite administrar la ejecución de archivos ejecutables y scripts, así como abrir archivos en formato Office. De esta manera, por ejemplo, puede evitar la ejecución de aplicaciones que considere inseguras. Como resultado, se puede detener la propagación de la amenaza. Prevención de ejecución admite un conjunto de intérpretes de scripts. Para usar el componente de Prevención de ejecución, debe añadir reglas de prevención de ejecución. La regla de Prevención de ejecución es un conjunto de criterios que la aplicación tiene en cuenta cuando reacciona a la ejecución de un objeto, por ejemplo, cuando bloquea la ejecución de un objeto. La aplicación identifica archivos por las rutas o sumas de verificación que se calculan mediante algoritmos hash MD5 y SHA256.
Acción al ejecutar o abrir un objeto prohibido	**Bloquear y escribirlo en el informe**. En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado. **Solo eventos del registro**. En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de iniciar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de manera predeterminada.

Sandbox en la nube

Sandbox en la nube es una tecnología que le permite detectar amenazas avanzadas en un ordenador. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados para analizarse a Sandbox en la nube. Sandbox en la nube ejecuta estos archivos en un entorno aislado para identificar la actividad maliciosa y decide su reputación. Luego, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Sandbox en la nube ha detectado un archivo malicioso, Kaspersky Endpoint Security realizará la acción apropiada para eliminar esta amenaza en todos los ordenadores en los que se detecte este archivo.

Nota: La tecnología de Sandbox en la nube está siempre activada y disponible para todos los usuarios de Kaspersky Security Network, independientemente del tipo de licencia que usen.

Integración con Endpoint Detection and Response Optimum

Para integrarse con Kaspersky Endpoint Detection and Response, debe añadir el componente Endpoint Detection and Response Optimum (EDR Optimum) y configurar Kaspersky Endpoint Security.

Nota: Los componentes EDR Optimum y Endpoint Detection and Response (KATA) no son compatibles entre sí.

Se deben cumplir las siguientes condiciones para que funcione Endpoint Detection and Response:

- La versión de Kaspersky Security Center es 13.2 o posterior. En versiones anteriores de Kaspersky Security Center, no se puede activar la función Endpoint Detection and Response.
- El complemento de administración de Kaspersky Endpoint Detection and Response está instalado. Este es un único complemento para trabajar con agentes en los sistemas operativos Windows, Mac y Linux. Cuando trabaje con Endpoint Detection and Response Optimum, necesitará el complemento de administración de Kaspersky Endpoint Security para crear tareas de respuesta ante amenazas y el complemento de administración de EDR para los detalles de alertas.
- El componente EDR Optimum como parte de Kaspersky Endpoint Security admite la interacción con la solución Kaspersky Endpoint Detection and Response Optimum 3.0. La interacción con versiones anteriores de Kaspersky Endpoint Detection and Response Optimum no es compatible.
- EDR Optimum se puede administrar en Web Console.
- La aplicación está activada y la licencia cubre la funcionalidad.
- El componente Endpoint Detection and Response está activado.

Integración con Kaspersky Endpoint Detection and Response Optimum

La integración con Kaspersky Endpoint Detection and Response Optimum consta de los siguientes pasos:

1. **Instalar el componente Endpoint Detection and Response Optimum**

   Puede elegir el componente Endpoint Detection and Response durante la instalación de Kaspersky Endpoint Security.

2. **Activar Endpoint Detection and Response**

   Si el componente Endpoint Detection and Response no es compatible con su licencia actual, debe activar Kaspersky Endpoint Detection and Response de manera independiente.

   Puede comprobar si la funcionalidad de Endpoint Detection and Response es compatible con la licencia actual en la ventana **Licencia**.

3. **Activar el componente Endpoint Detection and Response**

   Puede activar o desactivar el componente en la configuración de la directiva de Kaspersky Endpoint Security for Mac.

   Cómo activar o desactivar el componente Endpoint Detection and Response en Web Console

   1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
   2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
      Se abre la ventana de propiedades de la directiva.
   3. Elija la pestaña **Configuración de la aplicación**.
   4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
   5. Active el interruptor de **Endpoint Detection and Response**.

6. Guarde los cambios.

Análisis en busca de indicadores de peligro

Un **indicador de peligro (IOC)** es un conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al ordenador (vulneración de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de peligro. La tarea **Análisis de IOC** permite encontrar indicadores de peligro en el ordenador y tomar medidas de respuesta a las amenazas.

Kaspersky Endpoint Security busca indicadores de peligro mediante el uso de archivos de IOC. Los archivos de IOC son archivos que contienen los conjuntos de indicadores que la aplicación intenta vincular para contar una detección. Los archivos de IOC deben cumplir con las requisitos para los archivos de IOC.

Modo de ejecución de la tarea de Análisis de IOC

Kaspersky Endpoint Detection and Response le permite crear tareas de Análisis de IOC estándar para detectar datos vulnerados. La tarea de Análisis de IOC estándar es una tarea grupal o local que se crea y configura manualmente en Web Console. Las tareas se ejecutan con archivos de IOC preparados por el usuario. Si desea añadir un indicador de peligro manualmente, lea los requisitos para los archivos de IOC.

Crear una tarea de Análisis de IOC

Puede crear tareas de Análisis de IOC manualmente de las siguientes maneras:

- En los detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta para ver toda la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, por ejemplo, el historial de archivos que aparecen en el ordenador. Para obtener más información sobre la administración de los detalles de las alertas, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

- Con el Asistente de tareas.

Para crear una tarea de Análisis de IOC, siga estos pasos:

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**.

3. Defina la configuración de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Mac (12.2).

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

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

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

4. Seleccione los dispositivos de acuerdo con el alcance seleccionado de la tarea.

5. En la sección **Configuración del análisis de IOC**, cargue los archivos de IOC para buscar indicadores de peligro. Puede añadir un archivo de IOC o generar uno a partir de un archivo que contenga hashes de archivos o direcciones IP.

   Después de cargar los archivos de IOC, puede ver y editar la lista de indicadores de los archivos de IOC.

   Nota: No se recomienda añadir ni eliminar archivos de IOC después de ejecutar la tarea. Esto puede hacer que los resultados del Análisis de IOC se muestren incorrectamente para ejecuciones anteriores de la tarea. Para buscar indicadores de peligro según nuevos archivos de IOC, se recomienda añadir nuevas tareas.

6. Configure las acciones al detectar un IOC:

   - **Aislar el equipo de la red**. Si se selecciona esta opción, Kaspersky Endpoint Security aísla el ordenador de la red para evitar que la amenaza se propague. Puede configurar la duración del aislamiento en la configuración del componente Endpoint Detection and Response.

   - **Mover la copia a la cuarentena y eliminar objeto**. Si se selecciona esta opción, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el ordenador. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que el objeto deba restaurarse más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a la Cuarentena.

   - **Ejecutar análisis de áreas críticas**. Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea de Análisis rápido. De manera predeterminada, Kaspersky Endpoint Security analiza la memoria, los objetos de inicio y las carpetas del sistema.

7. Vaya a la sección Avanzado.
8. Seleccione los tipos de datos (documentos de IOC) que se deben analizar como parte de la tarea.

   Nota: Kaspersky Endpoint Security selecciona automáticamente los tipos de datos (documentos de IOC) para la tarea de Análisis de IOC de acuerdo con el contenido de los archivos de IOC cargados. No se recomienda anular la selección de los tipos de datos.

   Además, puede configurar la cobertura del análisis para los siguientes tipos de datos:

   - **Procesos: ProcessItem**
   - **Archivos: FileItem**
   - **Puertos de red: PortItem**
   - **Cuentas de usuario: UserItem**
   - **Tablas ARP: ArpEntryItem**
   - **Hosts: SystemInfoItem**
   - **Direcciones web – UrlHistoryItem**
   - **Rutas – RouteEntryItem**
9. Haga clic en **Aceptar**.
10. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar la tarea. Haga clic en **Siguiente**.

    Nota: De manera predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (root).

11. En el paso **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

    Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de la tarea. En esta ventana, puede verificar los parámetros de la tarea, modificarlos o configurar una programación de inicio de la tarea, si es necesario.

12. Haga clic en la tarea nueva.

    Se abre la ventana de propiedades de la tarea.

13. Seleccione la pestaña **Programar**.
14. Configurar la programación de la tarea.

    Nota: Asegúrese de que el ordenador esté encendido para ejecutar la tarea.

15. Haga clic en el botón **Guardar**.
16. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:

    a. Seleccione la casilla de verificación junto a la tarea.

17. Haga clic en el botón **Ejecutar**.

    Como resultado, Kaspersky Endpoint Security ejecuta la búsqueda de indicadores de peligro en el ordenador. Puede ver los resultados de la tarea en las propiedades de la tarea de la sección **Resultados**. Puede ver la información sobre los indicadores de vulneración detectados en las propiedades de la tarea: **Ajustes de la aplicación** > **Resultados del análisis de IOC**.

Nota: Los resultados del Análisis de IOC se conservan durante 30 días. Después de este período, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas.

Mover archivo a Cuarentena

Expandir todo | Contraer todo

Cuando reacciona a las amenazas, Kaspersky Endpoint Detection and Response puede crear tareas de *Mover archivo a la Cuarentena*. Esto es necesario para minimizar las consecuencias de la amenaza. La *Cuarentena* es un almacenamiento local especial en el ordenador. El usuario puede poner en cuarentena los archivos que considere peligrosos para el ordenador. Los archivos en cuarentena se almacenan en un estado cifrado y no amenazan la seguridad del dispositivo. Kaspersky Endpoint Security utiliza la Copia de seguridad como almacenamiento de archivos. Para obtener más información sobre cómo administrar la Cuarentena como parte de las soluciones, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

Puede crear tareas de *Mover archivo a la Cuarentena* de las siguientes maneras:

- En los detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta para ver toda la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, por ejemplo, el historial de archivos que aparecen en el ordenador. Para obtener más información sobre la administración de los detalles de las alertas, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

- Con el Asistente de tareas.

  Debe introducir la ruta del archivo o el hash (SHA256 o MD5), o tanto la ruta del archivo como el hash del archivo.

La tarea *Mover archivo a la Cuarentena* tiene las siguientes limitaciones:

- El tamaño del archivo no debe exceder los 100 MB.
- Puede configurar la tarea para EDR Optimum en Web Console.
- La capacidad de la Copia de seguridad está limitada por el espacio libre en disco.

Para crear una tarea de Mover archivo a la Cuarentena, siga estos pasos:

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**.

3. Defina la configuración de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Mac (12.2).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Mover archivo a la Cuarentena**.

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

   d. Seleccione una de las siguientes opciones:

   - **Asignar tarea a un grupo de administración**

     La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

     Por ejemplo, puede utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para los dispositivos incluidos en un grupo de administración específico.

     Si se asigna una tarea a un grupo de administración, no se mostrará la pestaña **Seguridad** en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a los ajustes de seguridad de los grupos a los que se aplican.

   - **Especificar direcciones de dispositivos manualmente o importar direcciones de una lista**

     Puede especificar nombres NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

     Puede utilizar esta opción a fin de ejecutar una tarea para una subred específica. Por ejemplo, puede instalar una determinada aplicación en los dispositivos de los contadores o analizar dispositivos en una subred que probablemente esté infectada.

   - **Asignar tarea a una selección de dispositivos**

     La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las siguientes selecciones:

     Por ejemplo, puede utilizar esta opción para ejecutar una tarea en dispositivos que tienen una versión específica del sistema operativo.

4. Seleccione los dispositivos de acuerdo con el alcance seleccionado de la tarea.

5. En el paso **Alcance de la tarea**, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   La configuración disponible depende de la opción que se selecciona en el paso anterior.

6. En la lista de archivos, haga clic en **Añadir**.

   Se inicia el asistente para añadir archivos.

7. En la lista desplegable **Indique el archivo que se moverá a Cuarentena**, seleccione una de las opciones y complete los campos requeridos. Para añadir el archivo, debe introducir la ruta completa al archivo, o tanto el hash del archivo como la ruta.

8. Si desea que la tarea se aplique a objetos críticos del sistema, seleccione la casilla **Aplicar a objetos críticos del sistema**.

9. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar la tarea. Haga clic en **Siguiente**.

   Nota: De manera predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (root).

10. En el paso **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

    Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de la tarea. En esta ventana, puede verificar los parámetros de la tarea, modificarlos o configurar una programación de inicio de la tarea, si es necesario.

11. Haga clic en la tarea nueva.

    Se abre la ventana de propiedades de la tarea.

12. Seleccione la pestaña **Programar**.

13. Configurar la programación de la tarea.

    Nota: Asegúrese de que el ordenador esté encendido para ejecutar la tarea.

14. Haga clic en el botón **Guardar**.

15. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:

    a. Seleccione la casilla de verificación junto a la tarea.

16. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security mueve el archivo a la Cuarentena.

La tarea *Mover archivo a la Cuarentena* puede finalizarse con el error *Acceso denegado* si intenta poner en cuarentena un archivo ejecutable que se está ejecutando. Cree una tarea de finalizar proceso para el archivo y vuelva a intentarlo.

La tarea *Mover archivo a la Cuarentena* puede finalizarse con el error *No hay suficiente espacio en el almacenamiento de la cuarentena* si intenta poner en cuarentena un archivo que es demasiado grande. Libere espacio en disco y vuelva a intentarlo.

Obtener archivo

Puede obtener archivos de los ordenadores de los usuarios. Por ejemplo, puede configurar la obtención de un archivo de registro de eventos creado por una aplicación de terceros. Para obtener el archivo, debe crear una tarea exclusiva. Como resultado de la ejecución de la tarea, el archivo se guarda en Copia de seguridad. Puede descargar este archivo desde Copia de seguridad a su ordenador mediante Web Console. En el ordenador del usuario, el archivo permanece en su carpeta original.

Importante: El tamaño del archivo no debe exceder los 100 MB. La capacidad de la Copia de seguridad está limitada por el espacio libre en disco.

Para crear una tarea Obtener archivo, siga estos pasos:

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**.

3. Defina la configuración de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Mac (12.2).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Obtener archivo**.

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

d. Seleccione una de las siguientes opciones:

- **Asignar tarea a un grupo de administración**

  La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

  Por ejemplo, puede utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para los dispositivos incluidos en un grupo de administración específico.

  Si se asigna una tarea a un grupo de administración, no se mostrará la pestaña **Seguridad** en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a los ajustes de seguridad de los grupos a los que se aplican.

- **Especificar direcciones de dispositivos manualmente o importar direcciones de una lista**

  Puede especificar nombres NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

  Puede utilizar esta opción a fin de ejecutar una tarea para una subred específica. Por ejemplo, puede instalar una determinada aplicación en los dispositivos de los contadores o analizar dispositivos en una subred que probablemente esté infectada.

- **Asignar tarea a una selección de dispositivos**

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las siguientes selecciones:

  Por ejemplo, puede utilizar esta opción para ejecutar una tarea en dispositivos que tienen una versión específica del sistema operativo.

4. Seleccione los dispositivos de acuerdo con el alcance seleccionado de la tarea. En la ventana **Obtener archivo**, haga clic en **Añadir**.

   Se abre el cuadro de diálogo **Obtener archivo**.

5. En la lista desplegable **Especifique qué archivo necesita obtener**, seleccione una de las opciones y complete los campos requeridos.

   Para añadir el archivo, debe introducir la ruta completa al archivo, o tanto el hash del archivo como la ruta.

6. Haga clic en **Aceptar**.

   La configuración del archivo que se añadirá se muestra en la lista de archivos.

7. Haga clic en **Siguiente**.

8. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar la tarea. Haga clic en **Siguiente**.

   Nota: De manera predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (root).

9. En el paso **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de la tarea. En esta ventana, puede verificar los parámetros de la tarea, modificarlos o configurar una programación de inicio de la tarea, si es necesario.

10. Haga clic en la tarea nueva.

    Se abre la ventana de propiedades de la tarea.

11. Seleccione la pestaña **Programar**.

12. Configurar la programación de la tarea.

    Nota: Asegúrese de que el ordenador esté encendido para ejecutar la tarea.

13. Haga clic en el botón **Guardar**.

14. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:

    a. Seleccione la casilla de verificación junto a la tarea.

15. Haga clic en el botón **Ejecutar**.

Como consecuencia, Kaspersky Endpoint Security crea una copia del archivo y mueve esa copia a la Copia de seguridad. Puede descargar el archivo desde Copia de seguridad en Web Console.

Eliminar el archivo

Puede eliminar archivos de manera remota mediante la tarea *Eliminar archivo*. Por ejemplo, puede eliminar un archivo de manera remota cuando responde a amenazas.

Para crear una tarea Eliminar archivo:

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**.

3. Defina la configuración de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Mac (12.2).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Eliminar archivo**.

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

   d. Seleccione una de las siguientes opciones:

   - Asignar tarea a un grupo de administración

     La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

     Por ejemplo, puede utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para los dispositivos incluidos en un grupo de administración específico.

     Si se asigna una tarea a un grupo de administración, no se mostrará la pestaña **Seguridad** en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a los ajustes de seguridad de los grupos a los que se aplican.

   - Especificar direcciones de dispositivos manualmente o importar direcciones de una lista

     Puede especificar nombres NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

     Puede utilizar esta opción a fin de ejecutar una tarea para una subred específica. Por ejemplo, puede instalar una determinada aplicación en los dispositivos de los contadores o analizar dispositivos en una subred que probablemente esté infectada.

   - Asignar tarea a una selección de dispositivos

     La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las siguientes selecciones:

     Por ejemplo, puede utilizar esta opción para ejecutar una tarea en dispositivos que tienen una versión específica del sistema operativo.

4. Seleccione los dispositivos de acuerdo con el alcance seleccionado de la tarea.

5. En la lista desplegable **Especifique qué archivo desea eliminar**, seleccione una de las opciones y complete los campos requeridos. Para añadir el archivo, debe introducir la ruta completa al archivo, o tanto el hash del archivo como la ruta.

6. Si desea que la tarea se aplique a objetos críticos del sistema, seleccione la casilla **Aplicar a objetos críticos del sistema**.

7. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar la tarea. Haga clic en **Siguiente**.

   Nota: De manera predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (root).

8. En el paso **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de la tarea. En esta ventana, puede verificar los parámetros de la tarea, modificarlos o configurar una programación de inicio de la tarea, si es necesario.

9. Haga clic en la tarea nueva.

   Se abre la ventana de propiedades de la tarea.

10. Seleccione la pestaña **Programar**.

11. Configurar la programación de la tarea.

Nota: Asegúrese de que el ordenador esté encendido para ejecutar la tarea.

12. Haga clic en el botón **Guardar**.

13. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:

    a. Seleccione la casilla de verificación junto a la tarea.

14. Haga clic en el botón **Ejecutar**.

    Como resultado, Kaspersky Endpoint Security elimina el archivo del ordenador. Si el archivo está bloqueado por un proceso diferente, la tarea se muestra como *Completada*, pero el archivo en sí se elimina después de reiniciar el ordenador. Después de reiniciar el ordenador, confirme que el archivo se haya eliminado.

La tarea *Eliminar archivo* puede finalizarse con el error *Acceso denegado* si intenta eliminar un archivo ejecutable que se está ejecutando actualmente. Cree una tarea de finalizar proceso para el archivo y vuelva a intentarlo.

Iniciar proceso

Expandir todo | Contraer todo

Puede ejecutar archivos de manera remota mediante la tarea *Iniciar proceso*.

Importante: Puede configurar la tarea para EDR Optimum en Web Console.

Para crear una tarea Iniciar proceso, siga estos pasos:

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Tareas**.

   Se abre la lista de tareas.

2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**.

3. Defina la configuración de la tarea:

   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Mac (12.2).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Iniciar proceso**.

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

   d. Seleccione una de las siguientes opciones:

   - Asignar tarea a un grupo de administración

     La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

     Por ejemplo, puede utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para los dispositivos incluidos en un grupo de administración específico.

     Si se asigna una tarea a un grupo de administración, no se mostrará la pestaña **Seguridad** en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a los ajustes de seguridad de los grupos a los que se aplican.

   - Especificar direcciones de dispositivos manualmente o importar direcciones de una lista

     Puede especificar nombres NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

     Puede utilizar esta opción a fin de ejecutar una tarea para una subred específica. Por ejemplo, puede instalar una determinada aplicación en los dispositivos de los contadores o analizar dispositivos en una subred que probablemente esté infectada.

   - Asignar tarea a una selección de dispositivos

     La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las siguientes selecciones:

     Por ejemplo, puede utilizar esta opción para ejecutar una tarea en dispositivos que tienen una versión específica del sistema operativo.

4. Seleccione los dispositivos de acuerdo con el alcance seleccionado de la tarea.
5. En el paso **Alcance de la tarea**, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   La configuración disponible depende de la opción que se selecciona en el paso anterior.
6. Defina la configuración de la tarea:
   a. En el campo **Comando ejecutable**, especifique el comando que se ejecutará en el dispositivo local.
   b. Si es necesario, especifique los argumentos de la línea de comandos en el campo **Argumentos de la línea de comandos (opcional)**.
   c. Si es necesario, especifique la ruta al archivo ejecutable en el campo **Ruta de acceso a la carpeta de trabajo (opcional)**.
7. En el paso **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de la tarea. En esta ventana, puede verificar los parámetros de la tarea, modificarlos o configurar una programación de inicio de la tarea, si es necesario.
8. Haga clic en la tarea nueva.

   Se abre la ventana de propiedades de la tarea.
9. Seleccione la pestaña **Programar**.
10. Configurar la programación de la tarea.

    Nota: Asegúrese de que el ordenador esté encendido para ejecutar la tarea.
11. Haga clic en el botón **Guardar**.
12. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:
    a. Seleccione la casilla de verificación junto a la tarea.
13. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security ejecuta el comando en modo silencioso e inicia el proceso. Puede ver los resultados de la tarea en las propiedades de la tarea de la sección **Resultados de la ejecución**.

Terminar proceso

Expandir todo | Contraer todo

Puede finalizar procesos de manera remota mediante la tarea *Finalizar proceso*. Por ejemplo, puede finalizar de manera remota una utilidad de prueba de velocidad de Internet que se inició mediante la tarea Iniciar proceso.

Si desea prohibir la ejecución de un archivo, puede configurar el componente de Prevención de ejecución. Puede prohibir la ejecución de archivos ejecutables, scripts y archivos en formato Office.

La tarea de *Finalizar proceso* tiene las siguientes limitaciones:

- Puede configurar la tarea solo para EDR Optimum en Web Console.

Para crear una tarea Finalizar proceso, siga estos pasos:

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Tareas**.

   Se abre la lista de tareas.
2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**.
3. Defina la configuración de la tarea:
   a. En la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Mac (12.2).
   b. En la lista desplegable **Tipo de tarea**, seleccione **Terminar proceso**.
   c. En el campo **Nombre de la tarea**, introduzca una breve descripción.
   d. Seleccione una de las siguientes opciones:
      - Asignar tarea a un grupo de administración

La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

Por ejemplo, puede utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para los dispositivos incluidos en un grupo de administración específico.

Si se asigna una tarea a un grupo de administración, no se mostrará la pestaña **Seguridad** en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a los ajustes de seguridad de los grupos a los que se aplican.

- Especificar direcciones de dispositivos manualmente o importar direcciones de una lista

  Puede especificar nombres NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los que desea asignar la tarea.

  Puede utilizar esta opción a fin de ejecutar una tarea para una subred específica. Por ejemplo, puede instalar una determinada aplicación en los dispositivos de los contadores o analizar dispositivos en una subred que probablemente esté infectada.

- Asignar tarea a una selección de dispositivos

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las siguientes selecciones:

  Por ejemplo, puede utilizar esta opción para ejecutar una tarea en dispositivos que tienen una versión específica del sistema operativo.

4. Seleccione los dispositivos de acuerdo con el alcance seleccionado de la tarea.
5. En el paso **Alcance de la tarea**, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   La configuración disponible depende de la opción que se selecciona en el paso anterior.
6. En este paso del asistente, en la lista desplegable **Indique el archivo cuyos procesos deben finalizarse**, seleccione una de las opciones y complete los campos obligatorios. Para especificar el archivo, debe introducir la ruta completa al archivo, o tanto el hash del archivo como la ruta.

   Nota: Si está creando esta tarea para un dispositivo local, puede especificar el proceso por PID.
7. Si desea que la tarea se aplique a objetos críticos del sistema, seleccione la casilla **Aplicar a objetos críticos del sistema**.
8. Introduzca las credenciales de la cuenta del usuario cuyos derechos desea usar para ejecutar la tarea. Haga clic en **Siguiente**.

   Nota: De manera predeterminada, Kaspersky Endpoint Security inicia la tarea como la cuenta de usuario del sistema (root).
9. En el paso **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de la tarea. En esta ventana, puede verificar los parámetros de la tarea, modificarlos o configurar una programación de inicio de la tarea, si es necesario.
10. Haga clic en la tarea nueva.

    Se abre la ventana de propiedades de la tarea.
11. Seleccione la pestaña **Programar**.
12. Configurar la programación de la tarea.

    Nota: Asegúrese de que el ordenador esté encendido para ejecutar la tarea.
13. Haga clic en el botón **Guardar**.
14. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:

    a. Seleccione la casilla de verificación junto a la tarea.
15. Haga clic en el botón **Ejecutar**.

Como resultado, Kaspersky Endpoint Security finaliza el proceso en el ordenador. Por ejemplo, si se está ejecutando una aplicación de *Juego* y finaliza el proceso de *Juego*, la aplicación se cierra sin guardar los datos. Puede ver los resultados de la tarea en las propiedades de la tarea de la sección **Resultados**.

Prevención de ejecución

Prevención de ejecución permite administrar la ejecución de archivos ejecutables y scripts, así como abrir archivos en formato Office. De esta manera, por ejemplo, puede evitar la ejecución de aplicaciones que considere inseguras. Como resultado, se puede detener la propagación de la amenaza. Prevención de ejecución admite un conjunto de intérpretes de scripts.

Regla de Prevención de ejecución

Prevención de ejecución administra el acceso de los usuarios a los archivos con reglas de Prevención de ejecución. La regla de Prevención de ejecución es un conjunto de criterios que la aplicación tiene en cuenta cuando reacciona a la ejecución de un objeto, por ejemplo, cuando bloquea la ejecución de un objeto. La aplicación identifica archivos por las rutas o sumas de verificación que se calculan mediante algoritmos hash MD5 y SHA256.

Puede crear reglas de Prevención de ejecución:

- En los detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta para ver toda la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, por ejemplo, el historial de archivos que aparecen en el ordenador. Para obtener más información sobre la administración de los detalles de las alertas, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.

- Con una directiva de grupo o la configuración de la aplicación local. Debe introducir la ruta del archivo o el hash (SHA256 o MD5), o tanto la ruta del archivo como el hash del archivo.

También puede administrar Prevención de ejecución localmente mediante la línea de comandos.

Nota: No se puede bloquear el inicio de objetos críticos del sistema (SCO). Los SCO son archivos que el sistema operativo y la aplicación Kaspersky Endpoint Security for Mac requieren para poder ejecutarse.

Modos de la regla de Prevención de ejecución

El componente de Prevención de ejecución puede funcionar en dos modos:

- **Solo estadísticas**

  En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de iniciar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de manera predeterminada.

- **Activa**

  En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado.

Administrar Prevención de ejecución

Importante: Solo puede definir la configuración del componente en Web Console.

Para evitar la ejecución, siga estos pasos:

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Ajustes de la aplicación**.
4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
5. Active el conmutador **Prevención de ejecución**.
6. En el bloque **Acción al ejecutar o abrir un objeto prohibido**, seleccione el modo de funcionamiento del componente:

   - **Bloquear y escribirlo en el informe**. En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado.

   - **Solo eventos del registro**. En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de iniciar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de manera predeterminada.

7. Cree una lista de reglas de Prevención de ejecución:

   a. Haga clic en **Agregar**.

   b. En el cuadro de diálogo que se abre, introduzca el nombre de la regla de Prevención de ejecución (por ejemplo, Aplicación A).

   c. En la lista desplegable **Tipo**, seleccione el objeto que desea bloquear: **Aplicación**, **Script**, **Documento**.

   Si selecciona un tipo de objeto incorrecto, Kaspersky Endpoint Security no bloquea el archivo o script.

   d. Para añadir el archivo, debe introducir el hash del archivo (SHA256 o MD5), la ruta completa al archivo o tanto el hash como la ruta.

> **Nota:** Si el archivo está ubicado en una unidad de red, introduzca la ruta del archivo de la siguiente manera: /Volúmenes/nombre_de_carpeta_compartida/nombre_de_archivo. Si la ruta del archivo contiene la letra de una unidad de red, Kaspersky Endpoint Security no bloquea el archivo o script.

   a. Haga clic en **Aceptar**.

8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security bloquea la ejecución de objetos: ejecutar archivos ejecutables y scripts, abrir archivos en formato Office. Sin embargo, por ejemplo, puede abrir un archivo de script en un editor de texto incluso si no se puede ejecutar el script. Cuando bloquea la ejecución de un objeto, Kaspersky Endpoint Security muestra una notificación estándar si las notificaciones están activadas en la configuración de la aplicación.

Aislamiento de la red informática

Expandir todo | Contraer todo

El aislamiento de la red informática permite aislar automáticamente un ordenador de la red en respuesta a la detección de un indicador de peligro (IOC); este es el modo automático. Puede activar Aislamiento de red manualmente mientras investiga la amenaza detectada; este es el modo manual.

Cuando Aislamiento de red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones de red TCP/IP nuevas en el ordenador, excepto las siguientes conexiones:

- Conexiones enumeradas en Exclusiones de Aislamiento de red.
- Conexiones iniciadas por los servicios de Kaspersky Endpoint Security.
- Conexiones iniciadas por el Agente de red de Kaspersky Security Center.

> **Importante:** Solo puede definir la configuración del componente en Web Console.

Modo de Aislamiento de red automático

Puede configurar Aislamiento de red para que se active automáticamente en respuesta a la detección de un IOC. Puede configurar el modo de Aislamiento de red automático con una directiva de grupo.

Cómo configurar Aislamiento de red para que se active automáticamente en respuesta a la detección de un IOC

1. En la ventana principal de Web Console, elija **Dispositivos** > **Tareas**.
2. Se abre la lista de tareas.
3. Haga clic en la tarea **Análisis de IOC** de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la tarea.

   Si es necesario, cree la tarea Análisis de IOC.
4. Elija la pestaña **Configuración de la aplicación**.
5. En el bloque **Acción al detectar una IOC**, seleccione la opción **Alertar y tomar medidas de respuesta después de encontrar un IOC** y, luego, la casilla **Aislar el ordenador de la red (8 horas)**.
6. Guarde los cambios.
7. Como resultado, cuando se detecta un IOC, la aplicación aísla el ordenador de la red para evitar que la amenaza se propague.

Puede configurar Aislamiento de red para que se desactive automáticamente después de que transcurra un tiempo especificado. De manera predeterminada, la aplicación desactiva Aislamiento de red después de que hayan pasado 8 horas desde el momento en que se activó. También puede desactivar Aislamiento de red manualmente (consulte las instrucciones a continuación). Después de desactivar Aislamiento de red, el ordenador puede usar la red sin restricciones.

Cómo configurar el retraso para desactivar Aislamiento de red de un ordenador en modo automático

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.
4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
5. En el bloque **Aislamiento de red**, haga clic en **Configure los ajustes de desbloqueo de equipos**.
6. En la ventana que se abre, seleccione la casilla **Desbloquear automáticamente el equipo aislado en** e introduzca el retraso para desactivar Aislamiento de red automáticamente.
7. Guarde los cambios.

Modo de Aislamiento de red manual

Puede activar y desactivar manualmente Aislamiento de red. Puede configurar el modo de Aislamiento de red manual mediante las propiedades del equipo en la consola de Kaspersky Security Center.

Puede activar Aislamiento de red de las siguientes maneras:

- En los detalles de alerta (solo para EDR Optimum).
  Detalles de alerta es una herramienta para ver toda la información recopilada sobre una amenaza detectada. Los detalles de la alerta incluyen, por ejemplo, el historial de archivos que aparecen en el ordenador. Para obtener más información sobre la administración de los detalles de las alertas, consulte la Ayuda de Kaspersky Endpoint Detection and Response Optimum.
- Con la configuración de la aplicación local.

Cómo activar Aislamiento de red de un ordenador manualmente

1. En la ventana principal de Web Console, elija **Dispositivos** > **Dispositivos administrados**.
2. Seleccione el ordenador para el que desea definir la configuración local de la aplicación.
   Se abren las propiedades del ordenador.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security for Mac**.
   Se abre la configuración local de la aplicación.
5. Elija la pestaña **Configuración de la aplicación**.
6. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
7. En el bloque **Aislamiento de red**, haga clic en **Aislar el equipo de la red**.

Puede configurar Aislamiento de red para que se desactive automáticamente después de que transcurra un tiempo especificado. De manera predeterminada, la aplicación desactiva Aislamiento de red después de que hayan pasado 8 horas desde el momento en que se activó. Después de desactivar Aislamiento de red, el ordenador puede usar la red sin restricciones.

Cómo configurar el retraso para desactivar Aislamiento de red de un ordenador en modo manual

1. En la ventana principal de Web Console, elija **Dispositivos** > **Dispositivos administrados**.
2. Seleccione el ordenador para el que desea definir la configuración local de la aplicación.
   Se abren las propiedades del ordenador.

3. Seleccione la pestaña **Tareas**.

   Se muestra la lista de tareas disponibles en el ordenador.

4. Seleccione la tarea **Aislamiento de red**.

5. Elija la pestaña **Configuración de la aplicación**.

6. En la ventana que se abre, seleccione el retraso para desactivar Aislamiento de red.

7. Guarde los cambios.

[Cómo desactivar Aislamiento de red de un ordenador manualmente]

1. En la ventana principal de Web Console, elija **Dispositivos** > **Dispositivos administrados**.

2. Seleccione el ordenador para el que desea definir la configuración local de la aplicación.

3. Se abren las propiedades del ordenador.

4. Seleccione la pestaña **Aplicaciones**.

5. Haga clic en Kaspersky Endpoint Security for Mac.

6. Se abre la configuración local de la aplicación.

7. Elija la pestaña **Configuración de la aplicación**.

8. Vaya a **Detection and Response** > **Endpoint Detection and Response**.

9. En el bloque de **Aislamiento de red**, haga clic en **Desbloquear el equipo aislado de la red**.

También puede desactivar Aislamiento de red localmente con la línea de comandos.

Exclusiones de Aislamiento de red

Puede configurar exclusiones de Aislamiento de red. Las conexiones de red que coinciden con las reglas no se bloquean en el ordenador cuando Aislamiento de red está activado.

Para configurar las exclusiones de Aislamiento de red, puede utilizar una lista de perfiles de red estándar. De manera predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y las funciones de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones manualmente (consulte las instrucciones a continuación).

Importante: Las exclusiones especificadas en las propiedades de la directiva se aplican solo si Aislamiento de red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del ordenador se aplican solo si Aislamiento de red se activa manualmente en las propiedades del ordenador en la consola de Kaspersky Security Center.

Nota: Una directiva activa no impide aplicar las exclusiones de Aislamiento de red configuradas en las propiedades del ordenador, ya que estos parámetros tienen diferentes escenarios de uso.

[Cómo añadir una exclusión de Aislamiento de red en modo automático]

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.

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

3. Se abre la ventana de propiedades de la directiva.

4. Elija la pestaña **Configuración de la aplicación**.

5. Vaya a **Detection and Response** > **Endpoint Detection and Response**.

6. En el bloque **Exclusiones de Aislamiento de red**, haga clic en **Exclusiones**.

7. Se abre una ventana. En esta ventana, haga clic en **Añadir desde el perfil** y seleccione los perfiles de red estándar para configurar las exclusiones.
8. Las exclusiones de Aislamiento de red del perfil se añaden a la lista de exclusiones de Aislamiento de red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de la conexión de red.
9. Si es necesario, añada una exclusión de Aislamiento de red manualmente. Para hacerlo, en la ventana con la lista de exclusiones, haga clic en **Añadir** y edite manualmente la configuración de la conexión de red.
10. Guarde los cambios.

[Cómo añadir una exclusión de Aislamiento de red en modo manual]

1. En la ventana principal de Web Console, elija **Dispositivos** > **Dispositivos administrados**.
2. Seleccione el ordenador para el que desea definir la configuración local de la aplicación.
3. Se abren las propiedades del ordenador.
4. Seleccione la pestaña **Tareas**.
5. Se muestra la lista de tareas disponibles en el ordenador.
6. Seleccione la tarea **Aislamiento de red**.
7. Elija la pestaña **Configuración de la aplicación**.
8. En la ventana que se abre, haga clic en **Exclusiones**.
9. En la siguiente ventana, haga clic en **Añadir desde el perfil** y seleccione los perfiles de red estándar para configurar las exclusiones.
10. Las exclusiones de Aislamiento de red del perfil se añaden a la lista de exclusiones de Aislamiento de red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de la conexión de red.
11. Si es necesario, añada una exclusión de Aislamiento de red manualmente. Para hacerlo, en la ventana con la lista de exclusiones, haga clic en **Añadir** y edite manualmente la configuración de la conexión de red.
12. Guarde los cambios.

También puede ver la lista de exclusiones de Aislamiento de red localmente mediante la línea de comandos. En este caso, el ordenador debe estar aislado.

Sandbox en la nube

Sandbox en la nube es una tecnología que le permite detectar amenazas avanzadas en un ordenador. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados para analizarse a Sandbox en la nube. Sandbox en la nube ejecuta estos archivos en un entorno aislado para identificar la actividad maliciosa y decide su reputación. Luego, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Sandbox en la nube detecta un archivo malicioso, Kaspersky Endpoint Security realizará la acción apropiada para eliminar la amenaza en todos los equipos en los que se detecte este archivo.

Importante: Para que Sandbox en la nube funcione, debe activar el uso de Kaspersky Security Network.

Nota: Si utiliza Kaspersky Private Security Network, la tecnología de Sandbox en la nube no está disponible.

Para activar Sandbox en la nube, siga estos pasos:

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
5. Active el interruptor **Sandbox en la nube**.

6. Guarde los cambios.

Siempre que existe una amenaza, Kaspersky Endpoint Security activa el contador de amenazas detectadas mediante Sandbox en la nube en la ventana principal de la aplicación de la sección **Detección de amenazas**. Kaspersky Endpoint Security también indica la tecnología de detección de amenazas Sandbox en la nube en el Informe sobre amenazas de la consola de Kaspersky Security Center.

Cifrado de disco de FileVault

Nota: La función de cifrado de disco de FileVault estará disponible en Kaspersky Security Center 10 SP3 Para obtener más información, comuníquese con el Servicio de soporte técnico de Kaspersky.

Kaspersky Endpoint Security permite la administración remota del cifrado de FileVault. El cifrado evita que otros usuarios tengan acceso no autorizado a datos confidenciales almacenados en el disco de inicio del equipo del usuario.

Cuando un administrador inicia el cifrado de FileVault de un equipo desde Kaspersky Security Center, Kaspersky Endpoint Security le solicita al usuario del equipo que introduzca sus credenciales. El cifrado del disco se inicia solo después de que el usuario proporciona las credenciales, se reinicia el ordenador y han pasado 30 minutos desde que se recibieron los ajustes de la directiva en el ordenador. El intervalo mínimo entre las solicitudes de credenciales también es de 30 minutos.

Para evitar que el usuario descifre el disco de inicio del Mac cuando el cifrado de FileVault está activado, un administrador debe usar JAMF para implementar un perfil de MDM que prohíba el descifrado de disco. Para descifrar el disco de inicio de un Mac con un perfil de MDM que prohíbe el descifrado del disco, el administrador primero debe eliminar el perfil.

Nota: Si la administración del cifrado de FileVault no está activada en Kaspersky Security Center, los usuarios con derechos de administrador pueden cifrar y descifrar sus discos de inicio de Mac desde Ajustes del sistema. Para obtener más información sobre FileVault, consulte la documentación de Apple.

Si el equipo tiene varias cuentas, el cifrado de FileVault hace que el disco sea inaccesible para todos los usuarios, excepto para el que introdujo las credenciales.

Permitir que otros usuarios desbloqueen el disco

1. Escoja el **menú Apple** > **Ajustes del sistema** > **Privacidad y seguridad**.
2. Haga clic en **FileVault**.
   Se abrirá la ventana **FileVault**.
3. Haga clic en **Activar usuarios**.
4. En la ventana que se abre, elija un usuario para autorizar el desbloqueo del equipo.
5. Introduzca la contraseña de la cuenta del equipo del usuario y haga clic en **Aceptar**.
6. Haga clic en **Continuar**.

El usuario puede acceder al disco cifrado.

Nota: Se requieren derechos de administrador para permitir que otros usuarios desbloqueen el disco.

Si un administrador administra Kaspersky Endpoint Security a través de la Consola de administración de Kaspersky Security Center, Web Console o Cloud Console y un usuario de este equipo se olvida o pierde sus credenciales y no puede acceder a un disco cifrado, el administrador puede obtener una clave de recuperación.

Cómo obtener una clave de recuperación mediante la Consola de administración de Kaspersky Security Center

Cómo obtener una clave de recuperación mediante Kaspersky Security Center Web Console y Cloud Console

Protección con contraseña

Kaspersky Endpoint Security permite limitar las acciones no deseadas en los dispositivos de los usuarios al establecer una contraseña de administrador.

Si la protección con contraseña está activada, Kaspersky Endpoint Security requiere una contraseña cuando se intenta realizar cualquiera de las siguientes acciones:

- Definir la configuración de la aplicación

- Salir de la aplicación
- Eliminar la clave de licencia
- Eliminar la aplicación

  Nota: La protección con contraseña restringe la eliminación de Kaspersky Endpoint Security solo cuando se realiza a través del programa de desinstalación.

- Restaurar archivos en cuarentena desde Copia de seguridad
- Ver informes.

Desactivar la protección con contraseña no desactiva la configuración de la directiva. Si la modificación de una configuración está prohibida en la directiva, no se puede editar incluso si la protección con contraseña está desactivada.

Activar la protección con contraseña mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, seleccione la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y seleccione **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Configuración adicional > Interacción con el usuario**.
7. En la sección **Protección con contraseña**, seleccione la casilla de verificación **Activar la protección con contraseña**.
8. En la ventana **Configuración de la protección con contraseña** que se abre, configure lo siguiente:
   - Introduzca la contraseña en el campo **Contraseña** y vuelva a introducirla en el campo **Confirmar contraseña**.
   - En la sección **Solicitar contraseña para**, seleccione las casillas requeridas para proteger las acciones correspondientes en el dispositivo del usuario.
9. Haga clic en **Aceptar** para guardar los cambios.
10. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
    - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
    - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** tras guardar los cambios.

Editar la configuración de protección con contraseña mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, seleccione la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y seleccione **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Configuración adicional > Interacción con el usuario**.
7. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
8. En la ventana **Configuración de la protección con contraseña** que se abre, edite la configuración que desea cambiar.
9. Haga clic en **Aceptar** para guardar los cambios.

Activar la protección con contraseña mediante Web Console

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
3. Se abre la ventana de propiedades de la directiva.
4. Seleccione la pestaña **Configuración de la aplicación**.
5. Seleccione **Ajustes adicional** > **Interacción con el usuario**.
6. Active el interruptor **Protección con contraseña**.
7. En el cuadro de diálogo **Configuración de la protección con contraseña** que se abre, configure lo siguiente:
   - Introduzca la contraseña en el campo **Contraseña** y vuelva a introducirla en el campo **Confirmar contraseña**. De forma predeterminada, los caracteres de la contraseña están ocultos por motivos de seguridad. Para ver la contraseña, haga clic en **Mostrar**.
   - En la sección **Solicitar contraseña para**, seleccione las casillas requeridas para proteger las acciones correspondientes en el dispositivo del usuario.
8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración de la protección con contraseña**.
9. Haga clic en **Aceptar** para cerrar la sección **Interacción con el usuario**.
10. Haga clic en **Guardar** para guardar los cambios en la directiva.

Editar la protección con contraseña mediante Web Console

1. En la ventana principal de Web Console, elija **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
3. Se abre la ventana de propiedades de la directiva.
4. Seleccione la pestaña **Configuración de la aplicación**.
5. Seleccione **Ajustes adicional** > **Interacción con el usuario**.
6. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
7. En el cuadro de diálogo **Configuración de la protección con contraseña** que se abre, edite la configuración que desea cambiar.
8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración de la protección con contraseña**.
9. Haga clic en **Aceptar** para cerrar la sección **Interacción con el usuario**.
10. Haga clic en **Guardar** para guardar los cambios en la directiva.

Activar la protección con contraseña mediante la aplicación Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Interfaz**, en la sección **Protección con contraseña**, seleccione la casilla **Activar la protección con contraseña**.
3. En la ventana que se abre, configure los siguientes ajustes:
   - Introduzca la contraseña en el campo **Contraseña** y vuelva a introducirla en el campo **Confirmar contraseña**.
   - En la sección **Solicitar contraseña para**, seleccione las casillas requeridas para proteger las acciones correspondientes en el dispositivo del usuario.
4. Haga clic en **Aceptar**.

Nota: Si selecciona **Cambiar la configuración de la aplicación** como acción protegida con contraseña, debe introducir la contraseña dos veces para cambiar la configuración de protección con contraseña.

Editar la protección con contraseña mediante la aplicación Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Interfaz**, en la sección **Protección con contraseña**, haga clic en **Ajustes**.
3. En la ventana que se abre, edite la configuración que desea cambiar.
4. Haga clic en **Aceptar**.

Prevención de exploits

El componente Prevención de exploits detecta el código del programa que aprovecha las vulnerabilidades en el equipo para explotar los privilegios de administrador o realizar actividades maliciosas. Por ejemplo, los exploits pueden utilizar un ataque de desbordamiento de búfer. Para hacerlo, el exploit envía una gran cantidad de datos a una aplicación vulnerable. Al procesar estos datos, la aplicación vulnerable ejecuta un código malicioso. Como resultado de este ataque, el exploit puede iniciar una instalación no autorizada de software malicioso. Cuando hay un intento de ejecutar un archivo ejecutable desde una aplicación vulnerable que no fue realizado por el usuario, Kaspersky Endpoint Security bloquea la ejecución de este archivo o notifica al usuario.

De manera predeterminada, la Prevención de exploits está activada. Puede desactivar la Prevención de exploits si es necesario.

Activar/desactivar la Prevención de exploits mediante Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas avanzadas** > **Prevención de exploits**.
5. Active/desactive el interruptor de **Prevención de exploits**.
6. Si la Prevención de exploits está activada, seleccione una de las siguientes acciones que se realizarán cuando se detecte un exploit:
   - Bloquear
     Si se selecciona esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea las operaciones de este exploit y realiza una entrada de registro con información sobre él.
   - Informar
     Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un exploit, registra una entrada que contiene información sobre el exploit y añade información sobre él a la lista de amenazas activas.
7. Guarde los cambios.

Activar/desactivar la Prevención de exploits mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, seleccione la pestaña **Directivas**.

5. Haga clic derecho en la directiva que desea configurar y seleccione **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Protección frente a amenazas avanzada** > **Prevención de exploits**.
7. Seleccione o anule la selección de la casilla **Prevención de exploits**.
8. Si es necesario, en la sección **Sobre la detección de exploits**, seleccione la acción que se realizará cuando Kaspersky Endpoint Security detecte un exploit.
9. Haga clic en **Aceptar** para guardar los cambios.
10. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
    - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
    - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** tras guardar los cambios.

Activar/desactivar la Prevención de exploits mediante la aplicación Kaspersky Endpoint Security

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Avanzado**, en la sección Prevención de exploits, seleccione o anule la selección de la casilla Activar la Prevención de exploits.
3. Si la casilla **Activar Detección de comportamiento** está seleccionada, seleccione una de las siguientes acciones que se realizarán cuando se detecte actividad de malware:
   - Bloquear de forma automática la actividad de software malicioso que presente un peligro
     Si se selecciona esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea las operaciones de este exploit y realiza una entrada de registro con información sobre él.
   - Informar
     Si se selecciona esta opción, cuando Kaspersky Endpoint Security detecta un exploit, registra una entrada que contiene información sobre el exploit y añade información sobre él a la lista de amenazas activas.

Ver el informe de Prevención de exploits

1. En la barra de menús, elija **Protección** > **Informes**.
   Se abre la ventana **Informes**.
2. Abra la pestaña **Prevención de exploits**.

Motor de reparación

El Motor de reparación permite que Kaspersky Endpoint Security revierta las acciones realizadas por malware en el sistema operativo.

Al revertir la actividad de malware en el sistema operativo, Kaspersky Endpoint Security maneja los siguientes tipos de actividad de malware:

- **Actividad de archivos**
  Kaspersky Endpoint Security realiza las siguientes acciones:
  - Elimina archivos ejecutables creados por malware (en todos los medios, excepto en las unidades de red).
  - Elimina archivos ejecutables que crearon programas infiltrados por malware.
  - Restaura archivos modificados o eliminados por malware.
- **Actividad del sistema**
  Kaspersky Endpoint Security realiza las siguientes acciones:
  - Finaliza los procesos iniciados por malware.

- Finaliza los procesos en los que penetró una aplicación maliciosa.
- No reanuda los procesos que fueron detenidos por malware.

- **Actividad de red**
  Kaspersky Endpoint Security realiza las siguientes acciones:
  - Bloquea la actividad de red del malware.

La reversión de acciones de malware puede iniciarse mediante los componentes Protección contra amenazas de archivos o Detección de comportamiento, o durante un análisis de malware.

La reversión de las operaciones de malware afecta un conjunto de datos estrictamente definido. La reversión no tiene efectos adversos en el sistema operativo ni en la integridad de los datos del ordenador.

Activar/desactivar el Motor de reparación en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, elija la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, elija **Protección frente a amenazas avanzada** > **Motor de reparación**.
7. Active o desactive la selección de la casilla **Motor de reparación**.
8. Haga clic en **Aceptar** para guardar los cambios.
9. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.

Activar/desactivar el Motor de reparación en Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección frente a amenazas avanzadas** > **Motor de reparación**.
5. Active/desactive el interruptor**Motor de reparación**.
6. Guarde los cambios.

Activar/desactivar el Motor de reparación en la interfaz de la aplicación

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Avanzado**, en la sección **Motor de reparación**, active o desactive la selección de la casilla Activar el Motor de reparación.

Como resultado, si el Motor de reparación está activado, Kaspersky Endpoint Security revierte las acciones realizadas por las aplicaciones maliciosas en el sistema operativo.

Control web

Control web administra el acceso de los usuarios a los recursos web. Esto permite reducir el tráfico y el uso inadecuado del tiempo de trabajo. Cuando un usuario intenta abrir un sitio web restringido por Control web, Kaspersky Endpoint Security bloquea el acceso o muestra una advertencia.

Puede bloquear el acceso a sitios web específicos o categorías seleccionadas de sitios web.

Nota: La aplicación de Kaspersky Endpoint Security solo puede bloquear el acceso a sitios web que usan HTTPS para las conexiones. La aplicación analiza las conexiones cifradas (HTTPS) solo si está seleccionada la casilla **Comprobar conexiones seguras (HTTPS)** en la sección **General** de la pestaña **Protección**.

Añadir una nueva regla en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, elija la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, elija **Controles de seguridad** > **Control web**.
7. Elija la casilla **Activar Control web**.
8. Haga clic en **Añadir**.
9. En la ventana que se abre, introduzca el nombre de una regla.
10. Si desea que la regla esté activa, elija la casilla **Regla activa**.
11. Realice una de las siguientes acciones:
    - Si desea que la regla se aplique a direcciones web específicas, elija la opción **Una dirección web o un grupo de direcciones web mediante máscara**.
    - Si desea que la regla se aplique a categorías específicas de sitios web, elija la opción **Categorías de sitios web**.
12. Haga clic en **Especificar**.
13. En la ventana que se abre, configure el alcance de la regla.
14. Realice una de las siguientes acciones:
    - Si desea que Kaspersky Endpoint Security bloquee el acceso, elija la opción **Bloquear**.
    - Si desea que Kaspersky Endpoint Security permita el acceso, elija la opción **Permitir**.
    - Si desea que Kaspersky Endpoint Security muestre una advertencia, elija la opción **Mostrar advertencia**.
15. Haga clic en **Aceptar** para guardar los cambios.
16. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
    - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
    - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.

Añadir una nueva regla en Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.

4. Vaya a **Controles de seguridad** > **Control web**.
5. Active el interruptor **Control web**.
6. Haga clic en **Agregar**.
7. En la ventana que se abre, introduzca el nombre de una regla.
8. Realice una de las siguientes acciones:
   - Si desea que la regla esté activa, elija la opción **Activa**.
   - Si desea que la regla esté inactiva, elija la opción **Inactiva**.
9. Realice una de las siguientes acciones:
   - Si desea que Kaspersky Endpoint Security permita el acceso, elija la opción **Permitir**.
   - Si desea que Kaspersky Endpoint Security bloquee el acceso, elija la opción **Bloquear**.
   - Si desea que Kaspersky Endpoint Security muestre una advertencia, elija la opción **Mostrar advertencia**.
10. Realice una de las siguientes acciones:
    - Si desea que la regla se aplique a categorías específicas de sitios web, elija la opción **Categorías** y haga clic en **Seleccionar categorías** para elegir las categorías.
    - Si desea que la regla se aplique a direcciones web específicas, elija la opción **Dirección particular** y añádalas a la tabla a continuación.
11. Guarde los cambios.

Nota: La configuración de Control web no se puede administrar en la aplicación de Kaspersky Endpoint Security.

Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a los dispositivos que están instalados o conectados al ordenador. Esto le permite proteger el ordenador de infecciones cuando dichos dispositivos están conectados y evitar pérdidas o fugas de datos.

Niveles de acceso a los dispositivos

Control de dispositivos controla el acceso en los siguientes niveles:

- **Tipo de dispositivo**. Por ejemplo, impresoras, unidades extraíbles y unidades de CD/DVD.

  Puede configurar el acceso a los dispositivos de la siguiente manera:
  - Permitir.
  - Bloquear.
  - Bloquear con excepciones (solo Wi-Fi).
- **Dispositivos de confianza.** Los dispositivos de confianza son dispositivos a los que los usuarios especificados en la configuración del dispositivo de confianza tienen acceso completo en todo momento.

  Puede añadir dispositivos de confianza sobre la base de los siguientes datos:
  - **Dispositivos por Id**. Cada dispositivo tiene un identificador único (Id. de hardware o HWID). Puede ver el ID en las propiedades del dispositivo usando herramientas del sistema operativo. Ejemplo de Id. de dispositivo: SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000. Añadir dispositivos por ID es conveniente si desea añadir varios dispositivos específicos.
  - **Dispositivos por modelo**. Cada dispositivo tiene un Id. de proveedor (VID) y un Id. de producto (PID). Puede ver los Id. en las propiedades del dispositivo mediante las herramientas del sistema operativo. Plantilla para introducir el VID y PID: VID_1234&PID_5678. Añadir dispositivos por modelo es conveniente si usa dispositivos de un determinado modelo en su organización. De esta manera, puede añadir todos los dispositivos de este modelo.
  - **Dispositivos por máscara de Id**. Si está usando varios dispositivos con Id. similares, puede añadir dispositivos a la lista de confianza mediante las máscaras. El carácter `*` reemplaza cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `WDC_C*`.

- **Dispositivos por modelo de máscara**. Si está usando varios dispositivos con VID o PID similares (por ejemplo, dispositivos del mismo fabricante), puede añadir dispositivos a la lista de confianza mediante las máscaras. El carácter `*` reemplaza cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al introducir una máscara. Por ejemplo, `VID_05AC y PID_*`.

Administrar el componente Control de dispositivos en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, elija la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, elija **Controles de seguridad** > **Control de dispositivos**.
7. Elija la casilla **Control de dispositivos**.
8. En la pestaña **Tipos de dispositivos**, configure las reglas de acceso para los tipos de dispositivos y las redes Wi-Fi.
9. En la pestaña **Dispositivos de confianza**, configure las reglas de acceso para dispositivos individuales o grupos de dispositivos.
10. Haga clic en **Aceptar** para guardar los cambios.
11. Realice alguna de las siguientes acciones para aplicar los cambios en la directiva:
    - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.
    - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la directiva>** después de guardar los cambios.

Administrar el componente Control de dispositivos en Web Console

1. En la ventana principal de Web Console, elija **Activos (Dispositivos)** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Elija la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad** > **Control de dispositivos**.
5. Active el interruptor **Control de dispositivos**.
6. En la sección **Configuración de Control de dispositivos**, configure las reglas de acceso para los dispositivos, los tipos de dispositivos y las redes Wi-Fi.
7. Guarde los cambios.

Nota: La configuración de Control de dispositivos no se puede administrar en la aplicación de Kaspersky Endpoint Security.

Como resultado, si Control de dispositivos está activado, la aplicación transmite información sobre los dispositivos conectados a Kaspersky Security Center. Puede ver la lista de dispositivos conectados en Kaspersky Security Center en la carpeta **Avanzado → Repositorios → Hardware**.

Ver el informe de Control de dispositivos

1. En la barra de menús, elija **Protección** > **Informes**.
   Se abre la ventana **Informes**.
2. Abra la pestaña **Control de dispositivos**.

Participación en Kaspersky Security Network

Cuando participa en Kaspersky Security Network las estadísticas de la aplicación Kaspersky Endpoint Security se envían automáticamente a Kaspersky para mejorar la protección de su Mac.

Nota: Kaspersky no recibe, procesa ni almacena datos personales sin su consentimiento explícito.

La participación en Kaspersky Security Network es voluntaria. La decisión de participar se toma al instalar la aplicación. No obstante, podrá cambiar de opinión más adelante en cualquier momento.

Activar Kaspersky Security Network

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.

   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Avanzado**, en la sección **KSN**, haga clic en **Mostrar la Declaración de KSN** para ver la Declaración de Kaspersky Security Network.

3. Si desea que Kaspersky Endpoint Security utilice información sobre la reputación de los archivos, los recursos web y las aplicaciones recibidas de Kaspersky Security Network y acepta todos los términos de la Declaración, seleccione la casilla de verificación **Participar en Kaspersky Security Network**.

4. En la ventana que se abre, haga clic en **Confirmar**.

Se seleccionarán las casillas de verificación **Participar en Kaspersky Security Network** y **Activar modo KSN extendido**.

Nota: De forma predeterminada, Kaspersky Endpoint Security utiliza el modo KSN extendido. *El modo KSN extendido* es un modo en el que Kaspersky Endpoint Security envía datos adicionales a Kaspersky. Si no desea proporcionar estos datos a Kaspersky, desmarque la casilla de verificación **Activar modo KSN extendido**.

Datos proporcionados a Kaspersky cuando usa Kaspersky Security Network

Si la casilla de verificación **Participar en Kaspersky Security Network** está seleccionada y la casilla de verificación **Activar modo KSN extendido** no está seleccionada, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Versión completa del software instalado;

  tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. de dispositivo único; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

Si las casillas de verificación **Participar en Kaspersky Security Network** y **Activar modo KSN extendido** están seleccionadas, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información sobre la versión del sistema operativo (SO) y los paquetes de servicios instalados en el ordenador, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del sistema operativo y los parámetros del modo de ejecución del sistema operativo; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO; versión de Service Pack del SO; fecha y hora de inicio del SO; tiempo de demora del procesamiento del evento acerca de la acción del SO en el subsistema de análisis de comportamiento; cantidad de eventos de acción del tipo actual demorados del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactiva; cantidad de eventos de acciones del SO

procesados; cantidad de eventos de acción sincrónicos procesados del SO; demora total de todos los eventos de acción del tipo actual del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento de eventos persistentes; demora total de todos los eventos de acción del SO; cantidad de eventos de acción sincrónicos del SO en espera; fecha y hora del evento recibido por una acción en el SO.

- Información sobre el último reinicio fallido del sistema operativo: número de reinicios fallidos.

- Información sobre la aplicación instalada del Titular de los derechos y el estado de la protección antivirus: id. de instalación del software (PCID); versión del registro de la base de datos del software; el identificador único de la instancia de la instalación de la aplicación en el ordenador, el tipo de aplicación, id. del tipo de aplicación, la versión completa de la aplicación instalada, el identificador de la versión de configuración de la aplicación, el identificador del tipo de ordenador, el identificador único del ordenador en el que está instalada la aplicación, el identificador de Usuario único en los servicios del Titular de los derechos, el idioma regional y el estado de funcionamiento, la versión de los componentes de Software instalados y su estado de funcionamiento, la versión del protocolo utilizado para conectarse con los servicios del Titular de los derechos; versión completa del software instalado; tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); cantidad de ciclos de actualizar y aplicar para bases de datos antivirus; fecha y hora de la última actualización y aplicación de las bases de datos antivirus; Fecha y hora de lanzamiento de las bases de datos del software; versión del componente del Software; id. de actualización de software; tipo del software instalado; fecha y hora de inicio de System Watcher; fecha y hora de instalación del software; probabilidad de enviar estadísticas por medio de System Watcher; código del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo máximo permitido para el procesamiento de un evento por parte de System watcher; tiempo de procesamiento del evento que tardó más tiempo del estándar en ser procesado por System Watcher; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por System Watcher.

- Información sobre todos los objetos y operaciones procesados: veredicto del software del objeto que se procesa; código de directorio; tamaño del objeto que se procesa; suma de control (SHA256) del objeto que se procesa; número del software detectado en el contexto de System Watcher; fecha y hora de detección de software por parte de System Watcher; detectar características; ID del registro activado en las bases de datos Antivirus del software; motivo de detección de software por System Watcher; suma de control (MD5) del objeto que se procesa; resultado de la comprobación de integridad del módulo; nombre del objeto que se procesa; tipo de registro en las bases de datos antivirus del software activado; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; la dirección URL y del referente desde las que se descargó; el tamaño de los archivos analizados y las rutas hasta ellos; la señal del archivo; la fecha y la hora de creación del archivo; el nombre, el tamaño y las sumas de control (MD5, SHA2-256) del compresor (si el archivo estaba comprimido); la entropía del archivo; el tipo de archivo; el código de tipo de archivo; la señal, el ID y el formato del archivo ejecutable; la suma de control del objeto (MD5, SHA2-256); el tipo y el valor de la suma de control complementaria del objeto; datos sobre la firma digital (certificado) del objeto: datos sobre el editor del certificado, número de inicios del objeto desde el envío de la última estadística, ID de la tarea de análisis de la aplicación, los medios para recibir información sobre la reputación del objeto, el valor del filtro de destino, los parámetros técnicos de las tecnologías de detección aplicables; ruta hacia el objeto que se procesa; código de directorio.

- Para archivos ejecutables: la entropía de las secciones del archivo, la marca de verificación de reputación o la marca de la firma del archivo, el nombre, el tipo, el tipo de ID, la suma de comprobación (MD5) y el tamaño de la aplicación cargada por el objeto que se está validando, la ruta de la aplicación y las rutas de las plantillas, un atributo que indica la presencia de la lista de autoejecución, la fecha de entrada, la lista de atributos, el nombre del compresor e información sobre la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME y la fecha y hora de creación del archivo.

- Información sobre las aplicaciones iniciadas y sus módulos: sumas de comprobación (MD5, SHA2-256) de los archivos en ejecución, tamaño, atributos, fecha de creación, nombre del compresor (si el archivo estaba comprimido), nombres de los archivos, información sobre los procesos que se ejecutan en el sistema (identificación del proceso [PID]), nombre del proceso, información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, la ruta completa a los archivos del proceso y la línea de comandos de inicio, una descripción de la aplicación a la que pertenece el proceso (el nombre de la aplicación e información sobre el editor), así como los certificados digitales que se usan e información necesaria para verificar su autenticidad o información sobre la ausencia de firma digital de un archivo e información sobre los módulos cargados en los procesos: sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación (MD5, SHA2-256, SHA1); las rutas a ellos; la información del encabezado de archivo PE; los nombres de los compresores (si se comprimió el archivo); la información sobre la disponibilidad y validez de estas estadísticas y el identificador del modo para generar las estadísticas que se envían.

- En caso de detectar una amenaza o vulnerabilidad, además de la información sobre el objeto escaneado se deberá proporcionar información sobre el identificador, la versión y el tipo de registro en la base de datos del antivirus; el nombre de la amenaza según la clasificación de Kaspersky, la fecha y la hora de la última actualización de la base de datos del antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de aplicación que solicitó la URL y en la cual ocurrió la detección; la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador del tipo de tráfico en el cual fue detectada la amenaza, el identificador de vulnerabilidad y el nivel de la amenaza recibida, la dirección URL y de referencia de la página web en la cual fue detectada la vulnerabilidad.

- Si se detectase un objeto potencialmente malicioso, se proveerá información sobre los datos contenidos en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo que realiza el ataque y número del puerto del equipo del usuario víctima del ataque de red, ID del protocolo de ataque, y nombre y tipo de ataque.

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

- El URL y la dirección IP del sitio web en el cual fue detectado el contenido malicioso o sospechoso; nombre, dimensión y suma de chequeo del archivo que solicitó dicho URL; identificador, peso y grado de aplicación de la norma establecida para dar el veredicto y objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: el estado de finalización de la tarea de actualización, el tipo de error que podría haber ocurrido durante el proceso de actualización, el número de actualizaciones fallidas y el identificador del componente de la aplicación que realiza las actualizaciones.

- Información acerca del uso de Kaspersky Security Network (KSN): el identificador de KSN, el identificador de la aplicación, la versión completa de la aplicación, la dirección IP impersonal del dispositivo del usuario, indicadores del nivel de satisfacción de las solicitudes de KSN, indicadores de la calidad de procesamiento de paquetes de KSN, indicadores del número de solicitudes de KSN e información sobre los tipos de solicitudes de KSN, fecha y hora en que se inició el envío de estadísticas, fecha y hora en que finalizó el envío de estadísticas, información sobre actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida y código de error de la actualización de la configuración.

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se ha detectado el evento, tipo y categoría de evento, nombre de la fuente del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la cual se solicita la reputación y el Referente, la conexión del tipo de protocolo de la conexión, el identificador interno del tipo de aplicación, el número del puerto usado, el identificador del Usuario, la suma de comprobación del archivo escaneado (MD5), el tipo de amenaza detectada, información sobre el registro usado para detectar una amenaza (el identificador del registro para las bases de datos antivirus, el registro de la marca de tiempo y el tipo); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

- Datos sobre la distribución territorial de la aplicación: la fecha de la instalación y activación de la aplicación, el ID del partner que proporciona la licencia para la activación de la aplicación, el ID de la aplicación, el ID de localización de idioma de la aplicación, el número de serie de la licencia de activación de la aplicación y el indicio de participación en KSN.

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Información sobre el hardware instalado en el equipo: tipo, nombre, nombre del modelo, versión de firmware y parámetros de los dispositivos integrados y conectados.

- Información sobre el dispositivo: ID de dispositivo.

- Información sobre el funcionamiento del componente Control web:

  la versión del componente, el motivo de la categorización, información adicional sobre el motivo de la categorización, la URL categorizada y la dirección IP de host de objeto bloqueado/categorizado.

Nota: Según la configuración de Kaspersky Security Center, puede participar en Kaspersky Private Security Network en lugar de Kaspersky Security Network. Kaspersky Endpoint Security le notifica cuando pasa de Kaspersky Private Security Network a Kaspersky Security Network y le pide que acepte las condiciones de la Declaración de Kaspersky Security Network. Para obtener información detallada sobre la participación en Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center.

Infraestructura de Kaspersky Security Network

Kaspersky Endpoint Security es compatible con las siguientes soluciones de infraestructura de Kaspersky Security Network:

- *KSN Global* es la solución utilizada por la mayoría de las aplicaciones de Kaspersky. Los participantes de KSN reciben información de Kaspersky Security Network y envían información de Kaspersky acerca de objetos detectados en el equipo del usuario a analistas de Kaspersky para un análisis adicional, que se incluye en las bases de datos de reputación y estadística de Kaspersky Security Network.

- *KSN privada* es una solución que permite a los usuarios de equipos que alojan Kaspersky Endpoint Security o alguna otra aplicación de Kaspersky obtener acceso a las bases de datos de reputación de Kaspersky, así como otras estadísticas, sin enviar datos a Kaspersky Security Network desde sus propios equipos. KSN privada está diseñada para clientes corporativos que no pueden participar en Kaspersky Security Network por alguna de las siguientes razones:

  - Las estaciones de trabajo locales no están conectadas a Internet.

  - La transmisión de cualquier dato fuera del país o de la LAN corporativa se encuentra prohibida por ley o restringida por directivas de seguridad corporativas.

De forma predeterminada, Kaspersky Security Center utiliza KSN Global. Puede configurar el uso de KSN privada en la Consola de administración de Kaspersky Security Center (MMC) y Kaspersky Security Center Web Console. No es posible configurar el uso de KSN privada en Kaspersky Security Center Cloud Console.

Proxy de KSN

Los equipos administrados por el Servidor de administración de Kaspersky Security Center pueden interactuar con Kaspersky Security Network a través del servicio de proxy de KSN.

El servicio de proxy de KSN proporciona las siguientes capacidades:

- El equipo del usuario puede realizar una búsqueda en KSN y enviar información a KSN incluso sin un acceso directo a Internet.
- El servicio de proxy de KSN almacena datos procesados en caché, lo que reduce la carga del canal de comunicación de la red externa y acelera la recepción de información solicitada por el equipo del usuario.

Para obtener más detalles sobre el servicio de proxy de KSN, consulte la Ayuda de Kaspersky Security Center.

Nota: La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y las actualizaciones de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Comprobar la integridad de los componentes de la aplicación

Kaspersky Endpoint Security contiene varios módulos binarios en forma de bibliotecas dinámicas vinculadas, archivos ejecutables, archivos de configuración y archivos de interfaz. Los intrusos pueden reemplazar uno o más módulos o archivos ejecutables de la aplicación por otros archivos que contengan código malicioso. Para evitar esto, Kaspersky Endpoint Security puede comprobar la integridad de los componentes de la aplicación. La aplicación comprueba los módulos y archivos en busca de cambios no autorizados o daños. Si un módulo o archivo de la aplicación tiene una suma de comprobación incorrecta, se considera que está dañado.

La integridad de los componentes de la aplicación se comprueba mediante la utilidad Integrity_checker que se encuentra en el directorio /Library/Application Support/Kaspersky Lab/KAV/Binaries. Esta utilidad comprueba la integridad del archivo de manifiesto que contiene una lista de archivos de la aplicación cuya integridad es crítica para el correcto funcionamiento del componente de la aplicación.

El archivo de manifiesto Integrity_check.xml, que está protegido por la firma criptográfica de Kaspersky, está ubicado en el mismo directorio que la utilidad integrity_check (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Nota: Se necesitan privilegios de cuenta de usuario raíz para ejecutar la utilidad integrity_checker.

La comprobación de integridad se puede realizar con la utilidad que se instala junto con la aplicación o mediante la utilidad en un CD certificado.

Para comprobar la integridad de los componentes de la aplicación, ejecute el siguiente comando:

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

De manera predeterminada, la utilidad usa el archivo integrity_check.xml ubicado en el directorio /Library/Application Support/Kaspersky Lab/KAV/Binaries.

Para mostrar la Ayuda de la configuración de la utilidad, ejecute el siguiente comando:

```
--help
```

El resultado de comprobar cada archivo de manifiesto se muestra junto al nombre del archivo de manifiesto en el siguiente formato:

- `SUCCEEDED`: se confirma la integridad de los archivos (código de retorno `0`)
- `FAILED`: la integridad de los archivos no está confirmada (el código de retorno no es `0`)

Administración de la aplicación mediante la Consola de administración de Kaspersky Security Center

Kaspersky Security Center está diseñado para administrar de forma centralizada la seguridad de redes corporativas. Para obtener información detallada sobre Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

También puede administrar Kaspersky Endpoint Security a través de la interfaz gráfica de usuario de la aplicación, Kaspersky Security Center Web Console y Cloud Console, y la línea de comandos.

Implementar Kaspersky Endpoint Security en una red corporativa

1. Despliegue el *Servidor de administración* en la red.

   El Servidor de administración es un componente de Kaspersky Security Center que almacena de forma centralizada información de todas las aplicaciones de Kaspersky instaladas en la red corporativa para administrarlas.

2. Instale la *Consola de administración* en la estación de trabajo del administrador de Kaspersky Security Center.

   La Consola de administración es un componente de Kaspersky Security Center que ofrece una interfaz de usuario para los servicios administrativos del Servidor de administración y del *Agente de red*. El Agente de red coordina la interacción entre el Servidor de administración y Kaspersky Endpoint Security instalados en equipos dentro de la red corporativa.

3. Instale el complemento de administración de Kaspersky Endpoint Security en la estación de trabajo del administrador de Kaspersky Security Center.

   Un *complemento de administración* es un componente especializado que ofrece una interfaz que permite administrar aplicaciones de Kaspersky a través de la Consola de administración. Cada aplicación tiene su propio complemento de administración. El complemento de administración se proporciona para todas las aplicaciones de Kaspersky que se pueden administrar desde Kaspersky Security Center.

4. Puede instalar el Agente de red en equipos Mac remotos mediante uno de los siguientes métodos:

   - Localmente
   - Remotamente con Apple Remote Desktop
   - Remotamente a través de Kaspersky Security Center
   - Uso remoto del protocolo SSH

   Nota: Para administrar Kaspersky Endpoint Security for Mac 12.2 a través de Kaspersky Security Center, debe instalar el Agente de red versión 15 en los equipos remotos.

5. Puede instalar Kaspersky Endpoint Security en equipos Mac remotos mediante uno de los siguientes métodos:

   - Localmente
   - Remotamente con Apple Remote Desktop
   - Uso remoto del protocolo SSH
   - Remotamente a través de Kaspersky Security Center

   Importante: Si Kaspersky Internet Security for Mac o el software anti software malicioso de un tercero están instalados en equipos remotos, desinstálelos antes de instalar Kaspersky Endpoint Security.

Para obtener información detallada sobre el despliegue del Servidor de administración y la instalación de la Consola de administración, consulte la Ayuda de Kaspersky Security Center.

Actualizar Kaspersky Endpoint Security versión 11.1 o posterior a la versión 12.2

Nota: Para administrar Kaspersky Endpoint Security for Mac 12.2 a través de Kaspersky Security Center, debe instalar el Agente de red versión 15 en los equipos remotos.

Puede actualizar Kaspersky Endpoint Security administrado a través de Kaspersky Security Center de la versión 11.1 o posterior a la versión 12.2 de una de las siguientes maneras:

- Actualice simultáneamente Kaspersky Endpoint Security a la versión 12.2 y el Agente de red a la versión 15 en los equipos remotos.
- Primero actualice el Agente de red a la versión 15 y después actualice Kaspersky Endpoint Security a la versión 12.2.

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

- Para actualizar Kaspersky Endpoint Security a la versión 12.2, se necesita macOS 12 o posterior.
- Debe descargar el archivo KES_11.3_profile.zip desde el sitio web de Soporte técnico para aplicar el nuevo perfil de configuración.
- Después de actualizar Kaspersky Endpoint Security a la versión 12.2, es posible que aparezcan dos elementos de Kaspersky Filter y de Kaspersky Monitor en la configuración de red.

- Si tiene Kaspersky Endpoint Security versión 11.0.1 o anterior, para actualizar la aplicación a la versión 12.2, debe desinstalar la aplicación y actualizar macOS a la versión 12 o posterior. Luego, puede instalar Kaspersky Endpoint Security versión 12.2.

Nota: La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y las actualizaciones de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Prepárese para la instalación remota de Kaspersky Endpoint Security

Esta sección contiene información sobre la instalación del complemento de administración de Kaspersky Endpoint Security en la estación de trabajo del administrador de Kaspersky Security Center y la instalación del Agente de red en el equipo remoto.

La instalación del complemento de administración de Kaspersky Endpoint Security y del Agente de red es un prerrequisito para la instalación de Kaspersky Endpoint Security a través de Kaspersky Security Center.

Instalación del complemento de administración de Kaspersky Endpoint Security

El complemento de administración de Kaspersky Endpoint Security proporciona una interfaz para la administración de Kaspersky Endpoint Security a través de la Consola de administración.

Instalación del complemento de administración de Kaspersky Endpoint Security

1. En la estación de trabajo del administrador de Kaspersky Security Center, descomprima el archivo con los archivos del paquete de instalación de Kaspersky Endpoint Security.
2. Abra la carpeta que contiene los archivos del paquete de instalación de Kaspersky Endpoint Security.
3. Haga doble clic en klcfginst.exe.

Se iniciará la instalación del complemento de administración de Kaspersky Endpoint Security.

Importante: Antes de instalar el complemento de administración de Kaspersky Endpoint Security, cierre la Consola de administración de la estación de trabajo del administrador de Kaspersky Security Center.

Instalación del Agente de red de forma local

El Agente de red coordina la interacción entre el Servidor de administración y Kaspersky Endpoint Security instalados en equipos dentro de la red corporativa.

Instalación del Agente de red de forma local

1. En el equipo remoto, abra la carpeta con el kit de distribución del Agente de red.
2. Abra el kit de distribución del Agente de red (archivo DMG).
   Se abrirá una ventana con los contenidos del kit de distribución.
3. En la ventana con el contenido del kit de distribución, haga doble clic en **Kaspersky Network Agent**.
4. Para confirmar que desea instalar el Agente de red, haga clic en **Continuar**.
5. En la ventana **Presentación**, haga clic en **Continuar**.
6. En la ventana **Licencia**, lea el texto del Contrato de licencia de usuario final del Agente de red entre usted y AO Kaspersky Lab y siga los pasos indicados a continuación:
   - Para aceptar todos los términos del contrato y seguir con la instalación, haga clic en **Continuar**.
   - Para imprimir el texto del contrato, haga clic en **Imprimir**.
   - Para guardar el contrato como archivo de texto, haga clic en **Guardar**.
7. En la ventana de confirmación, realice una de las siguientes acciones:
   - Para continuar con la instalación del Agente de red, haga clic en **Acepto**.

- Para volver a ver el texto del Contrato de licencia de usuario final, haga clic en **Leer licencia**.
- Para cancelar la instalación, haga clic en **No acepto**.

8. En la ventana **Ajustes**, haga lo siguiente:
   a. En el campo **Servidor**, especifique la dirección IP o el nombre de DNS del servidor en el que está instalado Kaspersky Security Center.
   b. En el campo **Puerto**, especifique el número del puerto para una conexión no cifrada con el servidor.
   c. En el campo **Puerto SSL**, especifique el número del puerto para una conexión SSL con el servidor.
   d. Si desea abrir el Agente de red inmediatamente después de la instalación, seleccione la casilla de verificación **Ejecutar después de la instalación**.

   Si no desea utilizar SSL para conectarse con el servidor, desactive la casilla de verificación **Usar SSL**. Para seguir con la instalación, haga clic en **Continuar**.
9. En la ventana **Tipo de instalación**, lea la información sobre el disco en el que se instalará el Agente de red.
   Para instalar el Agente de red mediante las preferencias recomendadas, haga clic en **Instalar** e introduzca la contraseña de administrador para confirmar su elección.
   Espere hasta que el programa de instalación del Agente de red termine de instalar los componentes de aplicación.
10. Haga clic en **Cerrar** para cerrar el programa de instalación.

Instalación del Agente de red con Apple Remote Desktop

1. En un equipo remoto, escoja el **menú Apple** > **Ajustes del sistema** > **General** > **Compartir**.
2. Seleccione la casilla de verificación **Administración remota**.
3. En otra Mac que desee usar como servidor, instale Apple Remote Desktop. Para obtener más información sobre Apple Remote Desktop, consulte Soporte técnico de Apple.
4. Abra Apple Remote Desktop.
5. En la ventana **Escritorio remoto**, haga clic en **Análisis** a la izquierda y seleccione los dispositivos en los que desea instalar el Agente de red.
6. Haga clic en **Copiar**.
7. Haga clic en + y seleccione los archivos de instalación del Agente de red: el archivo DMG, el archivo KUD y el archivo SH.
8. En el menú emergente **Colocar elementos en**, seleccione **Carpeta superior del disco**.
9. Haga clic en **Copiar**.
10. Una vez que los archivos se hayan copiado correctamente, haga clic en **Unix**.
11. Introduzca el siguiente comando:
    ```
    cd /;
    ./install.sh --accept_eula -r <dirección del servidor de administración>
    ```
    donde `<dirección del servidor de administración>` es el nombre DNS o la dirección IP del servidor de administración de Kaspersky Security Center.

    Nota: Al introducir este comando, acepta el Contrato de licencia de usuario final.
12. Elija ejecutar el comando como **Usuario** y escriba "root" en el campo.
13. Haga clic en **Enviar**.

La instalación del Agente de red se inicia en los dispositivos seleccionados.

Instalación del Agente de red con Kaspersky Security Center

Kaspersky Security Center instala el Agente de red en un equipo cliente mediante una conexión SSH.

Antes de instalar el Agente de red en un equipo cliente, asegúrese de que se cumplan las siguientes condiciones:

- El servidor de administración de Kaspersky Security Center se implementa en la red corporativa.

- Se ha instalado la Consola de administración en la estación de trabajo del administrador de Kaspersky Security Center.
- El inicio de sesión remoto está habilitado en los equipos remotos.
- Se crea en un equipo remoto una cuenta de administrador especializada que se usará para ejecutar la tarea de instalación remota. Puede usar una cuenta de dominio para la instalación.
- La contraseña de sudo está desactivada para la cuenta especializada.

Crear un paquete de instalación del Agente de red

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, seleccione la carpeta **Avanzado**, la subcarpeta **Instalación remota** y, a continuación, la subcarpeta **Paquetes de instalación**.
4. En el espacio de trabajo, haga clic en **Crear paquete de instalación**.
5. En la ventana **Seleccionar el tipo de paquete de instalación**, haga clic en **Crear un paquete de instalación para una aplicación de Kaspersky**.
6. En la ventana **Definición del nombre del paquete de instalación**, introduzca el nombre del nuevo paquete de instalación en el campo **Nombre** y haga clic en **Siguiente**.
7. En la ventana **Seleccionando el paquete de distribución para la instalación**, haga clic en **Examinar**.
   Se abrirá la ventana donde podrá seleccionar un archivo para crear el paquete de instalación.
8. Abra la carpeta que incluye el contenido del paquete de instalación del Agente de red y seleccione el archivo klnagent.kud.
   La ventana **Seleccionando el paquete de distribución para la instalación** indica el nombre y la versión de la aplicación que se instalará remotamente mediante el archivo que se ha agregado.
9. Haga clic en **Siguiente**.
   Se creará el paquete de instalación de Kaspersky Endpoint Security con la configuración especificada.
10. En la última ventana del asistente, haga clic en **Finalizar** para salir del asistente para nuevo paquete.

Crear la tarea de instalación remota del Agente de red en un equipo cliente

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. Seleccione la carpeta **Tareas**.
4. En el espacio de trabajo, inicie el Asistente para nueva tarea haciendo clic en **Nueva tarea**.
5. Siga los pasos del Asistente para nueva tarea para crear una tarea de instalación remota de Kaspersky Endpoint Security en el equipo cliente.

Para continuar al siguiente paso del asistente, haga clic en **Siguiente**. Para volver al paso anterior del asistente, haga clic en ←. Para salir del asistente en cualquier paso, haga clic en **Cancelar**.

Nota: El aspecto de los botones puede variar en función de la versión de Windows.

Paso 1. Seleccionar el tipo de tarea

1. En la ventana **Seleccionar tipo de tarea**, maximice el nodo **Servidor de Administración de Kaspersky Security Center**.
2. Seleccione la tarea **Instalar aplicación en remoto**.

Paso 2. Seleccionar el paquete de instalación

En la ventana **Seleccionar paquete de instalación**, realice una de las siguientes acciones:

- Si se ha creado anteriormente el paquete de instalación del Agente de red con los ajustes necesarios, selecciónelo en la lista de paquetes de instalación en la parte superior de la ventana **Seleccionar paquete de instalación**.
- Si aún no se ha creado el paquete de instalación requerido, haga clic en **Nuevo** para abrir el Asistente para nuevo paquete.

Paso 3. Configurar los ajustes de instalación

En la ventana **Ajustes**, haga lo siguiente:

1. Seleccione la casilla de verificación **Usando los recursos del sistema operativo mediante el Servidor de administración**.
2. Desmarque todas las otras casillas de verificación.

Paso 4. Seleccionar un grupo de administración para agregar en equipos después de la instalación

En la ventana **Mover a lista de dispositivos administrados**, seleccione un grupo al que se moverán los equipos después de la instalación, si es necesario.

Paso 5. Definir cómo seleccionar los equipos cliente para los que se creará la tarea

En la ventana **Seleccionar a qué dispositivos se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos detectados en la red por el Servidor de administración, seleccione la opción **Seleccionar dispositivos de red detectados por el Servidor de administración**.
- Para especificar manualmente las direcciones IP de los equipos o importarlas desde un archivo, seleccione la opción **Especificar direcciones de dispositivo manualmente o importar direcciones de la lista**.
- Para crear una tarea para una selección de dispositivos basada en un criterio predefinido, seleccione la opción **Asignar tarea a una selección de dispositivos**.
- Para seleccionar equipos de un grupo de administración específico, seleccione la opción **Asignar tarea a un grupo de administración**.

Paso 6. Seleccionar equipos cliente

En la ventana que se abre (**Seleccionar dispositivos**, **Selección de dispositivos**, o **Seleccionar grupo de administración**, según la opción que haya seleccionado en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipos o seleccione un grupo de administración al que se aplicará la tarea.

Paso 7. Seleccionar la cuenta para ejecutar la tarea

1. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, seleccione la casilla de verificación **Se necesita una cuenta (no se utiliza Agente de red)**.
2. Haga clic en **Agregar** > **Cuenta**.
   Se abre la ventana **Cuenta**.
3. Introduzca el nombre de usuario y la contraseña de la cuenta de administrador especializada de un equipo remoto.
4. Haga clic en **Aceptar**.

Paso 8. Configurar la programación de tareas

1. En la ventana **Configurar programación de tareas**, seleccione el modo de inicio en la lista desplegable **Inicio programado**.
2. Si es necesario, configure una tarea programada para que se inicie automáticamente (especificando la fecha y hora de inicio de la tarea).
3. Si desea ejecutar tareas que la aplicación no haya podido iniciar conforme a la programación (por ejemplo, porque el equipo se apagó a la hora programada), seleccione la casilla **Ejecutar tareas no realizadas**.

Kaspersky Endpoint Security iniciará la tarea una vez eliminado el impedimento para el inicio de la tarea.

Paso 9. Especificar el nombre de la tarea

En el campo **Nombre** de la ventana **Definir el nombre de la tarea**, introduzca el nombre de la tarea que está creando.

Paso 10. Terminar de crear la tarea

En la ventana **Finalizar la creación de tareas**, realice lo siguiente:

1. Si desea que la tarea se inicie en cuanto termine el asistente, seleccione la casilla de verificación **Ejecutar la tarea después de que finalice el asistente**.
2. Haga clic en **Finalizar**, pero no cierre el asistente.

Instalación del Agente de red mediante el protocolo SSH

Una manera de instalar el Agente de red en un equipo remoto es mediante el protocolo SSH.

Asegúrese de que se cumplan los siguientes requisitos:

- El servidor de administración de Kaspersky Security Center se implementa en la red corporativa.
- Se ha instalado la Consola de administración en la estación de trabajo del administrador de Kaspersky Security Center.
- Se ha creado el paquete de instalación del Agente de red y está almacenado en una carpeta compartida del Servidor de administración.
- El inicio de sesión remoto está habilitado en el equipo remoto.
- La cuenta de equipo usada para instalar el Agente de red está incluida en sudoers.

Para obtener información detallada sobre los paquetes de instalación, consulte la Ayuda de Kaspersky Security Center.

Instalación del Agente de red mediante el protocolo SSH

1. Inicie el cliente SSH en la estación de trabajo del administrador.
2. Conéctese al equipo remoto.
3. Conecte la carpeta compartida del Servidor de administración como unidad de red en el equipo remoto. Para ello, introduzca los siguientes comandos en el cliente SSH:

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<cuenta de administrador>:<contraseña>@<Dirección IP del servidor de administración>/KLSHARE
   /Volumes/KLSHARE
   ```

   Descripciones de parámetros:

   - `<cuenta de administrador>`: nombre de la cuenta de administrador en el Servidor de administración.
   - `<contraseña>`: contraseña del administrador del Servidor de administración.
   - `<dirección IP del servidor de administración>`: dirección IP del servidor en el que se aloja Kaspersky Security Center.
4. Ejecute el script de instalación. Para ello, introduzca el siguiente comando en el cliente SSH.

   ```
   cd /Volumes/KLSHARE/<klnagent_package_folder>
   ```

   donde `<klnagent_package_folder>` es la carpeta en la que se encuentra el paquete de instalación del Agente de red.

   ```
   sudo ./install.sh --accept_eula [-r <servidor>] [-p <número de puerto>] [-s use_ssl 0|1] [-l <número de
   puerto SSL>] [-x use_proxy 0|1] [-a <proxy>] [-n <proxy login>] [-w <proxy password>]
   ```

   Descripciones de parámetros:

   - `<servidor>`: dirección IP o nombre DNS del servidor en el que está instalado Kaspersky Security Center.
   - `<número de puerto>`: número del puerto que se utiliza para establecer una conexión no cifrada con el Servidor de administración. De forma predeterminada, se utilizará el puerto 14000.
   - `use_ssl 0|1`: parámetro que determina si se utiliza o no el cifrado al establecer la conexión entre el Agente de red y el Servidor de administración. Si el valor es "0", se utiliza una conexión no cifrada. Si el valor es "1", la conexión se establece a través del protocolo SSL

(valor predeterminado).

- `<número de puerto SSL>`: número del puerto que se utiliza para establecer una conexión cifrada con el Servidor de administración mediante el protocolo SSL. De forma predeterminada, se utilizará el puerto 13000.
- `use_proxy 0|1`: parámetro que define si se utilizará un servidor proxy al conectarse a Internet. Si el valor es "0", no se utiliza un servidor proxy. Si el valor es "1", la conexión se establece a través de un servidor proxy (valor predeterminado).
- `<proxy>`: dirección IP o nombre de DNS de un servidor proxy.
- `<proxy_login>`: cuenta de usuario para conectarse al servidor proxy.
- `<proxy_password>`: contraseña para conectarse al servidor proxy.

Importante: Se requieren derechos de administrador para ejecutar este comando.

5. Desconecte la unidad de red del equipo remoto. Para ello, introduzca el siguiente comando en el cliente SSH.
   ```
   umount /Volumes/KLSHARE
   ```
6. Compruebe si el Agente de red funciona correctamente en el equipo remoto. Para ello, introduzca los siguientes comandos en el cliente SSH:
   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```
   Si la comprobación es satisfactoria, significará que el Agente de red funciona correctamente.

Desinstalación del Agente de red de forma local

1. En el equipo remoto, abra la carpeta con el kit de distribución del Agente de red.
2. Abra el kit de distribución del Agente de red (archivo DMG).
   Se abrirá una ventana con los contenidos del kit de distribución.
3. En la ventana con el contenido del kit de distribución, haga doble clic en **Programa de desinstalación del Agente de red**.
4. En la ventana **Presentación**, haga clic en **Continuar**.
5. En la ventana **Información**, haga clic en **Desinstalar**.
6. En la solicitud de las credenciales del administrador, introduzca un nombre de administrador y una contraseña, y confirme que desea desinstalar el Agente de red.
   Se inicia la desinstalación del Agente de red.
7. Lea la información acerca de la desinstalación y haga clic en **Finalizar** para salir del programa de desinstalación.

El Agente de red ahora se ha eliminado ahora del equipo remoto.

Gestionar el Agente de red desde la línea de comandos

En esta sección se ofrece información sobre cómo administrar el Agente de red mediante la línea de comandos del equipo cliente.

Puede detener el Agente de red y volver a iniciarlo mediante la línea de comandos en un equipo cliente.

Además, puede conectar manualmente un equipo remoto al Servidor de administración mediante la utilidad klmover y comprobar la conexión entre el equipo remoto y el Servidor de administración con la utilidad klnagchk.

Puede desinstalar el Agente de red.

Iniciar/detener el Agente de red en un equipo remoto

Es posible detener y volver a iniciar el Agente de red en un equipo cliente mediante la línea de comandos.

Detener el Agente de red

En el equipo remoto, inicie la utilidad launchctl con el comando de descarga de la línea de comandos.

Sintaxis del comando:

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Iniciar el Agente de red

En el equipo remoto, inicie la utilidad launchctl con el comando de carga de la línea de comandos.

Sintaxis del comando:

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Importante: Se requieren derechos de administrador para detener e iniciar el Agente de red.

Comprobar manualmente la conexión entre un equipo cliente y el Servidor de administración. Utilidad Klnagchk

Comprobar la conexión entre un equipo remoto y el Servidor de administración

En el equipo remoto, inicie la utilidad klnagchk desde la línea de comandos.

La utilidad klnagchk se incluye en el kit de distribución del Agente de red.

Una vez instalado el Agente de red, la utilidad klnagchk se encontrará en la carpeta /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

En función de los parámetros que especifique, la utilidad klnagchk realizará las siguientes operaciones cuando se ejecute desde la línea de comandos:

- Muestra los ajustes especificados para la conexión entre el Agente de red instalado en el equipo remoto y el Servidor de administración o los guarda en un archivo.
- Guarda las estadísticas del Agente de red (desde su último arranque) y los resultados de la ejecución de la utilidad en un archivo o muestra esta información en la pantalla.
- Intenta establecer una conexión entre el Agente de red y el Servidor de administración.
- Si la utilidad no puede establecer una conexión, enviará un paquete ICMP para comprobar el estado del equipo en el que está instalado el Servidor de administración.

Antes de ejecutar la utilidad, abra la carpeta /Library/Application Support/Kaspersky Lab/klnagent/Binaries en la línea de comandos.

Sintaxis del comando:

```
sudo ./klnagchk [-logfile <nombre de archivo>] [-sp] [-savecert <ruta al archivo de certificado>] [-restart]
```

Importante: Para ejecutar la utilidad se requieren derechos de administrador.

Descripciones de parámetros

`-logfile <nombre de archivo>`: guarda los ajustes de la conexión entre el Agente de red y el Servidor de administración, y los resultados de la ejecución de la utilidad en un archivo. Si no se especifica este parámetro, se mostrarán los ajustes de conexión del servidor, los resultados de ejecución y los mensajes de error en la pantalla.

`-sp`: Muestra la contraseña para la autenticación del servidor proxy en la pantalla o la guarda en un archivo. Este parámetro se utiliza si el Agente de red se conecta al Servidor de administración a través de un servidor proxy. Este parámetro no se utiliza de forma predeterminada.

`-savecert <nombre de archivo>`: guarda en un archivo especificado el certificado para la autenticación en el Servidor de administración.

`-restart`: reinicia el Agente de red después de que la utilidad termine de ejecutarse.

Ejemplo:

sudo ./klnagchk -logfile klnagchk.log -sp

Conectar manualmente un equipo remoto al Servidor de administración. Utilidad Klmover

Conectar un equipo remoto al Servidor de administración

En el equipo remoto, ejecute la utilidad klmover desde la línea de comandos.

La utilidad klmover se incluye en el paquete de instalación del Agente de red.

Una vez instalado el Agente de red, la utilidad klmover se encontrará en la carpeta /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

En función de los parámetros que especifique, la utilidad klmover realizará las siguientes operaciones cuando se ejecute desde la línea de comandos:

- Conecta el Agente de red al Servidor de administración con los parámetros especificados.
- Guarda los resultados de la ejecución de la utilidad en un archivo o los muestra en la pantalla.

Antes de ejecutar la utilidad, abra la carpeta /Library/Application Support/Kaspersky Lab/klnagent/Binaries en la línea de comandos.

Sintaxis de la línea de comandos:

```
sudo ./klmover [-logfile <nombre de archivo>] [-dirección <dirección del servidor>] [-pn <número de puerto>] [-ps
<número de puerto SSL>] [-nossl] [-cert <ruta al archivo de certificado>] [-silent] [-dupfix]
```

Importante: Para ejecutar la utilidad se requieren los derechos de administrador.

Descripciones de parámetros

`-logfile <nombre de archivo>`: guarda los resultados de ejecución en un archivo. Si no se especifica este parámetro, los resultados de ejecución y los mensajes de error se mostrarán en la pantalla.

`-address <dirección del servidor>`: dirección que el Agente de red utiliza para conectarse al Servidor de administración. Puede especificar la dirección IP o el nombre de DNS del servidor.

Nota: También puede utilizar el comando con este parámetro para modificar la dirección del Servidor de administración al cual se conectan los equipos remotos.

`-pn <número de puerto>`: número del puerto que se utiliza para establecer una conexión no cifrada con el Servidor de administración. De forma predeterminada, se utilizará el puerto 14000.

`-ps <número de puerto SSL>`: número del puerto que se utiliza para establecer una conexión cifrada con el Servidor de administración mediante el protocolo SSL. De forma predeterminada, se utilizará el puerto 13000.

`-nossl`: utiliza una conexión no cifrada con el Servidor de administración. Si no se especifica este parámetro, el Agente de red establecerá una conexión segura con el Servidor de administración a través del protocolo SSL cifrado.

`-cert <ruta al archivo de certificado>`: utiliza el archivo de certificado especificado para realizar la autenticación en un nuevo Servidor de administración. Si no se especifica este parámetro, el Agente de red recibirá un certificado la primera vez que se realice la conexión con el Servidor de administración.

`-silent`: ejecuta la utilidad en modo silencioso.

`-dupfix`: este parámetro se utiliza si el método con el que se instaló el Agente de red difiere de los métodos descritos en esta ayuda; por ejemplo, si se recuperó de una imagen de disco con el Agente de red instalado. Si una autoidentificación automática del Agente de red provoca la duplicación de los iconos en el equipo original y en otros equipos de la Consola de administración, intente volver a conectar los equipos duplicados.

Nota: Al ejecutar la utilidad klmover, se recomienda especificar los valores para todos los parámetros.

Ejemplo:

sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

El equipo remoto que se conecta al Servidor de administración a través del Agente de red se denomina *equipo cliente*.

Desinstalar el Agente de red

Sintaxis del comando:

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Instalar y desinstalar Kaspersky Endpoint Security

En esta sección se describe la instalación y la desinstalación remota de Kaspersky Endpoint Security en un equipo cliente.

También puede instalar o desinstalar Kaspersky Endpoint Security localmente o a través de Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

Instalación de la aplicación mediante el protocolo SSH

Antes de instalar Kaspersky Endpoint Security en un equipo remoto, asegúrese de que se cumplan las siguientes condiciones:

- El servidor de administración de Kaspersky Security Center se implementa en la red corporativa.
- Se ha instalado la Consola de administración en la estación de trabajo del administrador de Kaspersky Security Center.
- Se ha creado un paquete de instalación para Kaspersky Endpoint Security y se encuentra en una carpeta compartida en el Servidor de administración.
- En la carpeta compartida del Servidor de administración se encuentra un archivo de claves para Kaspersky Endpoint Security (opcional).
- El inicio de sesión remoto está habilitado en el equipo remoto.
- La cuenta de equipo usada para instalar la aplicación está incluida en sudoers.

Instalar Kaspersky Endpoint Security en un equipo cliente mediante el protocolo SSH

1. Inicie el cliente SSH en la estación de trabajo del administrador de Kaspersky Security Center.
2. Conéctese al equipo remoto.
3. Conecte la carpeta compartida del Servidor de administración como unidad de red en el equipo remoto. Para ello, introduzca los siguientes comandos en el cliente SSH:
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<cuenta de administrador>:<contraseña>@<Dirección IP del servidor de administración>/KLSHARE
   /Volumes/KLSHARE
   ```
   Descripciones de parámetros:
   - `<cuenta de administrador>`: nombre de la cuenta de administrador en el Servidor de administración.
   - `<contraseña>`: contraseña del administrador del Servidor de administración.
   - `<dirección IP del servidor de administración>`: dirección IP del servidor en el que se aloja Kaspersky Security Center.
4. Ejecute el script de instalación. Para ello, introduzca los siguientes comandos en el cliente SSH:
   ```
   cd /Volumes/KLSHARE/<carpeta de paquete de KES>
   ./install.sh --accept_eula
   ```
   donde `<carpeta de paquete de KES>` es la carpeta en la que se encuentra el paquete de instalación de Kaspersky Endpoint Security.

   Importante: Se requieren derechos de administrador para ejecutar este comando.
5. Desconecte la unidad de red del equipo remoto. Para ello, introduzca el siguiente comando en el cliente SSH.
   ```
   umount /Volumes/KLSHARE
   ```

Instalación de la aplicación mediante Kaspersky Security Center

Antes de instalar Kaspersky Endpoint Security en un equipo cliente, asegúrese de que se cumplan las siguientes condiciones:

- El servidor de administración de Kaspersky Security Center se implementa en la red corporativa.
- Se ha instalado la Consola de administración en la estación de trabajo del administrador de Kaspersky Security Center.
- Se ha instalado el Agente de red en el equipo cliente.

- Se ha creado un paquete de instalación para Kaspersky Endpoint Security y está almacenado en una carpeta compartida en el Servidor de administración.
- Se ha almacenado un archivo de claves para Kaspersky Endpoint Security en una carpeta compartida del Servidor de administración (opcional).
- Se ha agregado el equipo cliente al grupo de administración **Dispositivos administrados** del Servidor de administración (opcional).

Para obtener información detallada sobre los grupos de administración del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

Para instalar Kaspersky Endpoint Security en un equipo cliente a través de Kaspersky Security Center, debe crear e iniciar la tarea **Instalar aplicación en remoto**.

Crear la tarea de instalación remota de Kaspersky Endpoint Security de un equipo cliente

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. Seleccione la carpeta **Tareas**.
4. En el espacio de trabajo, inicie el Asistente para nueva tarea haciendo clic en **Nueva tarea**.
5. Siga los pasos del Asistente para nueva tarea para crear una tarea de instalación remota de Kaspersky Endpoint Security en el equipo cliente.

Para continuar al siguiente paso del asistente, haga clic en **Siguiente**. Para volver al paso anterior del asistente, haga clic en ←. Para salir del asistente en cualquier paso, haga clic en **Cancelar**.

Nota: El aspecto de los botones puede variar en función de la versión de Windows.

Paso 1. Seleccionar el tipo de tarea

1. En la ventana **Seleccionar tipo de tarea**, maximice el nodo **Servidor de Administración de Kaspersky Security Center**.
2. Seleccione la tarea **Instalar aplicación en remoto**.

Paso 2. Seleccionar el paquete de instalación

En la ventana **Seleccionar paquete de instalación**, realice una de las siguientes acciones:

- Si se ha creado anteriormente el paquete de instalación de Kaspersky Endpoint Security con los ajustes necesarios, selecciónelo en la lista de paquetes de instalación de la parte superior de la ventana **Seleccionar paquete de instalación**.
- Si aún no se ha creado el paquete de instalación requerido, haga clic en **Nuevo** para abrir el Asistente para nuevo paquete.

Paso 3. Instalar aplicaciones adicionales

En la ventana **Avanzado**, seleccione **Instalar Agente de red junto con esta aplicación** y seleccione las casillas de verificación **<nombre del paquete de instalación del Agente de red>** si también desea instalarlo en el equipo cliente.

Nota: El paquete de instalación para el Agente de red debe crearse de antemano. Si no se ha creado, haga clic en **Crear** para iniciar el asistente de paquete nuevo.

Paso 4. Configurar los ajustes de instalación

En la ventana **Ajustes**, configure la instalación remota de la aplicación.

Paso 5. Seleccionar un grupo de administración para agregar en equipos después de la instalación

En la ventana **Mover a lista de dispositivos administrados**, seleccione un grupo al que se moverán los equipos después de la instalación, si es necesario.

Nota: La ventana **Mover a lista de dispositivos administrados** aparece si selecciona instalar el Agente de red en el paso 3.

Paso 6. Definir cómo seleccionar los equipos cliente para los que se creará la tarea

En la ventana **Seleccionar a qué dispositivos se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos detectados en la red por el Servidor de administración, seleccione la opción **Seleccionar dispositivos de red detectados por el Servidor de administración**.
- Para especificar manualmente las direcciones IP de los equipos o importarlas desde un archivo, seleccione la opción **Especificar direcciones de dispositivo manualmente o importar direcciones de la lista**.
- Para crear una tarea para una selección de dispositivos basada en un criterio predefinido, seleccione la opción **Asignar tarea a una selección de dispositivos**.
- Para seleccionar equipos de un grupo de administración específico, seleccione la opción **Asignar tarea a un grupo de administración**.

Paso 7. Seleccionar equipos cliente

En la ventana que se abre (**Seleccionar dispositivos**, **Selección de dispositivos**, o **Seleccionar grupo de administración**, según la opción que haya seleccionado en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipos o seleccione un grupo de administración al que se aplicará la tarea.

Paso 8. Seleccionar una cuenta para ejecutar la tarea

En la ventana **Seleccionar una cuenta para ejecutar la tarea**, seleccione la casilla de verificación **No es necesaria una cuenta (Agente de red instalado)**.

Se supone que ha instalado el Agente de red antes de iniciar este asistente.

Paso 9. Configurar la programación de tareas

1. En la ventana **Configurar programación de tareas**, seleccione el modo de inicio en la lista desplegable **Inicio programado**.
2. Si es necesario, configure una tarea programada para que se inicie automáticamente (especificando la fecha y hora de inicio de la tarea).
3. Si desea ejecutar tareas que la aplicación no haya podido iniciar conforme a la programación (por ejemplo, porque el equipo se apagó a la hora programada), seleccione la casilla **Ejecutar tareas no realizadas**.
   Kaspersky Endpoint Security iniciará la tarea una vez eliminado el impedimento para el inicio de la tarea.

Paso 10. Especificar el nombre de la tarea

En el campo **Nombre** de la ventana **Definir el nombre de la tarea**, introduzca el nombre de la tarea que está creando.

Paso 11. Terminar de crear la tarea

En la ventana **Finalizar la creación de tareas**, realice lo siguiente:

1. Si desea que la tarea se inicie en cuanto termine el asistente, seleccione la casilla de verificación **Ejecutar la tarea después de que finalice el asistente**.
2. Haga clic en **Finalizar**, pero no cierre el asistente.

La tarea que ha creado aparecerá en el espacio de trabajo de la carpeta **Tareas**.

Creación de un paquete de instalación

Cuando crea la tarea **Instalar aplicación en remoto**, puede usar un paquete de instalación existente o crear nuevo uno. Para ver la lista de los paquetes de instalación creados, haga clic **en Avanzado** > **Instalación remota** > **Paquetes de instalación**.

Crear un paquete de instalación en Kaspersky Security Center

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, seleccione la carpeta **Avanzado**, la subcarpeta **Instalación remota** y, a continuación, la subcarpeta **Paquetes de instalación**.
4. En el espacio de trabajo, haga clic en **Crear paquete de instalación**.
5. En la ventana **Seleccionar el tipo de paquete de instalación**, haga clic en **Crear un paquete de instalación para una aplicación de Kaspersky**.
6. En la ventana **Definición del nombre del paquete de instalación**, introduzca el nombre del nuevo paquete de instalación en el campo **Nombre** y haga clic en **Siguiente**.
7. En la ventana **Seleccionando el paquete de distribución para la instalación**, haga clic en **Examinar**.

   Se abrirá la ventana donde podrá seleccionar un archivo para crear el paquete de instalación.
8. Abra la carpeta que incluye el contenido del paquete de instalación de Kaspersky Endpoint Security y seleccione el archivo kesmac.kud.

   La ventana **Seleccionando el paquete de distribución para la instalación** indica el nombre y la versión de la aplicación que se instalará remotamente mediante el archivo que se ha agregado.
9. Seleccione la casilla de verificación **Copiar actualizaciones del repositorio al paquete de instalación** para copiar las actualizaciones de la aplicación del almacenamiento de Kaspersky Security Center al paquete de instalación si es necesario y haga clic en **Siguiente**.

   El paquete de instalación empezará a cargarse en el Servidor de administración. Cuando finalice la carga, se abrirá la ventana **Tipo de instalación**.
10. En la ventana **Tipo de instalación**, sección **Paquetes para instalar**, desactive las casillas situadas junto a los nombres de los componentes que desee omitir durante la instalación en el equipo cliente y haga clic en **Siguiente**.

    Se creará el paquete de instalación de Kaspersky Endpoint Security con la configuración especificada.
11. En la última ventana del asistente, haga clic en **Finalizar** para completar el asistente para nuevo paquete.

Desinstalación de la aplicación con Kaspersky Security Center

Antes de desinstalar Kaspersky Endpoint Security de un equipo cliente a través de Kaspersky Security Center, asegúrese de que se cumplan las siguientes condiciones:

- El servidor de administración de Kaspersky Security Center se implementa en la red corporativa.
- Se ha instalado la Consola de administración en la estación de trabajo del administrador de Kaspersky Security Center.
- Se ha instalado el Agente de red en el equipo cliente.

Para desinstalar Kaspersky Endpoint Security del equipo cliente a través de Kaspersky Security Center, debe crear e iniciar la tarea **Desinstalar aplicación en remoto**.

Importante: Desinstalar Kaspersky Endpoint Security de un equipo cliente puede suponer un riesgo de infección.

Crear una tarea de desinstalación remota de Kaspersky Endpoint Security desde un equipo cliente

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. Seleccione la carpeta **Tareas**.
4. En el espacio de trabajo, inicie el Asistente para nueva tarea haciendo clic en **Nueva tarea**.
5. Siga los pasos del Asistente para nueva tarea para crear la tarea de desinstalación remota de Kaspersky Endpoint Security del equipo cliente.

Para continuar al siguiente paso del asistente, haga clic en **Siguiente**. Para volver al paso anterior del asistente, haga clic en ←. Para salir del asistente en cualquier paso, haga clic en **Cancelar**.

Nota: El aspecto de los botones puede variar en función de la versión de Windows.

Paso 1. Seleccionar el tipo de tarea

1. En la ventana **Seleccionar tipo de tarea**, maximice el nodo **Servidor de Administración de Kaspersky Security Center**.
2. Expanda el nodo secundario **Avanzado**.
3. Seleccione la tarea **Desinstalar aplicación en remoto**.

Paso 2. Seleccionar la aplicación que se va a desinstalar

En la ventana **Seleccionar la aplicación que se desinstalará**, seleccione **Desinstalar aplicación compatible con Kaspersky Security Center**.

Paso 3. Configurar los ajustes de desinstalación

En la ventana **Ajustes**, haga lo siguiente:

1. En la lista desplegable **Aplicación que se desinstalará**, seleccione **Kaspersky Endpoint Security for Mac 12.2**.
2. Haga clic en **Siguiente**.
3. Configure la desinstalación remota de la aplicación.

Paso 4. Seleccionar la opción de reinicio del sistema operativo

En la ventana **Selección de una opción de reinicio del sistema operativo**, seleccione la opción **No reiniciar el dispositivo**.

Paso 5. Definir cómo seleccionar los equipos cliente para los que se creará la tarea

En la ventana **Seleccionar a qué dispositivos se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos detectados en la red por el Servidor de administración, seleccione la opción **Seleccionar dispositivos de red detectados por el Servidor de administración**.
- Para especificar manualmente las direcciones IP de los equipos o importarlas desde un archivo, seleccione la opción **Especificar direcciones de dispositivo manualmente o importar direcciones de la lista**.
- Para crear una tarea para una selección de dispositivos basada en un criterio predefinido, seleccione la opción **Asignar tarea a una selección de dispositivos**.
- Para seleccionar equipos de un grupo de administración específico, seleccione la opción **Asignar tarea a un grupo de administración**.

Paso 6. Seleccionar equipos cliente

En la ventana que se abre (**Seleccionar dispositivos**, **Selección de dispositivos**, o **Seleccionar grupo de administración**, según la opción que haya seleccionado en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipos o seleccione un grupo de administración al que se aplicará la tarea.

Paso 7. Seleccionar una cuenta de usuario para ejecutar la tarea

En la ventana **Seleccionar una cuenta para ejecutar la tarea**, seleccione la casilla de verificación **No es necesaria una cuenta (Agente de red instalado)**.

Se supone que ha instalado el Agente de red antes de iniciar este asistente.

Paso 8. Configurar la programación de tareas

1. En la ventana **Configurar programación de tareas**, seleccione el modo de inicio en la lista desplegable **Inicio programado**.
2. Si es necesario, configure una tarea programada para que se inicie automáticamente (especificando la fecha y hora de inicio de la tarea).
3. Si desea ejecutar tareas que la aplicación no haya podido iniciar conforme a la programación (por ejemplo, porque el equipo se apagó a la hora programada), seleccione la casilla **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security iniciará la tarea una vez eliminado el impedimento para el inicio de la tarea.

Paso 9. Especificar el nombre de la tarea

En el campo **Nombre** de la ventana **Definir el nombre de la tarea**, introduzca el nombre de la tarea que está creando.

Paso 10. Terminar de crear la tarea

En la ventana **Finalizar la creación de tareas**, realice lo siguiente:

1. Si desea que la tarea se inicie en cuanto termine el asistente, seleccione la casilla de verificación **Ejecutar la tarea después de que finalice el asistente**.
2. Haga clic en **Finalizar**, pero no cierre el asistente.

La tarea que ha creado aparecerá en el espacio de trabajo de la carpeta **Tareas**.

Iniciar y detener la aplicación a través de Kaspersky Security Center

Puede iniciar o detener Kaspersky Endpoint Security en un equipo seleccionado de la lista de dispositivos administrados mediante Kaspersky Security Center.

Iniciar o detener Kaspersky Endpoint Security a través de Kaspersky Security Center

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. Seleccione la pestaña **Dispositivos**.
6. Seleccione un equipo de la lista de equipos cliente.
7. Abra la ventana **Propiedades: <nombre del equipo>** de una de las siguientes formas:
   - Haga doble clic en el nombre del equipo cliente.
   - Haga clic con el botón derecho del ratón en el equipo cliente y elija **Propiedades** en el menú contextual.
8. Seleccione la sección **Aplicaciones**.
9. En la lista **Aplicaciones de Kaspersky instaladas en el dispositivo**, haga clic derecho para abrir el menú contextual del elemento **Kaspersky Endpoint Security for Mac 12.2** y realice una de las siguientes acciones:
   - Para iniciar la aplicación, seleccione el elemento **Iniciar**.
   - Para detener la aplicación, seleccione el elemento **Detener**.

Importante: Tras detener Kaspersky Endpoint Security, el equipo cliente seguirá ejecutándose en modo desprotegido, lo que puede suponer un riesgo de infección.

Crear y administrar tareas

En esta sección se describe cómo usar Kaspersky Security Center para crear y configurar tareas que Kaspersky Endpoint Security realiza en un equipo cliente o en un grupo de equipos.

Una tarea es un conjunto de acciones configurables que Kaspersky Endpoint Security realiza en un equipo cliente.

En Kaspersky Security Center, puede crear las siguientes tareas:

- Agregar clave
- Análisis rápido
- Deshacer
- Análisis
- Actualización

Puede llevar a cabo las siguientes acciones en las tareas:

- Iniciar y detener tareas.
- Configurar los ajustes de las tareas.
- Llevar el seguimiento del progreso de una tarea.
- Copiar y mover tareas de un grupo a otro.
- Eliminar tareas.
- Importar y exportar tareas.

Para obtener información detallada sobre las tareas, consulte la Ayuda de Kaspersky Security Center.

Crear tareas

Al utilizar Kaspersky Endpoint Security a través de Kaspersky Security Center, puede crear los siguientes tipos de tareas:

- Tareas locales. *Una tarea local* es una tarea que se ejecuta en un equipo cliente concreto.
- Tareas de grupo. *Una tarea de grupo* es una tarea que se ejecuta en equipos de un grupo de administración.
- Tareas para un conjunto arbitrario de equipos. Puede crear una tarea para ejecutarla en cualquier equipo independientemente de si pertenece a un grupo de administración o a una selección de equipos.

Creación de una tarea local para un equipo cliente concreto

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
6. Seleccione el equipo de la lista de equipos cliente.
7. Abra la ventana **Propiedades: <nombre del equipo>** de una de las siguientes formas:
   - Haga doble clic en el nombre del equipo cliente.
   - Haga clic con el botón derecho del ratón en el equipo cliente y elija **Propiedades** en el menú contextual.
8. En la ventana **Propiedades: <nombre del equipo>** seleccione la sección **Tareas**.
   En el espacio de trabajo de la derecha se mostrará la lista de tareas personalizadas y del sistema para el equipo cliente seleccionado.
9. Haga clic en **Agregar** en la parte inferior del espacio de trabajo.
   Se iniciará el Asistente para nueva tarea.

10. Siga los pasos del Asistente para nueva tarea a fin de crear una tarea local para un equipo cliente concreto.

Crear una tarea para equipos cliente de un grupo de administración

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Tareas**.
6. En el espacio de trabajo, haga clic en **Nueva tarea** para iniciar el Asistente para nueva tarea.
7. Siga los pasos del Asistente para nueva tarea a fin de crear una tarea para equipos cliente incluidos en el grupo de administración.

Para obtener información detallada sobre cómo crear tareas de grupo, consulte la Ayuda de Kaspersky Security Center.

Crear una tarea para un grupo arbitrario de equipos

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Tareas**.
4. En el espacio de trabajo, haga clic en **Nueva tarea** para iniciar el Asistente para nueva tarea.
5. Siga los pasos del Asistente para nueva tarea a fin de crear una tarea para un conjunto arbitrario de equipos.

Para continuar al siguiente paso del asistente, haga clic en **Siguiente**. Para volver al paso anterior del asistente, haga clic en ←. Para salir del asistente en cualquier paso, haga clic en **Cancelar**.

Nota: El aspecto de los botones puede variar en función de la versión de Windows.

Paso 1. Seleccionar una aplicación y definir el tipo de tarea

1. En la ventana **Seleccionar tipo de tarea**, maximice el nodo **Kaspersky Endpoint Security for Mac 12.2**.
2. Seleccione el tipo de tarea que desea crear:
   - Para crear una tarea de adición de clave, seleccione **Añadir clave**.
   - Para crear una tarea de análisis de áreas críticas, seleccione **Análisis rápido**.
   - Para crear una tarea de deshacer la última actualización, seleccione **Reversión**.
   - Para crear una tarea de análisis de software malicioso, seleccione **Análisis**.
   - Para crear una tarea de actualización, seleccione **Actualizar**.

Paso 2. Configurar los ajustes para el tipo de tarea seleccionada

El contenido de la ventana de configuración puede variar en función del tipo de tarea seleccionada en el paso anterior. Esta ventana no se muestra para la tarea Deshacer.

Activación de la aplicación

En la ventana **Activación de la aplicación**, realice los siguientes pasos:

1. Seleccione un código de activación o clave en el almacenamiento de Kaspersky Security Center o agregue un archivo de claves almacenado en su equipo.
2. Si desea agregar la clave especificada como clave de reserva, seleccione la casilla de verificación **Añadir como clave de reserva**.

   La clave de reserva se activará cuando caduque la clave activa actual.

En la ventana **Activación de la aplicación** se mostrará la información sobre la clave especificada (la clave, el tipo de clave y fecha de caducidad).

Actualización

Los servidores de actualización específicos de Kaspersky son el origen principal de las actualizaciones de Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede usar los puertos de distribución, las carpetas locales u otros servidores web como un *origen de actualizaciones*.

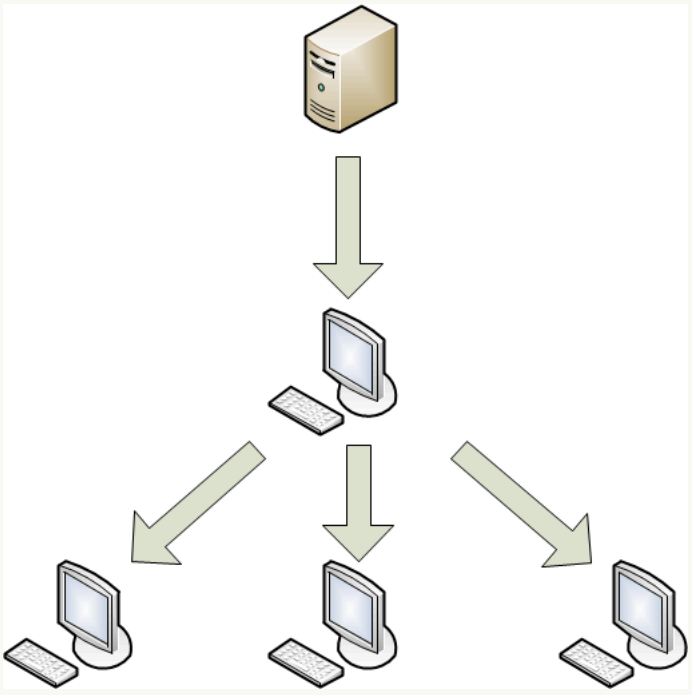
Puede colocar las actualizaciones descargadas en una carpeta local para actualizar las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security en otros equipos de la red corporativa a fin de reducir la cantidad de tráfico de Internet.

Puede configurar la distribución de actualizaciones de la siguiente manera:

1. Uno de los equipos de la red recibe un paquete de actualización de Kaspersky Endpoint Security desde los servidores de actualización de Kaspersky o desde otro origen de actualizaciones. Las actualizaciones obtenidas se ubican en una carpeta local compartida.

   Nota: La carpeta local compartida debe crearse de antemano.

2. Los otros equipos de la red se remiten a la carpeta local compartida como el origen de actualizaciones.



Distribución de actualizaciones a través de un equipo local

Si es necesario, edite la configuración de la tarea de actualización en la ventana **Actualizar**:

1. Para desactivar las actualizaciones de los módulos de la aplicación, desactive la casilla de verificación **Actualizar módulos de aplicación**.
2. Para cambiar el origen de actualizaciones:

   a. Haga clic en **Configuración**.

   Se abre la ventana **Configuración: Actualización**.

   b. Seleccione las casillas situadas junto a los orígenes de actualizaciones que desee utilizar.

3. Para especificar otro origen de actualizaciones, haga clic en **Añadir**.

   Se abre la ventana **Origen de actualizaciones**.

   a. Especifique la dirección web del origen de actualizaciones o la ruta a la carpeta local o de red que es un origen de actualizaciones y haga clic en **Aceptar**.

   b. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Actualización**.

Análisis y análisis rápido

De forma predeterminada, Kaspersky Endpoint Security utiliza el nivel de seguridad **Recomendado**, solicita al usuario que elija una acción al detectar un objeto infectado tras el análisis y analiza los siguientes objetos:

- Todas las unidades extraíbles
- Todas las unidades internas
- Todas las unidades de red
- Memoria

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Si es necesario, edite la configuración de Análisis de la ventana **Análisis**:

1. Seleccione uno de los niveles de seguridad predefinidos o personalice la configuración de seguridad.
2. Especifique las acciones que Kaspersky Endpoint Security debe ejecutar al detectar un objeto infectado.
3. Defina una cobertura del análisis.

Paso 3. Definir cómo seleccionar los equipos cliente para los que se creará la tarea

Nota: Este paso no es relevante para tareas locales o de grupo.

En la ventana **Seleccionar a qué dispositivos se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos detectados en la red por el Servidor de administración, seleccione la opción **Seleccionar dispositivos de red detectados por el Servidor de administración**.
- Para especificar manualmente las direcciones IP de los equipos o importarlas desde un archivo, seleccione la opción **Especificar direcciones de dispositivo manualmente o importar direcciones de la lista**.
- Para crear una tarea para una selección de dispositivos basada en un criterio predefinido, seleccione la opción **Asignar tarea a una selección de dispositivos**.
- Para seleccionar equipos de un grupo de administración específico, seleccione la opción **Asignar tarea a un grupo de administración**.

Paso 4. Seleccionar equipos cliente

Nota: Este paso no es relevante para tareas locales o de grupo.

En la ventana que se abre (**Seleccionar dispositivos**, **Selección de dispositivos**, o **Seleccionar grupo de administración**, según la opción que haya seleccionado en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipos o seleccione un grupo de administración al que se aplicará la tarea.

Paso 5. Configurar la programación de tareas

1. En la ventana **Configurar programación de tareas**, seleccione el modo de inicio en la lista desplegable **Inicio programado**.
2. Si es necesario, configure una tarea programada para que se inicie automáticamente (especificando la fecha y hora de inicio de la tarea).
3. Si desea ejecutar tareas que la aplicación no haya podido iniciar conforme a la programación (por ejemplo, porque el equipo se apagó a la hora programada), seleccione la casilla **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security iniciará la tarea una vez eliminado el impedimento para el inicio de la tarea.

4. Si desea que Kaspersky Security Center determine automáticamente el intervalo entre los inicios de las tareas en distintos equipos, seleccione la casilla de verificación **Usar el retraso aleatorio automáticamente para el inicio de tareas**.

   Esto ayuda a reducir la carga en el servidor de administración de Kaspersky Security Center.

5. Para especificar el intervalo entre inicios de tareas en diferentes equipos manualmente, seleccione la casilla de verificación **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)** y especifique el número de minutos.

   Esto ayuda a reducir la carga en el servidor de administración de Kaspersky Security Center.

Paso 6. Especificar el nombre de la tarea

En el campo **Nombre** de la ventana **Definir el nombre de la tarea**, introduzca el nombre de la tarea que está creando.

Paso 7. Terminar de crear la tarea

En la ventana **Finalizar la creación de tareas**, realice lo siguiente:

1. Si desea que la tarea se inicie en cuanto termine el asistente, seleccione la casilla de verificación **Ejecutar la tarea después de que finalice el asistente**.
2. Haga clic en **Finalizar**, pero no cierre el asistente.

Iniciar y detener tareas manualmente

Las tareas programadas se inician y se detienen automáticamente de acuerdo con una programación. Sin embargo, puede iniciar una tarea manualmente en cualquier momento.

Nota: Las tareas solo se inician en un equipo cliente si se está ejecutando el Agente de red. Si el Agente de red deja de ejecutarse, se interrumpirán todas las tareas activas.

Iniciar y detener tareas manualmente

1. Abra la lista de tareas que contiene la tarea que desea iniciar o detener.
2. Seleccione la tarea que desea iniciar o detener.
3. Puede iniciar o detener la tarea de alguna de las siguientes formas:
   - Haga clic con el botón derecho para mostrar el menú contextual de la tarea y seleccione **Iniciar** o **Detener**.
   - En el espacio de trabajo, haga clic en **Iniciar** o **Detener**.
   - Haga clic con el botón derecho para mostrar el menú contextual de la tarea y elija **Propiedades**. En la ventana que se abre, haga clic en **Iniciar** o **Detener**.

Importar y exportar tareas

Puede exportar tareas de grupo y tareas para un conjunto arbitrario de equipos a un archivo.

Exportar una tarea

1. Seleccione la lista de tareas de la cual quiere exportar la tarea:
   - Seleccione el grupo de administración y, a continuación, abra la pestaña **Tareas**.
   - En el árbol de la consola, haga clic en **Tareas**.
2. Haga clic derecho en la tarea que desea exportar y, en el menú de acceso directo de la tarea, elija **Todas las tareas** > **Exportar**.
3. En la ventana **Guardar como**, especifique el nombre de archivo y la ubicación en la que se guardará la tarea exportada.
4. Haga clic en **Guardar**.

Importar una tarea

1. Seleccione la lista de tareas en la cual desea importar la tarea:
   - Seleccione el grupo de administración y, a continuación, abra la pestaña **Tareas**.
   - En el árbol de la consola, haga clic en **Tareas**.
2. Importe la tarea de una de las siguientes maneras:
   - En el menú de acceso directo de la lista de la tarea, seleccione **Todas las tareas** > **Importación**.
   - Haga clic en **Importar tarea desde archivo**.
3. En la ventana **Abrir**, especifique la ruta al archivo de tarea que desea importar.
4. Haga clic en **Abrir**.

La tarea se muestra en la lista de tareas.

Ver tareas

Puede ver la lista de tareas creadas para un equipo específico, para equipos de un grupo de administración específico o de la lista de todas las tareas no locales.

Ver las tareas de un grupo de administración específico

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Tareas**.

Se mostrará la lista de tareas para equipos en el grupo de administración seleccionado.

Ver tareas locales

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
6. Seleccione el equipo de la lista de equipos cliente.
7. Abra la ventana **Propiedades: <nombre del equipo>** de una de las siguientes formas:
   - Haga doble clic en el nombre del equipo cliente.
   - Haga clic con el botón derecho del ratón en el equipo cliente y elija **Propiedades** en el menú contextual.
8. En la ventana **Propiedades: <nombre del equipo>** seleccione la sección **Tareas**.

En el espacio de trabajo de la derecha se mostrará la lista de tareas personalizadas y del sistema para el equipo cliente seleccionado.

Ver tareas no locales

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Tareas**.

Se mostrará la lista de tareas no locales creadas para equipos que pueden formar parte o no de los grupos de administración.

Gestionar la configuración de tareas específicas

Ver la configuración de una tarea local

1. Abra la lista de tareas locales.
2. Seleccione una tarea de la lista y abra la configuración de la tarea de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.

Ver la configuración de una tarea de grupo

1. Abra la lista de tareas de grupo de un grupo de administración.
2. Seleccione una tarea de la lista y abra la configuración de la tarea de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en el enlace **Configurar tarea** en el espacio de trabajo.

Ver la configuración de una tarea no local

1. Abra la lista de tareas no locales.
2. Seleccione una tarea de la lista y abra la configuración de la tarea de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en el enlace **Configurar tarea** en el espacio de trabajo.

Para obtener más información sobre las tareas, consulte la Ayuda de Kaspersky Security Center.

Tareas locales, tareas de grupo o tareas para un conjunto arbitrario de equipos

Administrar la configuración de la tarea Agregar clave

1. Abra la ventana con la configuración de la tarea **Añadir clave**.
2. Seleccione la sección **Activación de la aplicación**.
3. Si es necesario, agregue otra clave de una de las siguientes formas:
   - Para seleccionar un código de activación o una clave de entre los códigos de activación agregados al almacenamiento de Kaspersky Security Center, siga los pasos indicados a continuación:
     a. Seleccione la opción **Clave o código de activación**.

b. Haga clic en **Examinar**.

Se abre la ventana **Claves y códigos de activación en el almacén de Kaspersky Security Center**.

c. Seleccione una clave o código de activación.

d. Haga clic en **Aceptar**.

- Para agregar un archivo de claves:

a. Seleccione la opción **Archivo de claves**.

b. Haga clic en **Añadir**.

Se abre la ventana de selección de archivos.

c. Seleccione un archivo de claves.

d. Haga clic en **Abrir**.

Nota: La clave actual se eliminará cuando se agregue una clave distinta.

4. Para agregar la clave especificada como clave de reserva, seleccione la casilla **Añadir como clave de reserva**.

La clave de reserva se activará cuando caduque la clave actual.

Nota: La fecha de caducidad de la clave de reserva debe ser posterior a la fecha de caducidad de la clave actual.

5. Guarde los cambios de una de las siguientes formas:

- Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.
- Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.

Administrar la configuración de la tarea de Análisis rápido

1. Abra la ventana con la configuración de la tarea **Análisis rápido**.
2. Seleccione la sección **Análisis rápido**.
3. Para cambiar el nivel de seguridad con el que Kaspersky Endpoint Security ejecuta la tarea Análisis rápido, realice una de las siguientes acciones en la sección **Nivel de seguridad**:

- Para seleccionar un nivel de seguridad predefinido, suba o baje el control deslizante por el medidor.

Puede seleccionar uno de los siguientes niveles de seguridad:

- **Protección máxima**. Kaspersky Endpoint Security realiza el nivel máximo de supervisión de los archivos que se abren, guardan o ejecutan.
- **Recomendado**. Kaspersky Endpoint Security supervisa los archivos con la configuración recomendada por Kaspersky.

Este es el nivel de seguridad predeterminado.

- **Velocidad máxima**. Kaspersky Endpoint Security supervisa un conjunto mínimo de archivos. Puede elegir este nivel de seguridad si desea usar otras aplicaciones que requieren más recursos de memoria.

- Configurar manualmente los ajustes de seguridad:

a. Haga clic en **Configuración**.

Se abre la ventana **Configuración: Análisis**.

b. En la pestaña **General** de la sección **Tipos de archivos**, seleccione aquellos que Kaspersky Endpoint Security deberá analizar cuando ejecute la tarea Análisis rápido.

c. En la pestaña **General** de la sección **Optimización**, configure el rendimiento del análisis.

d. En la pestaña **General** de la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice en busca de objetos detectables.

e. En la pestaña **Avanzado** de la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el registro de información sobre objetos detectados en las estadísticas de la aplicación.

f. En la pestaña **Avanzado** de la sección **Analizador heurístico**, configure el uso del Analizador heurístico y seleccione el nivel de protección que este aplicará durante las tareas de análisis de software malicioso.

g. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.

El nivel de seguridad cambiará a **Personalizado**.

- Para restaurar las preferencias predeterminadas, haga clic en **Predeterminado**.

  El nivel de seguridad cambiará a **Recomendado**.

4. Si es necesario, en la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security deberá realizar cuando se detecte un objeto infectado.

5. Para especificar una cobertura del análisis, en la sección **Cobertura del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Cobertura del análisis** que se abre:

   a. Si desea que Kaspersky Endpoint Security analice la memoria del equipo, seleccione la casilla de verificación **Memoria**.

   b. Si desea que Kaspersky Endpoint Security analice los objetos de inicio, seleccione la casilla de verificación **Ítems de inicio**.

   c. Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas adicionales, haga clic en **Añadir** y especifique un archivo, una carpeta o una máscara de nombres de archivos o carpetas.

   d. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Cobertura del análisis**.

6. Guarde los cambios de una de las siguientes formas:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.

Administrar la configuración de la tarea de análisis

1. Abra la ventana con la configuración de la tarea de **Análisis**.

2. Seleccione la sección **Análisis**.

3. Para cambiar el nivel de seguridad con el que Kaspersky Endpoint Security ejecuta la tarea de análisis, realice una de las siguientes acciones en la sección **Nivel de seguridad**:

   - Para seleccionar un nivel de seguridad predefinido, suba o baje el control deslizante por el medidor.

     Puede seleccionar uno de los siguientes niveles de seguridad:

     - **Protección máxima**. Kaspersky Endpoint Security realiza el nivel máximo de supervisión de los archivos que se abren, guardan o ejecutan.
     - **Recomendado**. Kaspersky Endpoint Security supervisa los archivos con la configuración recomendada por Kaspersky.

       Este es el nivel de seguridad predeterminado.
     - **Velocidad máxima**. Kaspersky Endpoint Security supervisa un conjunto mínimo de archivos. Puede elegir este nivel de seguridad si desea usar otras aplicaciones que requieren más recursos de memoria.

   - Configurar manualmente los ajustes de seguridad:

     a. Haga clic en **Configuración**.

     Se abre la ventana **Configuración: Análisis**.

     b. En la pestaña **General** de la sección **Tipos de archivos**, seleccione aquellos que Kaspersky Endpoint Security deberá analizar cuando ejecute la tarea de análisis.

     c. En la pestaña **General** de la sección **Optimización**, configure el rendimiento del análisis.

     d. En la pestaña **General** de la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice en busca de objetos detectables.

     e. En la pestaña **Avanzado** de la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el registro de información sobre objetos detectados en las estadísticas de la aplicación.

f. En la pestaña **Avanzado** de la sección **Analizador heurístico**, configure el uso del Analizador heurístico y seleccione el nivel de protección que este aplicará durante las tareas de análisis de software malicioso.

g. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.

El nivel de seguridad cambiará a **Personalizado**.

- Para restaurar las preferencias predeterminadas, haga clic en **Predeterminado**.

  El nivel de seguridad cambiará a **Recomendado**.

4. Si es necesario, en la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security deberá realizar cuando se detecte un objeto infectado.

5. Para especificar una cobertura del análisis, en la sección **Cobertura del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Cobertura del análisis** que se abre:

   a. Si desea que Kaspersky Endpoint Security analice todas las unidades extraíbles, seleccione la casilla **Todas los discos extraíbles**.

   b. Si desea que Kaspersky Endpoint Security analice todas las unidades internas, seleccione la casilla **Todos los discos internos**.

   c. Si desea que Kaspersky Endpoint Security analice todas las unidades de red, seleccione la casilla **Todos los discos de red**.

   d. Si desea que Kaspersky Endpoint Security analice la memoria del equipo, seleccione la casilla de verificación **Memoria**.

   e. Si desea que Kaspersky Endpoint Security analice los objetos de inicio, seleccione la casilla de verificación **Ítems de inicio**.

   f. Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas, haga clic en **Añadir** y especifique un archivo, una carpeta o una máscara de nombres de archivos o carpetas.

   g. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Cobertura del análisis**.

6. Guarde los cambios de una de las siguientes formas:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.

Administrar la configuración de la tarea de actualización

1. Abra la ventana con la configuración de la tarea de **Actualizar**.

2. Seleccione la sección **Actualizar**.

3. Si desea que Kaspersky Endpoint Security actualice los módulos de la aplicación junto con las bases de datos de esta, seleccione la casilla **Actualizar módulos de aplicación**.

4. Para elegir un origen de actualizaciones:

   a. Haga clic en **Configuración**.

   Se abre la ventana **Configuración: Actualización**.

   b. Especifique el origen de actualizaciones de una de las siguientes formas:

   - Si desea que la aplicación descargue actualizaciones del Servidor de administración, seleccione la casilla de verificación **Kaspersky Security Center**.
   - Si desea que la aplicación descargue actualizaciones de los servidores de actualización de Kaspersky, seleccione la casilla de verificación **Servidores de actualización de Kaspersky**.
   - Para agregar un origen de actualizaciones distinto, haga clic en el botón **Añadir** y, en la ventana que se abre, introduzca la ruta al origen de actualizaciones.

     De forma predeterminada, Kaspersky Endpoint Security descarga las actualizaciones de los servidores de actualización de Kaspersky.

   c. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Actualización**.

5. Guarde los cambios de una de las siguientes formas:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <nombre de la tarea>** tras guardar los cambios.

Solo para tareas locales

Administrar la configuración de la tarea de Protección frente a amenazas en archivos

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea de Protección frente a amenazas en archivos y abra sus propiedades de una de las siguientes maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección **Protección frente a amenazas en archivos**.
4. Si es necesario, configure el siguiente ajuste:
   - Active o desactive el componente Protección frente a amenazas en archivos en el equipo cliente.
   - Para seleccionar uno de los niveles de seguridad predefinidos, utilice el control deslizante de la sección **Nivel de seguridad**.
   - Para configurar el ajuste de seguridad manualmente, haga clic en **Configuración** y en la ventana **Configuración: Protección frente a amenazas en archivos** que se abre, haga lo siguiente:
     a. En la pestaña **General** de la sección **Tipos de archivos**, seleccione aquellos que Kaspersky Endpoint Security deberá analizar cuando se abran, ejecuten o guarden.
     b. En la pestaña **General**, en la sección **Optimización**, ajuste la configuración del rendimiento del análisis, seleccione la tecnología de análisis y elija si Kaspersky Endpoint Security omitirá el análisis del volumen del sistema de solo lectura en los equipos cliente.
     c. En la pestaña **General** de la sección **Archivos compuestos**, seleccione qué archivos compuestos deberán analizarse para detectar objetos y establezca una restricción para el análisis de objetos de gran tamaño.
     d. En la pestaña **Cobertura de protección**, especifique los archivos o carpetas que el componente Protección frente a amenazas en archivos deberá analizar.
        De forma predeterminada, se analizarán todos los objetos ubicados en unidades extraíbles, internas y de red conectadas al equipo cliente. Puede agregar un objeto a la cobertura de protección, modificar un objeto de la lista, desactivar temporalmente el análisis de un objeto de la lista o quitar un objeto de la lista.
     e. En la pestaña **Avanzado**, en la sección **Modo de análisis**, seleccione el modo Protección frente a amenazas en archivos.
     f. En la pestaña **Avanzado** de la sección **Detener tarea**, active o desactive la puesta en pausa programada del componente Protección frente a amenazas en archivos y configure la puesta en pausa automática de tareas conforme a la programación.
     g. En la pestaña **Avanzado** de la sección **Analizador heurístico**, configure el uso del Analizador heurístico mediante la Protección frente a amenazas en archivos.
     h. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Protección frente a amenazas en archivos**.
   - En la sección **Si se detecta un objeto malicioso**, seleccione la acción que el componente Protección frente a amenazas en archivos realizará al detectar un objeto infectado.
5. Guarde los cambios de una de las siguientes formas:
   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Protección frente a amenazas en archivos** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Protección frente a amenazas en archivos** tras guardar los cambios.

Administrar la configuración de la tarea de Protección frente a amenazas web

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea Protección frente a amenazas web y abra sus propiedades de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.

- Haga clic en **Propiedades**.

3. Seleccione la sección **Protección frente a amenazas web**.

4. Si es necesario, configure el siguiente ajuste:

   - Active o desactive el componente Protección frente a amenazas web en el equipo cliente.
   - Para seleccionar uno de los niveles de seguridad predefinidos, utilice el control deslizante de la sección **Nivel de seguridad**.
   - Para configurar el ajuste de seguridad manualmente, haga clic en **Configuración** y en la ventana **Ajustes: Protección frente a amenazas web** que se abre, haga lo siguiente:

     a. En la pestaña **General**, en la sección **Modo de análisis**, active o desactive la comprobación de direcciones web con respecto a la base de datos de direcciones web maliciosas.

     b. En la pestaña **General**, en la sección **Configuración de prevención de phishing**, active o desactive la comprobación de direcciones web con respecto a la base de datos de direcciones web fraudulentas.

     c. En la pestaña **General**, en la sección **Configuración de prevención de phishing**, active o desactive el uso del Analizador heurístico para detectar vínculos fraudulentos.

     d. En la pestaña **Direcciones web de confianza**, active o desactive el análisis del tráfico web de las direcciones web de confianza y cree o edite una lista de direcciones web de confianza.

     e. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Ajustes: Protección frente a amenazas web**.

5. En la sección **Si se detecta un objeto malicioso**, seleccione la acción que el componente Protección frente a amenazas web realizará al detectar un objeto peligroso en el tráfico web.

6. Guarde los cambios de una de las siguientes formas:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Protección frente a amenazas web** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Protección frente a amenazas web** tras guardar los cambios.

Administrar la configuración de la tarea de Análisis rápido

1. Abra la lista de tareas locales para un equipo cliente.

2. En la lista de tareas locales, seleccione la tarea de Análisis rápido y abra sus propiedades de una de las siguientes formas:

   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.

3. Seleccione la sección **Análisis**.

4. Si es necesario, configure el siguiente ajuste:

   - Para seleccionar uno de los niveles de seguridad predefinidos, utilice el control deslizante de la sección **Nivel de seguridad**.
   - Para configurar el ajuste de seguridad manualmente, haga clic en **Configuración** y en la ventana **Configuración: Análisis** que se abre, haga lo siguiente:

     a. En la pestaña **General** de la sección **Tipos de archivos**, seleccione los tipos de archivos que Kaspersky Endpoint Security deberá analizar.

     b. En la pestaña **General** de la sección **Optimización**, configure el rendimiento del análisis.

     c. En la pestaña **General** de la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice.

     d. En la pestaña **Avanzado** de la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el guardado de información sobre objetos detectados en las estadísticas de la aplicación.

     e. En la pestaña **Avanzado** de la sección **Analizador heurístico**, configure el uso del Analizador heurístico y seleccione el nivel de protección que el Analizador heurístico aplicará.

     f. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.

- En la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security realizará al detectar un objeto infectado.
- Para especificar una cobertura del análisis, en la sección **Cobertura del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Cobertura del análisis** que se abre:
  - Si desea que Kaspersky Endpoint Security analice objetos de la lista predeterminada, seleccione la casilla que aparece junto a ese objeto.
  - Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas, haga clic en **Añadir** y especifique un archivo, una carpeta o una máscara de nombres de archivos o carpetas.
  - Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Cobertura del análisis**.

5. Guarde los cambios de una de las siguientes formas:

- Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Análisis rápido** tras guardar los cambios.
- Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Análisis rápido** tras guardar los cambios.

Administrar la configuración de la tarea de Análisis completo

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea de Análisis completo y abra sus propiedades de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección **Análisis**.
4. Si es necesario, configure el siguiente ajuste:
   - Para seleccionar uno de los niveles de seguridad predefinidos, utilice el control deslizante de la sección **Nivel de seguridad**.
   - Para configurar el ajuste de seguridad manualmente, haga clic en **Configuración** y en la ventana **Configuración: Análisis** que se abre, haga lo siguiente:
     a. En la pestaña **General** de la sección **Tipos de archivos**, seleccione los tipos de archivos que Kaspersky Endpoint Security deberá analizar.
     b. En la pestaña **General** de la sección **Optimización**, configure el rendimiento del análisis.
     c. En la pestaña **General** de la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice.
     d. En la pestaña **Avanzado** de la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el guardado de información sobre objetos detectados en las estadísticas de la aplicación.
     e. En la pestaña **Avanzado** de la sección **Analizador heurístico**, configure el uso del Analizador heurístico y seleccione el nivel de protección que el Analizador heurístico aplicará.
     f. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.
   - En la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security realizará al detectar un objeto infectado.
   - Para especificar una cobertura del análisis, en la sección **Cobertura del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Cobertura del análisis** que se abre:
     - Si desea que Kaspersky Endpoint Security analice objetos de la lista predeterminada, seleccione la casilla que aparece junto a ese objeto.
     - Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas, haga clic en **Añadir** y especifique un archivo, una carpeta o una máscara de nombres de archivos o carpetas.
     - Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Cobertura del análisis**.
5. Guarde los cambios de una de las siguientes formas:

- Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Análisis completo** tras guardar los cambios.

- Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Análisis completo** tras guardar los cambios.

Administrar la configuración de la tarea de Análisis personalizado

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea de Análisis personalizado y abra sus propiedades de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección **Análisis**.
4. Si es necesario, configure el siguiente ajuste:
   - Para seleccionar uno de los niveles de seguridad predefinidos, utilice el control deslizante de la sección **Nivel de seguridad**.
   - Para configurar el ajuste de seguridad manualmente, haga clic en **Configuración** y en la ventana **Configuración: Análisis** que se abre, haga lo siguiente:
     a. En la pestaña **General** de la sección **Tipos de archivos**, seleccione los tipos de archivos que Kaspersky Endpoint Security deberá analizar.
     b. En la pestaña **General** de la sección **Optimización**, configure el rendimiento del análisis.
     c. En la pestaña **General** de la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice.
     d. En la pestaña **Avanzado** de la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el guardado de información sobre objetos detectados en las estadísticas de la aplicación.
     e. En la pestaña **Avanzado** de la sección **Analizador heurístico**, configure el uso del Analizador heurístico y seleccione el nivel de protección que el Analizador heurístico aplicará.
     f. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.
   - En la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security realizará al detectar un objeto infectado.
   - Para especificar una cobertura del análisis, en la sección **Cobertura del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Cobertura del análisis** que se abre:
     - Haga clic en **Añadir** y especifique un archivo, carpeta o máscara de un archivo o carpeta.
     - Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Cobertura del análisis**.
5. Guarde los cambios de una de las siguientes formas:
   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Análisis personalizado** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Análisis personalizado** tras guardar los cambios.

Administrar la configuración de la tarea de Protección frente a amenazas en la red

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea Protección frente a amenazas en la red y abra sus propiedades de una de las siguientes formas:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic derecho para mostrar el menú de acceso directo de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección **Protección frente a amenazas en la red**.
4. Si es necesario, configure el siguiente ajuste:

- Active o desactive el componente Protección frente a amenazas en la red en el equipo cliente.
- En la sección **Configuración de Protección frente a amenazas en la red** frente a amenazas en la red, marque o desmarque la casilla de verificación **Bloquear los equipos atacantes durante <valor> min** y especifique el valor.
- También puede especificar las direcciones IP de los equipos cuya actividad de red no se bloqueará. Para ello, siga estos pasos:

  a. Haga clic en **Exclusiones**.
  Se abre la ventana **Exclusiones**.

  b. Haga clic en **Añadir**.
  Se abre la ventana **Dirección IP**.

  c. Especifique la dirección IP del equipo cuya actividad de red no se bloqueará y haga clic en **Aceptar**.

  d. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Exclusiones**.

5. Guarde los cambios de una de las siguientes formas:
   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Protección frente a amenazas en la red** tras guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Protección frente a amenazas en la red** tras guardar los cambios.

Crear y administrar directivas

Esta sección contiene información sobre cómo crear y configurar directivas para Kaspersky Endpoint Security.

Una directiva determina la configuración de una aplicación y administra la capacidad de configurar esa aplicación en equipos de un grupo de administración. Es necesario crear una directiva individual para cada aplicación. Puede crear múltiples directivas para las aplicaciones instaladas en los equipos de cada grupo de administración, pero solo se podrá aplicar una directiva a cada aplicación cada vez dentro de un grupo de administración.

Nota: A la hora de crear y configurar una directiva, puede impedir o permitir que se introduzcan cambios en cada grupo de ajustes de las directivas mediante los botones y .

Puede realizar las siguientes acciones en las tareas personalizadas:

- Crear directivas
- Configurar directivas
- Copiar o mover directivas de un grupo a otro
- Eliminar directivas
- Cambiar el estado de las directivas
- Exportar directivas a un archivo
- Importar directivas desde un archivo

Para obtener información detallada sobre las directivas de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

Crear una directiva

Esta sección contiene instrucciones sobre cómo iniciar el Asistente para una nueva directiva a fin de crear una directiva.

Crear una directiva desde la carpeta de un grupo de administración

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Directivas** y haga clic en **Nueva directiva**.
   Se abrirá el Asistente para una nueva directiva.

6. Siga los pasos del Asistente para una nueva directiva para crear una directiva.

Crear una directiva desde la carpeta Directivas

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Directivas**.
4. En el espacio de trabajo, haga clic en **Nueva directiva**.
   Se abrirá el Asistente para una nueva directiva.
5. Siga los pasos del Asistente para una nueva directiva para crear una directiva.

Para continuar al siguiente paso del asistente, haga clic en **Siguiente**. Para volver al paso anterior del asistente, haga clic en ←. Para salir del asistente en cualquier paso, haga clic en **Cancelar**.

Nota: El aspecto de los botones puede variar en función de la versión de Windows.

Paso 1. Seleccionar una aplicación

En la lista de aplicaciones de la ventana **Seleccione la aplicación para la que desea crear una directiva de grupo**, seleccione **Kaspersky Endpoint Security for Mac (12.2)**.

Paso 2. Especificar el nombre de la directiva

1. En el campo **Nombre** de la ventana **Introducir nombre de directiva de grupo**, especifique el nombre de la directiva que está creando. No se admiten los siguientes símbolos en el nombre: " * < : > ? \ |.
2. Seleccione la casilla de verificación **Usar configuración de directivas para una versión anterior de la aplicación** si desea importar los ajustes de una directiva existente de Kaspersky Endpoint Security en una nueva directiva.

Paso 3. Especificar configuración de protección

En la ventana **Protección**, configure los siguientes ajustes si es necesario:

- Configure los ajustes de protección para el sistema operativo en el equipo cliente.
- Configurar la Zona de confianza.
  Puede crear una lista de objetos que Kaspersky Endpoint Security no analiza ni supervisa.
- Configurar las Aplicaciones de confianza.
  Puede crear una lista de aplicaciones cuya actividad de red y archivos no será supervisada por Kaspersky Endpoint Security.
- Seleccione los tipos de objetos que se detectarán.
- Active o desactive el inicio de las tareas programadas cuando el equipo funcione con batería.
- Limitar el uso de las tareas de análisis de la CPU.

Paso 4. Configurar los ajustes de Protección frente a amenazas en archivos

En la ventana **Protección frente a amenazas en archivos**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas en archivos.
  El componente Protección frente a amenazas en archivos está activado de forma predeterminada.
- Seleccione el nivel de seguridad.
  El nivel de seguridad recomendado por Kaspersky está seleccionado de forma predeterminada.

- Configure el ajuste de Protección frente a amenazas en archivos.
- Seleccione la acción que se realizará cuando se detecte un objeto malicioso.

Paso 5. Configurar los ajustes de Protección frente a amenazas web

En la ventana **Protección frente a amenazas web**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas web.
  El componente Protección frente a amenazas web está activado de forma predeterminada.
- Seleccione el nivel de seguridad.
  El nivel de seguridad recomendado por Kaspersky está seleccionado de forma predeterminada.
- Configure el ajuste de Protección frente a amenazas web.
- Seleccione la acción que se realizará cuando se detecte un objeto malicioso en el tráfico web.

Paso 6. Configurar los ajustes de Protección frente a amenazas en la red

En la ventana **Protección frente a amenazas en la red**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas en la red.
  El componente Protección frente a amenazas en la red está activado de forma predeterminada.
- Configure el ajuste de Protección frente a amenazas en la red.
- Cree o edite una lista de las direcciones IP de los equipos remotos a los cuales Kaspersky Endpoint Security nunca bloquea su actividad de red.

Paso 7. Configurar los ajustes de actualización

En la ventana **Actualizar**, haga lo siguiente si es necesario:

- Active o desactive las actualizaciones de los módulos de la aplicación.
- Especifique los orígenes de actualización.

Paso 8. Configurar los ajustes de KSN

En la ventana **Kaspersky Security Network**, haga lo siguiente si es necesario:

- Para leer el texto completo de la Declaración de Kaspersky Security Network, haga clic en el botón **Declaración de KSN**.
- Vea la información sobre la infraestructura de KSN proporcionada por Kaspersky Security Center.
- Active o desactive el uso de Kaspersky Security Network.
- Active o desactive el modo KSN extendido.
- Active o desactive el uso del proxy de KSN.
- Active o desactive el uso de servidores de Kaspersky cuando el proxy de KSN no esté disponible.

  Nota: El uso de Kaspersky Security Network y un proxy de KSN en equipos remotos solo está disponible si el Servidor de administración de Kaspersky Security Center se utiliza como el servidor proxy. Para obtener información detallada sobre las propiedades del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

  Cuando Kaspersky Security Center utiliza una infraestructura de KSN Global y usted elige participar en Kaspersky Security Network en una configuración de directiva, las estadísticas de Kaspersky Endpoint Security de los equipos cliente a los que se aplica la directiva se envían automáticamente a Kaspersky para mejorar la protección de estos equipos.

Nota: Kaspersky no recibe, procesa ni almacena datos personales sin su consentimiento explícito.

Datos proporcionados a Kaspersky cuando usa Kaspersky Security Network en la infraestructura de KSN global

Si la casilla de verificación **Acepto usar Kaspersky Security Network** está seleccionada y la casilla de verificación **Activar modo KSN extendido** no está seleccionada, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Versión completa del software instalado;

  tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. de dispositivo único; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

Si las casillas de verificación **Acepto usar Kaspersky Security Network** y **Activar modo KSN extendido** están seleccionadas, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información sobre la versión del sistema operativo (SO) y los paquetes de servicios instalados en el ordenador, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del sistema operativo y los parámetros del modo de ejecución del sistema operativo; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO; versión de Service Pack del SO; fecha y hora de inicio del SO; tiempo de demora del procesamiento del evento acerca de la acción del SO en el subsistema de análisis de comportamiento; cantidad de eventos de acción del tipo actual demorados del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactiva; cantidad de eventos de acciones del SO procesados; cantidad de eventos de acción sincrónicos procesados del SO; demora total de todos los eventos de acción del tipo actual del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento de eventos persistentes; demora total de todos los eventos de acción del SO; cantidad de eventos de acción sincrónicos del SO en espera; fecha y hora del evento recibido por una acción en el SO.

- Información sobre el último reinicio fallido del sistema operativo: número de reinicios fallidos.

- Información sobre la aplicación instalada del Titular de los derechos y el estado de la protección antivirus: id. de instalación del software (PCID); versión del registro de la base de datos del software; el identificador único de la instancia de la instalación de la aplicación en el ordenador, el tipo de aplicación, id. del tipo de aplicación, la versión completa de la aplicación instalada, el identificador de la versión de configuración de la aplicación, el identificador del tipo de ordenador, el identificador único del ordenador en el que está instalada la aplicación, el identificador de Usuario único en los servicios del Titular de los derechos, el idioma regional y el estado de funcionamiento, la versión de los componentes de Software instalados y su estado de funcionamiento, la versión del protocolo utilizado para conectarse con los servicios del Titular de los derechos; versión completa del software instalado; tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); cantidad de ciclos de actualizar y aplicar para bases de datos antivirus; fecha y hora de la última actualización y aplicación de las bases de datos antivirus; Fecha y hora de lanzamiento de las bases de datos del software; versión del componente del Software; id. de actualización de software; tipo del software instalado; fecha y hora de inicio de System Watcher; fecha y hora de instalación del software; probabilidad de enviar estadísticas por medio de System Watcher; código del evento que demoró más

del tiempo estándar en ser procesado por System watcher; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo máximo permitido para el procesamiento de un evento por parte de System watcher; tiempo de procesamiento del evento que tardó más tiempo del estándar en ser procesado por System Watcher; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por System Watcher.

- Información sobre todos los objetos y operaciones procesados: veredicto del software del objeto que se procesa; código de directorio; tamaño del objeto que se procesa; suma de control (SHA256) del objeto que se procesa; número del software detectado en el contexto de System Watcher; fecha y hora de detección de software por parte de System Watcher; detectar características; ID del registro activado en las bases de datos Antivirus del software; motivo de detección de software por System Watcher; suma de control (MD5) del objeto que se procesa; resultado de la comprobación de integridad del módulo; nombre del objeto que se procesa; tipo de registro en las bases de datos antivirus del software activado; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; la dirección URL y del referente desde las que se descargó; el tamaño de los archivos analizados y las rutas hasta ellos; la señal del archivo; la fecha y la hora de creación del archivo; el nombre, el tamaño y las sumas de control (MD5, SHA2-256) del compresor (si el archivo estaba comprimido); la entropía del archivo; el tipo de archivo; el código de tipo de archivo; la señal, el ID y el formato del archivo ejecutable; la suma de control del objeto (MD5, SHA2-256); el tipo y el valor de la suma de control complementaria del objeto; datos sobre la firma digital (certificado) del objeto: datos sobre el editor del certificado, número de inicios del objeto desde el envío de la última estadística, ID de la tarea de análisis de la aplicación, los medios para recibir información sobre la reputación del objeto, el valor del filtro de destino, los parámetros técnicos de las tecnologías de detección aplicables; ruta hacia el objeto que se procesa; código de directorio.

- Para archivos ejecutables: la entropía de las secciones del archivo, la marca de verificación de reputación o la marca de la firma del archivo, el nombre, el tipo, el tipo de ID, la suma de comprobación (MD5) y el tamaño de la aplicación cargada por el objeto que se está validando, la ruta de la aplicación y las rutas de las plantillas, un atributo que indica la presencia de la lista de autoejecución, la fecha de entrada, la lista de atributos, el nombre del compresor e información sobre la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME y la fecha y hora de creación del archivo.

- Información sobre las aplicaciones iniciadas y sus módulos: sumas de comprobación (MD5, SHA2-256) de los archivos en ejecución, tamaño, atributos, fecha de creación, nombre del compresor (si el archivo estaba comprimido), nombres de los archivos, información sobre los procesos que se ejecutan en el sistema (identificación del proceso [PID]), nombre del proceso, información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, la ruta completa a los archivos del proceso y la línea de comandos de inicio, una descripción de la aplicación a la que pertenece el proceso (el nombre de la aplicación e información sobre el editor), así como los certificados digitales que se usan e información necesaria para verificar su autenticidad o información sobre la ausencia de firma digital de un archivo e información sobre los módulos cargados en los procesos: sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación (MD5, SHA2-256, SHA1); las rutas a ellos; la información del encabezado de archivo PE; los nombres de los compresores (si se comprimió el archivo); la información sobre la disponibilidad y validez de estas estadísticas y el identificador del modo para generar las estadísticas que se envían.

- En caso de detectar una amenaza o vulnerabilidad, además de la información sobre el objeto escaneado se deberá proporcionar información sobre el identificador, la versión y el tipo de registro en la base de datos del antivirus; el nombre de la amenaza según la clasificación de Kaspersky, la fecha y la hora de la última actualización de la base de datos del antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de aplicación que solicitó la URL y en la cual ocurrió la detección; la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador del tipo de tráfico en el cual fue detectada la amenaza, el identificador de vulnerabilidad y el nivel de la amenaza recibida, la dirección URL y de referencia de la página web en la cual fue detectada la vulnerabilidad.

- Si se detectase un objeto potencialmente malicioso, se proveerá información sobre los datos contenidos en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo que realiza el ataque y número del puerto del equipo del usuario víctima del ataque de red, ID del protocolo de ataque, y nombre y tipo de ataque.

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

- El URL y la dirección IP del sitio web en el cual fue detectado el contenido malicioso o sospechoso; nombre, dimensión y suma de chequeo del archivo que solicitó dicho URL; identificador, peso y grado de aplicación de la norma establecida para dar el veredicto y objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: el estado de finalización de la tarea de actualización, el tipo de error que podría haber ocurrido durante el proceso de actualización, el número de actualizaciones fallidas y el identificador del componente de la aplicación que realiza las actualizaciones.

- Información acerca del uso de Kaspersky Security Network (KSN): el identificador de KSN, el identificador de la aplicación, la versión completa de la aplicación, la dirección IP impersonal del dispositivo del usuario, indicadores del nivel de satisfacción de las solicitudes de KSN, indicadores de la calidad de procesamiento de paquetes de KSN, indicadores del número de solicitudes de KSN e información sobre los tipos de solicitudes de KSN, fecha y hora en que se inició el envío de estadísticas, fecha y hora en que finalizó el envío de estadísticas, información sobre actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida y código de error de la actualización de la configuración.

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se ha detectado el evento, tipo y categoría de evento, nombre de la fuente del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la cual se solicita la reputación y el Referente, la conexión del tipo de protocolo de la conexión, el identificador interno del tipo de aplicación, el número del puerto usado, el identificador del Usuario, la suma de comprobación del archivo escaneado (MD5), el tipo de amenaza detectada, información sobre el registro usado para detectar una amenaza (el identificador del registro para las bases de datos antivirus, el registro de la marca de tiempo y el tipo); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

- Datos sobre la distribución territorial de la aplicación: la fecha de la instalación y activación de la aplicación, el ID del partner que proporciona la licencia para la activación de la aplicación, el ID de la aplicación, el ID de localización de idioma de la aplicación, el número de serie de la licencia de activación de la aplicación y el indicio de participación en KSN.
- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.
- Información sobre el hardware instalado en el equipo: tipo, nombre, nombre del modelo, versión de firmware y parámetros de los dispositivos integrados y conectados.
- Información sobre el dispositivo: ID de dispositivo.
- Información sobre el funcionamiento del componente Control web:

  la versión del componente, el motivo de la categorización, información adicional sobre el motivo de la categorización, la URL categorizada y la dirección IP de host de objeto bloqueado/categorizado.

Cuando Kaspersky Security Center utiliza una infraestructura de KSN Privada y usted elige participar en Kaspersky Security Network en una configuración de directiva, Kaspersky Endpoint Security no envía estadísticas de los equipos cliente a los que se aplica la directiva a Kaspersky.

Después de que se elimine o desactive una directiva, la configuración de KSN en un equipo cliente vuelve al estado original.

Paso 9. Configurar los ajustes de interacción del usuario

En la ventana **Interacción con el usuario**, configure los ajustes de interacción de Kaspersky Endpoint Security con el usuario del equipo cliente si es necesario.

Paso 10. Configurar las preferencias de conexión de red

En la ventana **Red**, haga lo siguiente si es necesario:

- Configuración de la conexión a un servidor proxy.
- Active o desactive el análisis del tráfico HTTPS entrante y saliente.
- Seleccione el almacenamiento de certificados para comprobar el tráfico HTTPS cifrado en el navegador Mozilla Firefox.
- Administre la lista de certificados raíz de confianza.
- Configure los puertos supervisados.

  Puede crear una lista de puertos que supervisará Kaspersky Endpoint Security.

Paso 11. Configuración de los ajustes de Informes y copias de seguridad

En la ventana **Informes y copias de seguridad**, haga lo siguiente si es necesario:

- Configure los ajustes para la generación y el almacenamiento de informes.
- Configure los ajustes de almacenamiento de objetos en el Depósito de copias de seguridad.

Paso 12. Configurar codificación del disco de FileVault

En la ventana **Cifrado de disco de FileVault**, haga lo siguiente si es necesario:

- Active o desactive la administración de cifrado del disco de FileVault para el disco de inicio del usuario.

  De forma predeterminada, la administración de cifrado del disco de FileVault se desactiva.
- Elija la opción **Cifrar disco** si desea cifrar el disco de inicio del usuario cuando la directiva se aplique a un equipo cliente.

Si la casilla **Activar la administración de cifrado de disco de FileVault** no está seleccionada, los usuarios con derechos de administrador pueden cifrar y descifrar los discos de inicio de su Mac desde Ajustes del sistema.

Si la casilla **Activar la administración de cifrado de disco de FileVault** y la opción **Cifrar disco** están seleccionadas, los usuarios con derechos de administrador no pueden descifrar el disco de inicio de su Mac desde Ajustes del sistema.

Si la casilla **Activar la administración de cifrado de disco de FileVault** y la opción **Descifrar disco** están seleccionadas, los usuarios con derechos de administrador no pueden cifrar el disco de inicio de su Mac desde Ajustes del sistema.

Paso 13. Configurar Control Web

En la ventana **Control web**, haga lo siguiente si es necesario:

- Active o desactive el Control Web.

  Nota: Si habilita el control web para bloquear el acceso a recursos web peligrosos, Kaspersky Endpoint Security muestra la notificación de que el **Control web está activado** en el Centro de protección del equipo remoto.
  Kaspersky Endpoint Security muestra notificaciones cuando el usuario accede a los recursos web que bloquea el control web del equipo remoto si la **Comprobar conexiones seguras (HTTPS)** está seleccionada en la ventana **Red** del Asistente de nueva directiva.

- Agregue una nueva regla para Control Web haciendo clic en **Añadir**.

  Puede introducir un nombre de regla, elegir si desea activar la regla, especificar un área de la regla al crear una lista de direcciones web específicas o al seleccionar categorías de sitio web y puede seleccionar una acción para que Kaspersky Endpoint Security realice cuando un usuario ingresa a un sitio web incluido en esta regla.

- Edite, elimine u organice reglas creadas en la lista.

El orden en el que se clasifican las reglas determina la prioridad de su aplicación en Kaspersky Endpoint Security.

Paso 14. Configurar Managed Detection and Response

En la ventana **Managed Detection and Response**, haga lo siguiente si es necesario:

- Active o desactive Managed Detection and Response.

  De forma predeterminada, Managed Detection and Response está desactivada.

- Importe o elimine un archivo de configuración para activar el componente Managed Detection and Response en dispositivos administrados.

Si la casilla de verificación **Managed Detection and Response** está seleccionada y el archivo de configuración MDR está importado, el componente Managed Detection and Response está activo e interactúa con el servicio de Kaspersky Managed Detection and Response. Este servicio detecta y elimina constantemente las amenazas de seguridad que se dirigen a su organización.

Paso 15. Configurar Endpoint Detection and Response (KATA)

En la ventana **Endpoint Detection and Response (KATA)**, haga lo siguiente si es necesario:

- Active o desactive Endpoint Detection and Response (KATA).

  De manera predeterminada, Endpoint Detection and Response (KATA) está desactivado.

- Configure la conexión del servidor y añada un certificado TLS.

- Añada un servidor KATA.

Si la casilla de verificación **Endpoint Detection and Response (KATA)** está seleccionada y se añaden un certificado TLS y un servidor KATA, el componente Endpoint Detection and Response (KATA) está activo e interactúa con la solución Kaspersky Anti Targeted Attack Platform. Esta solución detecta de inmediato amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas y ataques de día cero, entre otras.

Paso 16. Configurar el análisis de discos externos

En la ventana **Análisis de discos externos**, configure los siguientes ajustes:

- La acción que realiza Kaspersky Endpoint Security cuando se conecta un disco externo.

- La acción que realiza Kaspersky Endpoint Security cuando detecta un objeto malicioso.

Paso 17. Configurar Detección de comportamiento

En la ventana **Detección de comportamiento**, haga lo siguiente si es necesario:

- Activar o desactivar la Detección de comportamiento.
  De forma predeterminada, la Detección de comportamiento está activada.
- Seleccione la acción que se realizará cuando se detecte actividad de software malicioso.
- Active o desactive la protección de carpetas compartidas contra el cifrado externo.
  - Seleccione la acción que se realizará cuando se detecte actividad de software malicioso.

Paso 18. Configurar la Protección frente a amenazas en el correo

En la ventana **Protección frente a amenazas en el correo**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas en el correo.
  El componente Protección frente a amenazas en el correo está activado de manera predeterminada.
- Seleccione la acción que se realizará cuando se detecte un objeto malicioso.
- Ajuste la configuración de Protección frente a amenazas en el correo.

Paso 19. Configurar la prevención de exploits

En la ventana **Prevención de exploits**, haga lo siguiente si es necesario:

- Active o desactive la prevención de exploits.
  De manera predeterminada, la Prevención de exploits está activada.
- Seleccione la acción que se realizará cuando se detecte un exploit.

Paso 20. Configurar el motor de reparación

En la ventana **Motor de reparación**, haga lo siguiente si es necesario:

- Active o desactive el motor de reparación.
  De manera predeterminada, el motor de reparación está activado.

Paso 21. Configurar el control de dispositivos

En la ventana **Control de dispositivos**, haga lo siguiente si es necesario:

- Active o desactive el control de dispositivos.
  De manera predeterminada, el control de dispositivos está activado.
- Ajuste la configuración de Control de dispositivos.

Paso 22. Configurar el firewall

En la ventana **Firewall**, haga lo siguiente si es necesario:

- Active o desactive el firewall.
  De manera predeterminada, el firewall está activado.
- Ajuste la configuración del Firewall.

Paso 23. Definir el grupo de administración al cual se aplicará la directiva

En la ventana **Grupo de destino**, haga clic en **Examinar** para seleccionar un grupo de administración al cual desea aplicar la directiva.

Paso 24. Seleccionar el estado de la directiva y completar su creación

En la ventana **Crear una directiva de grupo para la aplicación**, haga lo siguiente:

1. Seleccione el estado que se asignará a la directiva:
   - *Directiva activa*: La directiva se aplica al grupo de administración seleccionado.
   - *Directiva inactiva*: No se aplica la directiva.
   - *Directiva fuera de la oficina*: La directiva se aplica al grupo de administración seleccionado cuando los equipos se desconectan de la red corporativa.

   Nota: Puede crear varias directivas para una aplicación en un grupo de administración, pero solo una puede estar activa.

   Para obtener información detallada sobre los estados de las directivas, consulte la Ayuda de Kaspersky Security Center.
2. Seleccione la casilla de verificación **Una vez creada la directiva, abrir sus propiedades** si desea revisar la configuración de la directiva una vez creada.
3. Haga clic en **Finalizar** para cerrar el Asistente para una nueva directiva.

   La directiva que ha creado aparecerá en la pestaña **Directivas** del espacio de trabajo del grupo de administración correspondiente. La directiva se aplica a los equipos cliente tras la primera sincronización con el Servidor de administración.

Puede editar los ajustes de la directiva que ha creado. También puede impedir o permitir que se realicen cambios en cada grupo de configuración desde un equipo cliente mediante los botones y para cada grupo de configuración. El botón situado junto a un grupo de configuración indica que el usuario de un equipo cliente no tiene permiso para editar estos ajustes en el equipo del usuario. El botón situado junto a un grupo de configuración indica que el usuario de un equipo cliente tiene permiso para editar estos ajustes en el equipo del usuario.

Ver la lista de directivas

Puede crear un número ilimitado de directivas para las aplicaciones instaladas en los equipos de cada grupo de administración, pero solo se podrá aplicar una directiva a cada aplicación cada vez dentro de un grupo de administración.

Ver la lista de directivas de un grupo de administración

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Directivas**.

   Se muestra la lista de directivas.

Configurar los ajustes de la directiva

Expandir todo | Contraer todo

Puede realizar cambios en la directiva que creó en Kaspersky Security Center e impedir que se modifique su configuración en las directivas de subgrupos y tareas.

La configuración de directivas de Kaspersky Endpoint Security incluye la configuración de aplicaciones y de tareas.

Configurar los ajustes de la directiva

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. En el espacio de trabajo, seleccione la pestaña **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y seleccione **Propiedades**.
6. En la ventana **Propiedades: <nombre de directiva>**, configure los ajustes de la directiva:

- En la sección **Protección frente a amenazas básica**

  Configurar el siguiente ajuste de Protección frente a amenazas en archivos

  - Active o desactive el componente Protección frente a amenazas en archivos.
  - Seleccione uno de los niveles de seguridad predefinidos o configure los ajustes de seguridad manualmente.
  - Seleccione la acción que se realizará cuando se detecte un objeto malicioso.

  Configurar el siguiente ajuste de Protección frente a amenazas web

  - Active o desactive el componente Protección frente a amenazas web.
  - Seleccione uno de los niveles de seguridad predefinidos o configure los ajustes de seguridad manualmente.
  - Active o desactive la comprobación de direcciones web con respecto a la base de datos de direcciones web maliciosas.
  - Configure los ajustes de prevención de phishing.
  - Agregue las direcciones de confianza cuyo tráfico no analizará el componente Protección frente a amenazas web.
  - Seleccione la acción que se realizará cuando se detecte un objeto malicioso en el tráfico web.

  Ajustar la siguiente configuración de Protección frente a amenazas en el correo

  - Active o desactive el componente Protección frente a amenazas en el correo.
  - Seleccione la acción que se realizará cuando se detecte un objeto malicioso.
  - Ajuste la configuración de Protección frente a amenazas en el correo.

  Configurar el siguiente ajuste de Protección frente a amenazas en la red

  - Active o desactive el componente Protección frente a amenazas en la red.
  - Configure el ajuste de Protección frente a amenazas en la red.
  - Especifique las direcciones IP de los equipos cuya actividad de red no se bloqueará.

  Ajustar la siguiente configuración del Firewall

  - Active o desactive el firewall.
  - Ajuste la configuración del Firewall.

- En la sección **Protección frente a amenazas avanzada**

  Configurar el siguiente ajuste de KSN

- Para leer el texto completo de la Declaración de Kaspersky Security Network, haga clic en **Declaración de KSN**.
- Active o desactive el uso de Kaspersky Security Network.
- Active o desactive el modo KSN extendido.
- Active o desactive el modo Nube.
- Active o desactive el uso del proxy de KSN.
- Active o desactive el uso de servidores de Kaspersky cuando el proxy de KSN no esté disponible.

Nota: El uso de Kaspersky Security Network y un proxy de KSN en equipos remotos solo está disponible si el Servidor de administración de Kaspersky Security Center se utiliza como el servidor proxy. Para obtener información detallada sobre las propiedades del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

Configure los siguientes ajustes de la Detección de comportamiento

- Activar o desactivar la Detección de comportamiento.
  De forma predeterminada, la Detección de comportamiento está activada.
- Seleccione la acción que se realizará cuando se detecte actividad de software malicioso.

Ajustar la siguiente configuración de prevención de exploits

- Active o desactive la prevención de exploits.
- Seleccione la acción que se realizará cuando se detecte un exploit.

Ajustar la siguiente configuración del motor de reparación

Active o desactive el motor de reparación.

- En la sección **Controles de seguridad**

  Ajustar la siguiente configuración de Control de dispositivos

  - Active o desactive el control de dispositivos.
  - Ajuste la configuración de Control de dispositivos.

  Configurar el siguiente ajuste de Control Web

  - Active o desactive el Control Web.
  - Agregue una nueva regla para Control Web haciendo clic en **Añadir**.
  - Edite, elimine u organice reglas creadas en la lista.

- En la sección **Cifrado de datos**

  Configurar el siguiente ajuste del cifrado de disco de FileVault

  - Active o desactive la administración de cifrado de disco de FileVault para los equipos cliente.
  - Cifre o descifre el disco de inicio en los equipos cliente.

Si la casilla **Activar la administración de cifrado de disco de FileVault** no está seleccionada, los usuarios con derechos de administrador pueden cifrar y descifrar los discos de inicio de su Mac desde Ajustes del sistema.

Si la casilla **Activar la administración de cifrado de disco de FileVault** y la opción **Cifrar disco** están seleccionadas, los usuarios con derechos de administrador no pueden descifrar el disco de inicio de su Mac desde Ajustes del sistema.

Si la casilla **Activar la administración de cifrado de disco de FileVault** y la opción **Descifrar disco** están seleccionadas, los usuarios con derechos de administrador no pueden cifrar el disco de inicio de su Mac desde Ajustes del sistema.

- En la sección **Detection and Response**

  Configure los siguientes parámetros en Managed Detection and Response

  - Active o desactive Managed Detection and Response.
  - Importar o eliminar un archivo de configuración que se utiliza para activar el componente Managed Detection and Response en dispositivos administrados.

  Configure los siguientes ajustes de Endpoint Detection and Response (KATA)

  - Active o desactive Endpoint Detection and Response (KATA).
  - Configure la conexión del servidor y añada un certificado TLS.
  - Añada un servidor KATA.

- En la sección **Tareas locales**

  Configure los siguientes ajustes del Análisis de discos externos

  - La acción que realiza Kaspersky Endpoint Security cuando se conecta un disco externo.
  - La acción que realiza Kaspersky Endpoint Security cuando detecta un objeto malicioso.

- En la sección **Actualizar**

  Configurar el siguiente ajuste de Actualización

  - Active o desactive las actualizaciones de los módulos de aplicación.
  - Especifique los orígenes de actualización.

- En la sección **Configuración adicional**

  Configurar el siguiente ajuste de protección

  - Active o desactive la protección en tiempo real del equipo cliente.
  - Active o desactive el inicio de Kaspersky Endpoint Security cuando se inicie el equipo cliente.
  - Configurar la Zona de confianza.
  - Configurar las Aplicaciones de confianza.
  - Seleccione los tipos de objetos que se detectarán.
  - Active o desactive el inicio de las tareas programadas cuando el equipo funcione con batería.

  Configurar el siguiente ajuste de red

  - Active o desactive el uso de un servidor proxy.
  - Especifique la dirección del servidor proxy.

- Active o desactive el uso de un servidor proxy para direcciones locales.
- Especifique el nombre de usuario y la contraseña para la autenticación del servidor proxy.
- Active o desactive el análisis del tráfico HTTPS entrante y saliente.
- Seleccione el almacén de certificados para comprobar el tráfico HTTPS cifrado en el navegador Mozilla Firefox.
- Configure los puertos supervisados.

Configurar los siguientes ajustes de Informes y copias de seguridad

- Active o desactive el guardado de eventos no críticos en el informe.
- Active o desactive el guardado de eventos recientes solamente.
- Active o desactive la eliminación de eventos tras el período especificado.
- Especifique el período de almacenamiento de eventos.
- Active o desactive la eliminación de objetos del Depósito de copias de seguridad tras el período especificado.
- Especifique el período de almacenamiento de objetos en el Depósito de copias de seguridad.

Configurar el siguiente ajuste de interacción con el usuario

- Active o desactive las notificaciones de eventos.
- Seleccione la forma en la que Kaspersky Endpoint Security notificará los eventos al usuario.
- Active o desactive la visualización del icono de Kaspersky Endpoint Security en la barra de menús.
- Configure si un usuario puede abrir la ventana principal de Kaspersky Endpoint Security y usar la interfaz de la aplicación en el equipo cliente.
- Active o desactive la disponibilidad del elemento **Salir** en el menú de acceso directo del icono de Kaspersky Endpoint Security del equipo cliente.
- Seleccione el idioma utilizado para mostrar los eventos de Kaspersky Security Center.
- Configure los ajustes de Kaspersky Endpoint Security disponibles para los usuarios del equipo cliente.
- Configure la Protección con contraseña para limitar las acciones no deseadas en los dispositivos de los usuarios.

7. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana de propiedades de la directiva.

Cambiar el estado de una directiva

Un estado de directiva define el funcionamiento de una directiva. La directiva puede tener los estados activa, ausente o inactiva. Puede cambiar el estado de la directiva en la configuración de directivas.

Cambiar el estado de una directiva

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Directivas**.
6. Haga clic derecho en la directiva cuyo estado quiere modificar y elija **Propiedades** en el menú contextual.

7. En la ventana **Propiedades: <nombre de la directiva>**, seleccione la sección **General**.
8. En la sección **Estado de la directiva**, seleccione uno de los siguientes estados de directivas:
   - **Directiva activa**. La directiva se aplica siempre al grupo de administración seleccionado.
   - **Directiva fuera de la oficina**. La directiva se aplica al grupo de administración seleccionado cuando los equipos cliente se desconectan de la red corporativa.
   - **Directiva inactiva**. La directiva no se aplica al grupo de administración seleccionado.
9. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Propiedades: <nombre de la directiva>**.

Exportación de una directiva a un archivo KLP

Puede exportar una directiva personalizada a un archivo para usarla en otro Servidor de administración.

Exportación de una directiva a un archivo KLP

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Directivas**.
6. Haga clic con el botón derecho del ratón en la directiva para mostrar su menú contextual y elegir **Exportar**.
   Se abre la ventana **Guardar como**.
7. Seleccione la carpeta en la cual quiere guardar el archivo KLP de la directiva.
8. Especifique el nombre de archivo.
9. Haga clic en **Guardar** para guardar el archivo en la carpeta seleccionada.

Importar una directiva desde un archivo KLP

Puede importar una directiva existente con una configuración predefinida desde un archivo.

Importar una directiva desde un archivo KLP

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. En el espacio de trabajo, seleccione la pestaña **Directivas**.
6. Abra la ventana de selección de archivos de una de estas maneras:
   - Haciendo clic en el botón **Importar directiva desde archivo**.
   - Haciendo clic con el botón derecho del ratón en un área vacía del espacio de trabajo para abrir el menú contextual y seleccionando el elemento **Importar**.
7. Seleccione un archivo KLP con una directiva y haga clic en **Abrir**.

La directiva importada se agregará a la lista de directivas del espacio de trabajo.

Crear y administrar perfiles de directivas

Un perfil de directiva es un conjunto de ajustes variables para una directiva, que se activa en un equipo cliente cuando se cumplen las condiciones específicas. La activación de un perfil modifica los ajustes de la directiva que estén activos en el dispositivo cuando se activa el perfil de directiva.

Crear un perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración para el que desea crear un perfil de directiva.
2. En el espacio de trabajo, seleccione la pestaña **Directivas**.
3. Siga uno de los procedimientos siguientes para abrir las propiedades de la directiva para la que desea crear un perfil:
   - Haga doble clic en el nombre de la directiva.
   - Haga doble clic con el botón derecho del ratón en el nombre de la directiva para mostrar el menú contextual y elija **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva**.
4. En la ventana **Propiedades: <nombre de directiva>**, seleccione la sección **Perfiles de directiva**.
5. En el espacio de trabajo, haga clic en **Agregar**.
6. En la ventana **Asignación de perfiles de directiva**, lea la información sobre directivas y haga clic en el botón **Siguiente**.
   Si no desea que se muestre esta ventana cuando cree nuevos perfiles de directiva, seleccione la casilla de verificación **No mostrar esta ventana otra vez** antes de hacer clic en el botón **Siguiente**.
7. En la ventana **Nombre de perfil de directiva**, configure el perfil de directiva:
   - Introduzca el nombre del nuevo perfil de directiva.

     Nota: El nombre de un perfil no puede incluir más de 100 caracteres.

   - En la sección **Estado del perfil de directiva**, seleccione si el perfil de directiva está activado o desactivado.
   - En la lista desplegable de la sección **Estado del perfil de directiva**, seleccione si puede editarse el perfil de directiva.
   - Si desea configurar reglas de activación para el perfil de directiva, seleccione la casilla de verificación **Después de cerrar el nuevo asistente de perfiles de directivas, proceder con la configuración de la regla de activación de perfiles de directivas**.
8. Haga clic en **Finalizar**.
9. Si ha seleccionado la casilla de verificación **Después de cerrar el nuevo asistente de perfiles de directivas, proceda a configurar la regla de activación de perfiles de directivas**, realice los pasos que indica el asistente de regla de activación de perfil de directiva.

El perfil de directiva que ha creado se muestra en la sección **Perfiles de directiva** en la ventana **Propiedades: <nombre de directiva>**.

Crear una regla de activación del perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración para el que desea crear una regla de activación del perfil de directiva.
2. En el espacio de trabajo, seleccione la pestaña **Directivas**.
3. Realice alguna de las siguientes acciones para abrir las propiedades de la directiva:
   - Haga doble clic en el nombre de la directiva.
   - Haga doble clic con el botón derecho del ratón en el nombre de la directiva para mostrar el menú contextual y elija **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva**.
4. En la ventana **Propiedades: <nombre de directiva>**, seleccione la sección **Perfiles de directiva**.
5. En el espacio de trabajo, seleccione el perfil de directiva para la que desea crear una regla de activación y haga clic en **Propiedades**.
   Se abre la ventana **Propiedades: <nombre del perfil de directiva>**.
6. Seleccione la sección **Reglas de activación**.
7. En el espacio de trabajo, haga clic en **Agregar**.

Se inicia el asistente de regla de activación de perfil de directiva.

Siga los pasos que indica este asistente.

Modificar un perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración en el que desea modificar un perfil de directiva.
2. En el espacio de trabajo, seleccione la pestaña **Directivas**.
3. Siga uno de los procedimientos siguientes para abrir las propiedades de la directiva para la que desea modificar un perfil:
   - Haga doble clic en el nombre de la directiva.
   - Haga doble clic con el botón derecho del ratón en el nombre de la directiva para mostrar el menú contextual y elija **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva**.
4. En la ventana **Propiedades: <nombre de directiva>**, seleccione la sección **Perfiles de directiva**.
5. En el espacio de trabajo, seleccione el perfil de directiva que desea modificar y haga clic en **Propiedades**.
   Se abre la ventana **Propiedades: <nombre del perfil de directiva>**.
6. Configure el perfil si es necesario:
   - En la sección **General**, modifique el nombre del perfil, o actívelo o desactívelo marcando o desmarcando la casilla de verificación **Activar perfil**.
   - En la sección **Reglas de activación**, cree, edite o elimine las reglas de activación.
   - En la sección **Dispositivos**, elija los dispositivos a los que se aplica el perfil de directiva.
   - Modifique los ajustes de directiva en las secciones relevantes.
7. Haga clic en **Aceptar**.

Si el perfil de directiva está activo, los ajustes modificados se aplicarán cuando el equipo cliente se haya sincronizado con el Servidor de administración. Si el perfil de directiva está inactivo, se aplicarán tras activarse la regla de activación.

Modificar la prioridad de un perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración para el que desea cambiar la prioridad de un perfil de directiva.
2. En el espacio de trabajo, seleccione la pestaña **Directivas**.
3. Siga uno de los procedimientos a continuación para abrir las propiedades de la directiva para la que desea cambiar la prioridad de un perfil de directiva:
   - Haga doble clic en el nombre de la directiva.
   - Haga doble clic con el botón derecho del ratón en el nombre de la directiva para mostrar el menú contextual y elija **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva**.
4. En la ventana **Propiedades: <nombre de directiva>**, seleccione la sección **Perfiles de directiva**.
5. En el espacio de trabajo, seleccione el perfil de directiva cuya prioridad desea modificar.
6. Para aumentar o reducir la prioridad del perfil seleccionado, haga clic en los botones .

Suprimir un perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración del que desea eliminar un perfil de directiva.
2. En el espacio de trabajo, seleccione la pestaña **Directivas**.

3. Siga uno de los procedimientos a continuación para abrir las propiedades de la directiva para la que desea eliminar un perfil:
   - Haga doble clic en el nombre de la directiva.
   - Haga doble clic con el botón derecho del ratón en el nombre de la directiva para mostrar el menú contextual y elija **Propiedades**.
   - Haga clic en el vínculo **Configurar directiva**.
4. En la ventana **Propiedades: <nombre de directiva>**, seleccione la sección **Perfiles de directiva**.
5. En el espacio de trabajo, seleccione el perfil que desea eliminar y haga clic en el botón **Eliminar**.

Para obtener información detallada sobre los perfiles de directivas, consulte la Ayuda de Kaspersky Security Center.

Generar un informe sobre objetos detectados

Generar un informe sobre objetos detectados

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Dispositivos administrados**.
4. Seleccione el grupo de administración que contiene el equipo cliente requerido.
5. Seleccione la pestaña **Dispositivos**.
6. Seleccione el equipo de la lista de equipos cliente.
7. Haga clic derecho en el equipo seleccionado para abrir el menú contextual y elegir **Todas las tareas** > **Ver el informe de amenazas**.

Se abrirá el informe generado en una ventana del navegador.

Puede encontrar información sobre otras formas de generar un informe de objetos que la aplicación detecta en el equipo cliente en la Ayuda de Kaspersky Security Center.

Obtener una clave de recuperación para un disco cifrado

Si un usuario de un equipo cliente se olvida o pierde sus credenciales y no puede acceder a un disco cifrado, puede obtener una clave de recuperación.

Obtener una clave de recuperación

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo **Servidor de administración <nombre del servidor>**.
3. En el árbol de la consola, seleccione la carpeta **Avanzado**, la subcarpeta **Protección y cifrado de datos** y, a continuación, la subcarpeta **Dispositivos cifrados**.
4. En el espacio de trabajo, haga clic con el botón derecho en el dispositivo con el disco cifrado para mostrar el menú de acceso directo y seleccione **Obtener clave de recuperación para macOS**.

   Se abrirá una ventana con la clave de recuperación.
5. Guarde la clave de recuperación de cualquier manera conveniente.

Puede usar esta clave de recuperación en un equipo cliente para acceder al disco cifrado.

Administración remota de la aplicación a través de Kaspersky Security Center Web Console y Cloud Console

Kaspersky Security Center Web Console (Web Console) es una aplicación web diseñada para realizar de manera centralizada las principales tareas que se requieren para administrar y mantener el sistema de seguridad de la red de una organización. Web Console es un componente de Kaspersky Security Center que proporciona una interfaz de usuario para administrar Kaspersky Endpoint Security en una ventana del navegador. Para obtener información detallada sobre Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

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

También puede administrar Kaspersky Endpoint Security a través de la interfaz gráfica de usuario de la aplicación, la Consola de administración de Kaspersky Security Center y la línea de comandos.

Instalación del complemento web de Kaspersky Endpoint Security

El complemento web de Kaspersky Endpoint Security permite la interacción entre Kaspersky Endpoint Security y Kaspersky Security Center. El complemento web debe instalarse en un dispositivo que tenga instalado Kaspersky Security Center Web Console. La funcionalidad del complemento web está disponible para todos los administradores que tienen acceso a Kaspersky Security Center Web Console en un navegador.

Puede instalar el complemento web de la siguiente manera:

- Con el Asistente de inicio rápido de Kaspersky Security Center Web Console.

  Web Console le solicita automáticamente que ejecute el Asistente de inicio rápido cuando conecta Web Console al Servidor de administración por primera vez. También puede ejecutar el Asistente de inicio rápido en la interfaz de Web Console (**Descubrimiento y despliegue** → **Despliegue y asignación** → **Asistente de inicio rápido**). El Asistente de inicio rápido también puede comprobar si los complementos web instalados están actualizados y descargar las actualizaciones necesarias. Para obtener más información sobre el Asistente de inicio rápido para Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

- Manualmente, con un paquete de distribución en Web Console desde una fuente externa.

  Para instalar el complemento web, añada el archivo comprimido ZIP del paquete de distribución para el complemento web de Kaspersky Endpoint Security en la interfaz de Web Console: **Ajustes de la consola** > **Complementos web**. El paquete de distribución del complemento web se puede descargar en el sitio web de Kaspersky.

Para instalar el complemento web de Kaspersky Endpoint Security manualmente:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Ajustes de la consola** > **Complementos web**.

   Se abre una lista de complementos web instalados.

2. Inicie la instalación del complemento web de Kaspersky Endpoint Security de una de las siguientes maneras:

   - Instalación desde la lista de complementos web de Kaspersky:

     a. Haga clic en **Agregar**.

        Se abre una lista de todos los complementos web de Kaspersky disponibles. La lista se actualiza automáticamente después de que se publican nuevas versiones de complementos web.

     b. Busque el complemento web de Kaspersky Endpoint Security for Mac 12.2 en la lista y haga clic en su nombre.

     c. En la ventana que se abre con una descripción del complemento web, haga clic en el botón **Instalar complemento**.

     d. Espere a que se complete la instalación y haga clic en **Aceptar** en la ventana de información.

   - Instalación del complemento web desde una fuente externa (los archivos comprimidos necesarios para instalar los complementos web se incluyen en el kit de distribución):

     a. Haga clic en el botón **Añadir desde archivo**.

     b. En la ventana que se abre, especifique la ruta al archivo comprimido ZIP con el kit de distribución para el complemento web y la ruta al archivo de firma en formato TXT. Este archivo está en el archivo comprimido con el complemento web.

     c. Haga clic en **Agregar**.

     d. Espere a que se complete la instalación y haga clic en **Aceptar** en la ventana de información.

   El nuevo complemento se muestra en la lista de complementos web instalados (**Ajustes de la consola** > **Complementos web**).

Nota: Si selecciona un idioma que no está incluido en el paquete de distribución de Kaspersky Endpoint Security en las propiedades del Servidor de administración de Kaspersky Security Center, el Contrato de licencia y toda la interfaz de Kaspersky Security Center Web Console se mostrarán en inglés.

Crear directivas

Esta sección contiene información sobre cómo crear y configurar directivas para Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console y Cloud Console.

Una directiva determina la configuración de una aplicación y administra la capacidad de configurar esa aplicación en equipos de un grupo de administración. Es necesario crear una directiva individual para cada aplicación. Puede crear múltiples directivas para las aplicaciones instaladas en los equipos de cada grupo de administración, pero solo se podrá aplicar una directiva a cada aplicación cada vez dentro de un grupo de administración.

Nota: A la hora de crear y configurar una directiva, puede impedir o permitir que se introduzcan cambios en cada grupo de ajustes de las directivas mediante el conmutador **Aplicar**.

Crear una directiva

1. En la sección **Dispositivos** a la izquierda, seleccione la sección **Directivas y perfiles**.
2. Haga clic en **Agregar**.
3. Seleccione la aplicación para la cual desea crear una directiva y haga clic en **Siguiente**.

   Se abrirá la ventana **Nueva directiva**.
4. En la pestaña **General**, especifique el nombre de la directiva y configure el estado de la directiva y las opciones de herencia de los ajustes de la directiva.
5. En la pestaña **Ajustes de la aplicación**, configure los parámetros de la aplicación que se aplicarán a Kaspersky Endpoint Security en el equipo cliente cuando se aplique la directiva.
6. Haga clic en **Guardar**.

Puede realizar las siguientes acciones en las tareas personalizadas:

- Crear directivas
- Configurar directivas
- Copiar o mover directivas de un grupo a otro
- Eliminar directivas
- Cambiar el estado de las directivas

Para obtener información detallada sobre las directivas de Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

Para obtener información detallada sobre las directivas de Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Nota: Después de crear un perfil de directiva para una directiva de Kaspersky Endpoint Security mediante Kaspersky Security Center Web Console y Cloud Console, deberá verificar que la configuración se aplique correctamente en los equipos cliente.

Configure el ajuste de Protección frente a amenazas avanzadas

En la sección **Protección frente a amenazas avanzadas**, puede elegir si Kaspersky Endpoint Security en equipos cliente participa en Kaspersky Security Network y configurar el uso del proxy de KSN.

Haga lo siguiente si es necesario:

- Para leer el texto completo de la Declaración de Kaspersky Security Network, haga clic en el vínculo **Declaración de KSN**.
- Para ver la información sobre la infraestructura de KSN proporcionada por Kaspersky Security Center, haga clic en el vínculo **Declaración de KSN**.

  Nota: La infraestructura de KSN Global se usa en Kaspersky Security Center de forma predeterminada. Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console y según los ajustes de Kaspersky Security Center, puede participar en Kaspersky Private Security Network en lugar de Kaspersky Security Network. Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la participación en Kaspersky Private Security Network no está disponible. Para obtener información detallada sobre la participación en Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center.
- Active o desactive el uso de Kaspersky Security Network.
- Active o desactive el modo KSN extendido.

- Activar/desactivar el modo Nube.
- Active o desactive el uso del proxy de KSN.
- Active o desactive el uso de servidores de Kaspersky cuando el proxy de KSN no esté disponible.

Nota: Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console, el uso de Kaspersky Security Network y un proxy de KSN en equipos remotos solo está disponible si el servidor de administración de Kaspersky Security Center se utiliza como el servidor proxy. Para obtener información detallada sobre las propiedades del Servidor de administración, consulte la Ayuda de Kaspersky Security Center. Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, puede usar Kaspersky Security Network y un proxy de KSN en equipos remotos a través de puntos de distribución que ejecuten un sistema operativo Windows.

Cuando Kaspersky Security Center utiliza una infraestructura de KSN Global y usted elige participar en Kaspersky Security Network en una configuración de directiva, las estadísticas de Kaspersky Endpoint Security de los equipos cliente a los que se aplica la directiva se envían automáticamente a Kaspersky para mejorar la protección de estos equipos.

Nota: Kaspersky no recibe, procesa ni almacena datos personales sin su consentimiento explícito.

Datos proporcionados a Kaspersky cuando usa Kaspersky Security Network en la infraestructura de KSN global

Si el conmutador **Kaspersky Security Network** está activado y el conmutador **Modo KSN extendido** está desactivado, Kaspersky Endpoint Security que se ejecuta en los equipos cliente proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.
- Versión completa del software instalado;

  tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. de dispositivo único; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

Si los conmutadores **Kaspersky Security Network** y **Modo KSN extendido** están activados, Kaspersky Endpoint Security que se ejecuta en los equipos cliente proporciona a Kaspersky los siguientes datos:

- Información sobre la versión del sistema operativo (SO) y los paquetes de servicios instalados en el ordenador, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del sistema operativo y los parámetros del modo de ejecución del sistema operativo; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO; versión de Service Pack del SO; fecha y hora de inicio del SO; tiempo de demora del procesamiento del evento acerca de la acción del SO en el subsistema de análisis de comportamiento; cantidad de eventos de acción del tipo actual demorados del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactiva; cantidad de eventos de acciones del SO procesados; cantidad de eventos de acción sincrónicos procesados del SO; demora total de todos los eventos de acción del tipo actual del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento de eventos persistentes; demora total de todos los eventos de acción del SO; cantidad de eventos de acción sincrónicos del SO en espera; fecha y hora del evento recibido por una acción en el SO.
- Información sobre el último reinicio fallido del sistema operativo: número de reinicios fallidos.
- Información sobre la aplicación instalada del Titular de los derechos y el estado de la protección antivirus: id. de instalación del software (PCID); versión del registro de la base de datos del software; el identificador único de la instancia de la instalación de la aplicación en el ordenador, el tipo de aplicación, id. del tipo de aplicación, la versión completa de la aplicación instalada, el identificador de la versión de configuración de la aplicación, el identificador del tipo de ordenador, el identificador único del ordenador en el que está instalada la aplicación, el identificador de Usuario único en los servicios del Titular de los derechos, el idioma regional y el estado de funcionamiento, la versión de los componentes de Software instalados y su estado de funcionamiento, la versión del protocolo utilizado para conectarse con los servicios del Titular de los derechos; versión completa del software instalado; tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID

del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); cantidad de ciclos de actualizar y aplicar para bases de datos antivirus; fecha y hora de la última actualización y aplicación de las bases de datos antivirus; Fecha y hora de lanzamiento de las bases de datos del software; versión del componente del Software; id. de actualización de software; tipo del software instalado; fecha y hora de inicio de System Watcher; fecha y hora de instalación del software; probabilidad de enviar estadísticas por medio de System Watcher; código del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo máximo permitido para el procesamiento de un evento por parte de System watcher; tiempo de procesamiento del evento que tardó más tiempo del estándar en ser procesado por System Watcher; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por System Watcher.

- Información sobre todos los objetos y operaciones procesados: veredicto del software del objeto que se procesa; código de directorio; tamaño del objeto que se procesa; suma de control (SHA256) del objeto que se procesa; número del software detectado en el contexto de System Watcher; fecha y hora de detección de software por parte de System Watcher; detectar características; ID del registro activado en las bases de datos Antivirus del software; motivo de detección de software por System Watcher; suma de control (MD5) del objeto que se procesa; resultado de la comprobación de integridad del módulo; nombre del objeto que se procesa; tipo de registro en las bases de datos antivirus del software activado; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; la dirección URL y del referente desde las que se descargó; el tamaño de los archivos analizados y las rutas hasta ellos; la señal del archivo; la fecha y la hora de creación del archivo; el nombre, el tamaño y las sumas de control (MD5, SHA2-256) del compresor (si el archivo estaba comprimido); la entropía del archivo; el tipo de archivo; el código de tipo de archivo; la señal, el ID y el formato del archivo ejecutable; la suma de control del objeto (MD5, SHA2-256); el tipo y el valor de la suma de control complementaria del objeto; datos sobre la firma digital (certificado) del objeto: datos sobre el editor del certificado, número de inicios del objeto desde el envío de la última estadística, ID de la tarea de análisis de la aplicación, los medios para recibir información sobre la reputación del objeto, el valor del filtro de destino, los parámetros técnicos de las tecnologías de detección aplicables; ruta hacia el objeto que se procesa; código de directorio.

- Para archivos ejecutables: la entropía de las secciones del archivo, la marca de verificación de reputación o la marca de la firma del archivo, el nombre, el tipo, el tipo de ID, la suma de comprobación (MD5) y el tamaño de la aplicación cargada por el objeto que se está validando, la ruta de la aplicación y las rutas de las plantillas, un atributo que indica la presencia de la lista de autoejecución, la fecha de entrada, la lista de atributos, el nombre del compresor e información sobre la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME y la fecha y hora de creación del archivo.

- Información sobre las aplicaciones iniciadas y sus módulos: sumas de comprobación (MD5, SHA2-256) de los archivos en ejecución, tamaño, atributos, fecha de creación, nombre del compresor (si el archivo estaba comprimido), nombres de los archivos, información sobre los procesos que se ejecutan en el sistema (identificación del proceso [PID]), nombre del proceso, información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, la ruta completa a los archivos del proceso y la línea de comandos de inicio, una descripción de la aplicación a la que pertenece el proceso (el nombre de la aplicación e información sobre el editor), así como los certificados digitales que se usan e información necesaria para verificar su autenticidad o información sobre la ausencia de firma digital de un archivo e información sobre los módulos cargados en los procesos: sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación (MD5, SHA2-256, SHA1); las rutas a ellos; la información del encabezado de archivo PE; los nombres de los compresores (si se comprimió el archivo); la información sobre la disponibilidad y validez de estas estadísticas y el identificador del modo para generar las estadísticas que se envían.

- En caso de detectar una amenaza o vulnerabilidad, además de la información sobre el objeto escaneado se deberá proporcionar información sobre el identificador, la versión y el tipo de registro en la base de datos del antivirus; el nombre de la amenaza según la clasificación de Kaspersky, la fecha y la hora de la última actualización de la base de datos del antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de aplicación que solicitó la URL y en la cual ocurrió la detección; la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador del tipo de tráfico en el cual fue detectada la amenaza, el identificador de vulnerabilidad y el nivel de la amenaza recibida, la dirección URL y de referencia de la página web en la cual fue detectada la vulnerabilidad.

- Si se detectase un objeto potencialmente malicioso, se proveerá información sobre los datos contenidos en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo que realiza el ataque y número del puerto del equipo del usuario víctima del ataque de red, ID del protocolo de ataque, y nombre y tipo de ataque.

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

- El URL y la dirección IP del sitio web en el cual fue detectado el contenido malicioso o sospechoso; nombre, dimensión y suma de chequeo del archivo que solicitó dicho URL; identificador, peso y grado de aplicación de la norma establecida para dar el veredicto y objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: el estado de finalización de la tarea de actualización, el tipo de error que podría haber ocurrido durante el proceso de actualización, el número de actualizaciones fallidas y el identificador del componente de la aplicación que realiza las actualizaciones.

- Información acerca del uso de Kaspersky Security Network (KSN): el identificador de KSN, el identificador de la aplicación, la versión completa de la aplicación, la dirección IP impersonal del dispositivo del usuario, indicadores del nivel de satisfacción de las solicitudes de KSN, indicadores

de la calidad de procesamiento de paquetes de KSN, indicadores del número de solicitudes de KSN e información sobre los tipos de solicitudes de KSN, fecha y hora en que se inició el envío de estadísticas, fecha y hora en que finalizó el envío de estadísticas, información sobre actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida y código de error de la actualización de la configuración.

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se ha detectado el evento, tipo y categoría de evento, nombre de la fuente del evento y descripción del evento.
- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la cual se solicita la reputación y el Referente, la conexión del tipo de protocolo de la conexión, el identificador interno del tipo de aplicación, el número del puerto usado, el identificador del Usuario, la suma de comprobación del archivo escaneado (MD5), el tipo de amenaza detectada, información sobre el registro usado para detectar una amenaza (el identificador del registro para las bases de datos antivirus, el registro de la marca de tiempo y el tipo); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.
- Datos sobre la distribución territorial de la aplicación: la fecha de la instalación y activación de la aplicación, el ID del partner que proporciona la licencia para la activación de la aplicación, el ID de la aplicación, el ID de localización de idioma de la aplicación, el número de serie de la licencia de activación de la aplicación y el indicio de participación en KSN.
- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.
- Información sobre el hardware instalado en el equipo: tipo, nombre, nombre del modelo, versión de firmware y parámetros de los dispositivos integrados y conectados.
- Información sobre el dispositivo: ID de dispositivo.
- Información sobre el funcionamiento del componente Control web:

  la versión del componente, el motivo de la categorización, información adicional sobre el motivo de la categorización, la URL categorizada y la dirección IP de host de objeto bloqueado/categorizado.

Cuando Kaspersky Security Center utiliza una infraestructura de KSN Privada y usted elige participar en Kaspersky Security Network en una configuración de directiva, Kaspersky Endpoint Security no envía estadísticas de los equipos cliente a los que se aplica la directiva a Kaspersky.

Configure el ajuste de Protección frente a amenazas básicas

En la sección **Protección frente a amenazas básicas**, puede configurar los siguientes componentes:

- Protección frente a amenazas en archivos
- Protección frente a amenazas web
- Protección frente a amenazas en la red

Puede abrir una ventana para configurar los ajustes de los componentes al hacer clic en el vínculo correspondiente.

Configure el ajuste de Protección frente a amenazas en archivos

En la ventana **Protección frente a amenazas en archivos**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas en archivos.
  El componente Protección frente a amenazas en archivos está activado de forma predeterminada.
- Creación de una cobertura de protección.
- Seleccione la acción que se realizará cuando se detecte un objeto malicioso.
- Seleccione si Kaspersky Endpoint Security analizará solo los archivos nuevos y modificados o todos los archivos.
- Seleccione si Kaspersky Endpoint Security omitirá el análisis de volumen del sistema de solo lectura en los equipos cliente.
- Seleccione si Kaspersky Endpoint Security utilizará la tecnología iSwift al analizar los archivos.

  Nota: iSwift permite a Kaspersky Endpoint Security usar un algoritmo especial para excluir algunos objetos del análisis, con objeto de aumentar la velocidad del análisis.

- Seleccione qué tipos de archivos analizará Kaspersky Endpoint Security.
- Seleccione las acciones que Kaspersky Endpoint Security realiza para los archivos compuestos.

Configure el ajuste de Protección frente a amenazas web

En la ventana **Protección frente a amenazas web**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas web.
  El componente Protección frente a amenazas web está activado de forma predeterminada.
- Seleccione la acción que se realizará cuando se detecte un objeto malicioso en el tráfico web.
- Cree o modifique una lista de direcciones web de confianza.

Configure el ajuste de Protección frente a amenazas en la red

En la ventana **Protección frente a amenazas en la red**, haga lo siguiente si es necesario:

- Active o desactive el componente Protección frente a amenazas en la red.
  El componente Protección frente a amenazas en la red está activado de forma predeterminada.
- Active o desactive el bloqueo de los equipos atacantes.
- Cree o edite una lista de las direcciones IP de los equipos remotos a los cuales Kaspersky Endpoint Security nunca bloquea su actividad de red.

Configure los Controles de seguridad

En la sección **Controles de seguridad**, haga lo siguiente si es necesario:

- Active o desactive el Control Web.

  Nota: Si activa el Control Web para bloquear el acceso a recursos web peligrosos, Kaspersky Endpoint Security muestra la notificación **Control web está activado** en el Centro de protección en el equipo remoto.
  Kaspersky Endpoint Security muestra notificaciones cuando el usuario accede a recursos web bloqueados por Control Web en el equipo remoto si el conmutador **Comprobación de conexiones seguras (HTTPS)** está activado en la ventana **Red** del Asistente para una nueva directiva.

- Agregue reglas que definirán qué direcciones web o categorías de sitio web supervisará y administrará el Control Web en el equipo de un usuario.
- Edite, elimine u organice reglas creadas en la lista.

El orden en el que se clasifican las reglas determina la prioridad de su aplicación en Kaspersky Endpoint Security.

Configurar el cifrado de datos

En la sección **Cifrado de datos**, puede activar o desactivar el cifrado de los discos de inicio del equipo cliente para evitar que usuarios tengan acceso no autorizado a datos confidenciales. De forma predeterminada, el cifrado del disco de FileVault se desactiva.

Configurar los ajustes de Detection and Response

En la sección **Detection and Response**, puede configurar los siguientes componentes:

- Managed Detection and Response
- Endpoint Detection and Response
- Endpoint Detection and Response (KATA)

Puede abrir una ventana para configurar los ajustes de los componentes al hacer clic en el vínculo correspondiente.

Configurar Managed Detection and Response

En la ventana **Managed Detection and Response**, haga lo siguiente si es necesario:

- Activar o desactivar el componente Managed Detection and Response
- Importar o eliminar el archivo de configuración de MDR

El componente Managed Detection and Response proporciona una interacción con el servicio de Kaspersky Managed Detection and Response, que detecta y elimina constantemente las amenazas de seguridad dirigidas a su organización.

De forma predeterminada, Managed Detection and Response está desactivada.

Configurar Endpoint Detection and Response

En la ventana **Endpoint Detection and Response**, haga lo siguiente si es necesario:

- Active o desactive el componente Endpoint Detection and Response
- Establezca los ajustes de Aislamiento de red del dispositivo del usuario:
  - Especifique el retraso para desactivar automáticamente el Aislamiento de red.
  - Configure las exclusiones de Aislamiento de red.
- Active o desactive Prevención de ejecución.
- Seleccione la acción que se realizará al ejecutar o abrir un objeto prohibido.
- Cree una lista de reglas de Prevención de ejecución.
- Active o desactive la tecnología Sandbox en la nube.

El componente Endpoint Detection and Response combina la detección automática de amenazas con la capacidad de reaccionar a estas amenazas para contrarrestar ataques avanzados, incluidos nuevos exploits, ransomware, ataques sin archivos y métodos que utilizan herramientas legítimas del sistema.

De manera predeterminada, Endpoint Detection and Response está desactivada.

Configurar Endpoint Detection and Response (KATA)

En la ventana **Endpoint Detection and Response (KATA)**, haga lo siguiente si es necesario:

- Activar o desactivar el componente Endpoint Detection and Response (KATA)
- Configurar los ajustes de la conexión del servidor:
  - Especifique el tiempo de espera de respuesta del servidor KATA.
  - Añada un certificado TLS para configurar una conexión de confianza.
  - Elija si Kaspersky Endpoint Security utilizará la verificación bidireccional para conectarse a un servidor KATA.
  - Cargue un contenedor de cifrado protegido por contraseña para permitir la verificación bidireccional.
- Añada un servidor KATA.
- Elija si Kaspersky Endpoint Security utilizará TTL para los paquetes enviados a un servidor KATA.
- Configure los ajustes para enviar datos a servidores KATA.
- Restrinja el número de eventos transmitidos a un servidor KATA por Kaspersky Endpoint Security.

El componente Endpoint Detection and Response (KATA) facilita la interacción con la solución Kaspersky Anti Targeted Attack Platform, que detecta rápidamente amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas, ataques de día cero y otros.

De manera predeterminada, Endpoint Detection and Response (KATA) está desactivado.

Configurar los ajustes de actualización

En la sección **Actualizar**, haga lo siguiente si es necesario:

- Active/desactive las actualizaciones de los módulos de la aplicación.
- Agregue o elimine los orígenes de actualizaciones que se utilizarán para actualizar Kaspersky Endpoint Security.

Configurar los ajustes adicionales

En la sección **Configuración adicional**, haga lo siguiente si es necesario:

- Configure los ajustes de protección para el sistema operativo en el equipo cliente.

- Seleccione los tipos de objetos que se detectarán.
- Active o desactive el inicio de las tareas programadas cuando el equipo funcione con batería.
- Configure los ajustes para la generación y el almacenamiento de informes.
- Configure los ajustes de almacenamiento de objetos en el Depósito de copias de seguridad.
- Configure los ajustes de Kaspersky Endpoint Security para la interacción con el usuario del equipo cliente.
- Configuración de la conexión a un servidor proxy.
- Active o desactive el análisis del tráfico HTTPS entrante y saliente.
- Seleccione el almacenamiento de certificados para comprobar el tráfico HTTPS cifrado en el navegador Mozilla Firefox.
- Configure los puertos supervisados.
- Edite las listas de archivos, carpetas y aplicaciones de confianza que Kaspersky Endpoint Security no supervisará.

Crear tareas

En esta sección se describe cómo usar Kaspersky Security Center Web Console y Cloud Console para crear y configurar tareas que Kaspersky Endpoint Security realiza en un equipo cliente o en un grupo de equipos administrados a través de Kaspersky Security Center.

Una tarea es un conjunto de acciones configurables que Kaspersky Endpoint Security realiza en un equipo cliente.

En Kaspersky Security Center Web Console y Cloud Console, puede crear las siguientes tareas:

- Análisis
- Actualización
- Deshacer
- Agregar clave

Crear una tarea

1. En la sección **Dispositivos** a la izquierda, seleccione la sección **Tareas**.
2. Haga clic en **Agregar**.
   Se iniciará el Asistente para agregar tareas.
3. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Mac 12.2**.
4. En la lista desplegable **Tipo de tarea**, seleccione la tarea que quiera crear.
5. De ser necesario, edite el nombre de la tarea en el campo **Nombre de la tarea**.
6. Seleccionar a qué dispositivos se asignará la tarea.
7. Configure los ajustes para el tipo de tarea seleccionado.
8. Para completar el Asistente para agregar tarea, haga clic en **Finalizar**.

Nota: Si selecciona la casilla de verificación **Abrir los detalles de la tarea cuando se complete la creación** en la ventana **Finalizar la creación de tareas**, puede proceder a modificar los ajustes predeterminados de la tarea. Si no selecciona esta casilla de verificación, la tarea se crea con los ajustes predeterminados. Puede modificar los ajustes predeterminados de la tarea más tarde, en cualquier momento.

Puede llevar a cabo las siguientes acciones en las tareas:

- Iniciar y detener tareas.
- Configurar los ajustes de las tareas.
- Llevar el seguimiento del progreso de una tarea.
- Copiar y mover tareas de un grupo a otro.

- Eliminar tareas.

Para obtener información detallada sobre las tareas de Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center.

Para obtener información detallada sobre las tareas de Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Configurar los ajustes de la tarea de análisis

En la pestaña **Ajustes de la aplicación**, puede configurar los ajustes de la tarea de **Análisis** para Kaspersky Endpoint Security en equipos remotos.

Abra la configuración de la tarea de análisis

1. Vaya a **Dispositivos** > **Tareas**.
2. Haga doble clic en una tarea con el tipo de tarea de **Análisis**.
3. Haga clic en la pestaña **Ajustes de la aplicación**.

Puede hacer lo siguiente si es necesario:

- Defina una cobertura del análisis.
- Especifique las acciones que Kaspersky Endpoint Security debe ejecutar al detectar un objeto infectado.
- Seleccione qué tipos de archivos analizará Kaspersky Endpoint Security cuando ejecute la tarea de análisis.
- Configure los ajustes del rendimiento del análisis.
- Seleccione qué archivos compuestos analizará Kaspersky Endpoint Security.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Configurar los ajustes de la tarea Agregar clave

En la pestaña **Configuración de la aplicación**, puede configurar la tarea **Añadir clave** de Kaspersky Endpoint Security en equipos remotos.

Abra la configuración de la tarea Agregar clave

1. Vaya a **Dispositivos** > **Tareas**.
2. Haga doble clic en una tarea con el tipo de tarea **Añadir clave**.
3. Haga clic en la pestaña **Ajustes de la aplicación**.

Puede hacer lo siguiente si es necesario:

- Haga que la clave de licencia actual sea una clave de reserva.
- Seleccione otra clave para activar Kaspersky Endpoint Security en el equipo de un usuario.
- Agregue una nueva clave de licencia al repositorio de Kaspersky Security Center.

Configurar la tarea de actualización

En la pestaña **Ajustes de la aplicación**, puede configurar la tarea **Actualizar** de Kaspersky Endpoint Security en equipos remotos.

Abra la configuración de la tarea de actualización

1. Vaya a **Dispositivos** > **Tareas**.
2. Haga doble clic en una tarea con el tipo de tarea de **Actualizar**.

3. Haga clic en la pestaña **Ajustes de la aplicación**.

Los servidores de actualización específicos de Kaspersky son el origen principal de las actualizaciones de Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede usar los puertos de distribución, las carpetas locales u otros servidores web como un *origen de actualizaciones*.

Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console, la lista de orígenes de actualizaciones incluye los servidores de actualización de Kaspersky y los servidores de Kaspersky Security Center de forma predeterminada. Kaspersky Endpoint Security descarga primero las actualizaciones de los servidores de Kaspersky Security Center y luego de los servidores de actualización de Kaspersky.

Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la lista de orígenes de actualizaciones incluye los servidores de actualización de Kaspersky y los puntos de distribución de forma predeterminada. Kaspersky Endpoint Security descarga primero las actualizaciones de los puntos de distribución y luego de los servidores de actualización de Kaspersky. Para obtener información detallada sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

Puede hacer lo siguiente si es necesario:

- Active o desactive las actualizaciones de los módulos de la aplicación.
- Agregue o elimine los orígenes de actualizaciones que se utilizarán para actualizar Kaspersky Endpoint Security.

Obtener una clave de recuperación para una unidad cifrada

Si un usuario de un equipo cliente se olvida o pierde sus credenciales y no puede acceder a una unidad cifrada, puede obtener una clave de recuperación.

Obtener una clave de recuperación

1. Haga clic en el nombre de la cuenta de administrador en la esquina inferior izquierda de la ventana de Kaspersky Security Center Web Console o Cloud Console.
2. Seleccione **Opciones de interfaz**.
3. En el cuadro de diálogo que se abre, active el conmutador **Mostrar la protección y el cifrado de datos** para permitir la administración del cifrado de datos y haga clic en **Guardar**.
4. Vaya a **Operaciones** > **Protección y cifrado de datos** > **Unidades cifradas.**

   Se abre la lista de dispositivos cifrados.
5. Seleccione la casilla de verificación situada junto al dispositivo con la unidad cifrada.
6. Haga clic en **Conceder acceso al dispositivo en modo sin conexión**.
7. En el cuadro de diálogo **Conceder acceso al dispositivo en modo sin conexión**, seleccione el complemento web de Kaspersky Endpoint Security y haga clic en **Aceptar**.
8. Haga clic en **Obtener clave de recuperación**.

   Aparecerá una clave de recuperación en la ventana del cuadro de diálogo actual.
9. Guarde la clave de recuperación de cualquier manera conveniente.

Puede usar esta clave de recuperación en un equipo cliente para acceder a la unidad cifrada.

La ventana Tipo de instalación

Expandir todo | Contraer todo

En la sección **Paquetes para instalar**, puede seleccionar los componentes de aplicación que se instalarán en un equipo cliente.

Análisis

Esta casilla de verificación agrega el componente Análisis al paquete de instalación de Kaspersky Endpoint Security.

La casilla de verificación está seleccionada de forma predeterminada y no se puede desactivar.

Protección frente a amenazas en archivos

Esta casilla de verificación activa o desactiva la adición del componente Protección frente a amenazas en archivos al paquete de instalación de Kaspersky Endpoint Security.

Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en archivos se incluirá en el paquete de instalación de Kaspersky Endpoint Security.

Si no se selecciona esta casilla de verificación, el componente Protección frente a amenazas en archivos no se incluirá en el paquete de instalación de Kaspersky Endpoint Security.

Esta casilla de verificación está seleccionada de forma predeterminada.

Protección frente a amenazas web

Esta casilla de verificación activa o desactiva la adición del componente Protección frente a amenazas web al paquete de instalación de Kaspersky Endpoint Security.

Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas web se incluirá en el paquete de instalación de Kaspersky Endpoint Security.

Si no se selecciona esta casilla de verificación, el componente Protección frente a amenazas web no se incluirá en el paquete de instalación de Kaspersky Endpoint Security.

Esta casilla de verificación está seleccionada de forma predeterminada.

Protección frente a amenazas en la red

Esta casilla de verificación activa o desactiva la adición del componente Protección frente a amenazas en la red al paquete de instalación de Kaspersky Endpoint Security.

Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en la red se incluirá en el paquete de instalación de Kaspersky Endpoint Security.

Si no se selecciona esta casilla de verificación, el componente Protección frente a amenazas en la red no se incluirá en el paquete de instalación de Kaspersky Endpoint Security.

Esta casilla de verificación está seleccionada de forma predeterminada.

Conector de Agente de red

Esta casilla de verificación agrega el componente Conector de Agente de red al paquete de instalación de Kaspersky Endpoint Security.

La casilla de verificación está seleccionada de forma predeterminada y no se puede desactivar.

La ventana “Información de la licencia”

Expandir todo | Contraer todo

En la ventana **Información de la licencia**, puede ver información sobre una licencia, que incluye la fecha de vencimiento, la cantidad de equipos en los que puede usar Kaspersky Endpoint Security con esta licencia y el tipo de licencia.

Añadir como clave de reserva

Esta casilla de verificación activa o desactiva la adición de un archivo de claves o un código de activación específico como una clave de reserva.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security agregará el archivo de claves o el código de activación especificado como una clave de reserva.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security agregará el archivo de claves o el código de activación especificado como una clave activa.

Esta casilla de verificación no está seleccionada de forma predeterminada.

La ventana “Análisis”

Expandir todo | Contraer todo

Cobertura del análisis

Al hacer clic en este vínculo, se abrirá una ventana donde puede crear la cobertura del análisis.

En la sección **Si se detecta un objeto malicioso**, puede seleccionar la acción que desea que Kaspersky Endpoint Security realice al detectar un objeto infectado.

Pedir al usuario que tome medidas al terminar el análisis

Kaspersky Endpoint Security no procesa objetos hasta que finaliza el análisis. En ese momento, Kaspersky Endpoint Security muestra una notificación con información acerca de cada objeto infectado y solicita al usuario que seleccione qué acción se debe llevar a cabo. Las opciones disponibles dependen del tipo de objeto.

Esta opción está seleccionada de forma predeterminada.

Pedir al usuario que tome medidas de inmediato

Kaspersky Endpoint Security muestra una notificación con información sobre cada objeto infectado que la aplicación detecte y solicitará al usuario que seleccione la acción que se debe realizar a continuación. Las opciones disponibles dependen del tipo de objeto.

No preguntar al usuario

Kaspersky Endpoint Security registra información sobre los objetos detectados en el informe sin procesarlos.

Desinfectar automáticamente

Esta casilla de verificación activa o desactiva la desinfección de los objetos infectados que Kaspersky Endpoint Security detecte sin solicitar confirmación al usuario.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security desinfectará los objetos infectados automáticamente.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los objetos infectados.

Esta casilla de verificación está disponible si se selecciona la opción **No preguntar al usuario**.

Esta casilla de verificación está seleccionada de forma predeterminada.

Desinfectar; eliminar si la desinfección falla

Esta casilla de verificación activa o desactiva la eliminación de archivos infectados o posiblemente infectados tras un intento fallido de desinfección.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security eliminará de forma automática los objetos infectados que no se han podido desinfectar.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security no elimina los objetos infectados que no se han podido desinfectar.

Esta casilla de verificación se muestra si se ha elegido la opción **No preguntar al usuario** y se ha seleccionado la casilla de verificación **Desinfectar automáticamente**.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Tipos de archivos**, puede seleccionar el formato de los archivos que debe analizar Kaspersky Endpoint Security.

Analizar todos los archivos

Kaspersky Endpoint Security analiza todos los objetos del sistema de archivos que se ejecutan, abren o guardan.

Analizar aplicaciones y documentos (por contenido)

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados según el formato del archivo.

Kaspersky define la lista de formatos de archivo, que se incluye en las bases de datos de Kaspersky Endpoint Security.

Analizar aplicaciones y documentos (por extensión)

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados según la extensión del archivo.

Kaspersky define la lista de extensiones de archivo, que forma parte de las bases de datos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security siempre analiza los archivos sin extensiones.

En la sección **Optimización**, puede configurar el rendimiento del análisis.

Analizar solo archivos nuevos y modificados

Esta casilla de verificación activa o desactiva solo el análisis de aquellos archivos que Kaspersky Endpoint Security reconozca como nuevos o modificados desde el último análisis.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará solo los archivos que reconozca como nuevos o modificados desde el último análisis.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará todos los archivos.

Omitir el análisis del volumen de sistema de solo lectura

Esta casilla de verificación activa o desactiva el análisis del volumen del sistema de solo lectura por parte de Kaspersky Endpoint Security.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security omite el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el volumen del sistema de solo lectura.

Esta casilla de verificación está seleccionada de forma predeterminada.

Omitir si el archivo supera los <valor> MB

Esta casilla de verificación activa o desactiva la exclusión del análisis de los archivos superiores al tamaño especificado.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security omitirá los archivos con un tamaño superior al especificado.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará los archivos independientemente de su tamaño.

Esta casilla de verificación no está seleccionada de forma predeterminada.

De forma predeterminada, el tamaño está definido en 100 MB.

Omitir si el análisis dura más de <valor> segundos

Esta casilla de verificación activa o desactiva el límite de la duración de los análisis de archivos. Kaspersky Endpoint Security omite un archivo si el análisis del este supera el límite de tiempo especificado.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security omitirá un archivo si el análisis de este supera el límite de tiempo especificado.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará los archivos independientemente del tiempo que lleve su análisis.

El valor predeterminado es de 30 segundos.

En la sección **Archivos compuestos**, puede seleccionar los tipos de archivos compuestos que Kaspersky Endpoint Security analiza.

Analizar archivos

Esta casilla de verificación activa o desactiva el análisis de archivos.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará los archivos.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los archivos durante el análisis.

Todos

Kaspersky Endpoint Security analiza todos los archivos.

Esta opción está disponible si se selecciona la casilla de verificación **Analizar archivos**.

Solo nuevos

Kaspersky Endpoint Security analiza solo los archivos nuevos.

Esta opción está disponible si se selecciona la casilla de verificación **Analizar archivos**.

Analizar archivos protegidos por contraseña

Esta casilla de verificación activa o desactiva el análisis de archivos protegidos por contraseña.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará los archivos protegidos por contraseña.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los archivos protegidos por contraseña durante el análisis.

Analizar los objetos OLE incrustados

Esta casilla activa o desactiva el análisis de los objetos incrustados en un archivo, como hojas de cálculo Excel, macros y archivos adjuntos a un correo electrónico.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará objetos OLE incrustados.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los objetos OLE incrustados durante el análisis.

Todos

Kaspersky Endpoint Security analiza todos los objetos OLE.

Esta opción está disponible si se selecciona la casilla de verificación **Analizar los objetos OLE incrustados**.

Solo nuevos

Kaspersky Endpoint Security analiza solo los objetos OLE incrustados nuevos.

Esta opción está disponible si se selecciona la casilla de verificación **Analizar los objetos OLE incrustados**.

Analizar archivos en formato de correo electrónico

Esta casilla de verificación activa o desactiva el análisis de archivos en formato de correo electrónico y bases de datos de correo electrónico.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará los archivos en formato de correo electrónico y las bases de datos de correo electrónico.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los archivos en formato de correo electrónico y las bases de datos de correo electrónico durante el análisis.

La ventana "Cobertura del análisis"

Expandir todo | Contraer todo

Agregar

Al hacer clic en este botón, se abrirá un cuadro de diálogo en el que puede especificar un archivo, carpeta o máscara de archivos o carpetas para agregarlos a la cobertura del análisis.

Eliminar

Al hacer clic en este botón, se elimina un objeto de la cobertura del análisis.

Este botón está disponible si se selecciona la casilla de verificación situada junto al objeto.

No puede eliminar los objetos predeterminados incluidos en la cobertura del análisis.

Cobertura del análisis

Esta columna contiene los objetos analizados durante un análisis de software malicioso.

Estado

El conmutador de esta columna activa o desactiva el análisis de los objetos agregados a la cobertura del análisis.

Si el conmutador está activado, Kaspersky Endpoint Security analiza el objeto correspondiente.

Si el conmutador está desactivado, Kaspersky Endpoint Security no analiza el objeto correspondiente.

Adicional

Esta columna indica si Kaspersky Endpoint Security analiza las subcarpetas del objeto correspondiente.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

El cuadro de diálogo "Agregar cobertura del análisis"

Expandir todo | Contraer todo

Escriba el nombre del archivo, carpeta o máscara

Ruta a un archivo, a una carpeta o a una máscara de archivos o carpetas.

El objeto es una carpeta

Esta casilla de verificación activa o desactiva el análisis de un objeto como carpeta.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el objeto que haya especificado en el campo **Escriba el nombre del archivo, carpeta o máscara** como una carpeta.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el objeto que haya especificado en el campo **Escriba el nombre del archivo, carpeta o máscara** como un archivo.

Esta casilla de verificación está seleccionada de forma predeterminada.

Incluir subcarpetas

Esta casilla de verificación activa o desactiva el análisis de las subcarpetas en la carpeta especificada en el campo **Escriba el nombre del archivo, carpeta o máscara**.

Si se selecciona la casilla, Kaspersky Endpoint Security analizará las subcarpetas durante los análisis de software malicioso.

Si no se selecciona esta casilla, Kaspersky Endpoint Security solo analizará los archivos contenidos directamente en la carpeta especificada en el campo **Escriba el nombre del archivo, carpeta o máscara** durante los análisis de software malicioso.

Esta casilla de verificación está seleccionada de forma predeterminada.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

La ventana Parámetros del archivo

Se admiten los siguientes tipos de hash de archivos:

- **MD5**
  Un hash de este tipo debe tener 32 caracteres y contener 0-9, a-f, A-F.
- **SHA256**
  Un hash de este tipo debe tener 64 caracteres y contener 0-9, a-f, A-F.

La ventana "Red"

Expandir todo | Contraer todo

En la sección **Configuración de servidor proxy**, puede definir el uso de un servidor proxy y la configuración que se utilizará para conectarse a un servidor proxy.

No usar un servidor proxy

Si se selecciona esta opción, Kaspersky Endpoint Security no utilizará un servidor proxy para conectarse a orígenes de actualizaciones de módulos y bases de datos de la aplicación.

Usar configuración de servidor proxy del sistema

Si se selecciona esta opción, Kaspersky Endpoint Security se conectará a orígenes de actualizaciones de módulos y bases de datos de la aplicación mediante la configuración de servidor proxy definida en su sistema operativo.

Esta opción está seleccionada de forma predeterminada.

Usar la siguiente configuración de servidor proxy

Si se selecciona esta opción, Kaspersky Endpoint Security se conectará a orígenes de actualizaciones de módulos y bases de datos de la aplicación mediante la configuración de servidor proxy que ha especificado.

Dirección

Dirección IP o nombre simbólico de un servidor proxy.

Este campo está disponible si se selecciona la opción **Usar la siguiente configuración de servidor proxy**.

Puerto

Número de puerto del servidor proxy.

El número de puerto predeterminado es 8080.

Este campo está disponible si se selecciona la opción **Usar la siguiente configuración de servidor proxy**.

Usar autenticación

Esta casilla de verificación activa o desactiva el uso de autenticación para conectarse a un servidor proxy.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security solicitará las credenciales del usuario para conectarse a un servidor proxy.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security no solicitará las credenciales del usuario para conectarse a un servidor proxy.

Esta casilla de verificación está seleccionada de forma predeterminada.

Esta casilla de verificación está disponible si se selecciona la opción **Usar la siguiente configuración de servidor proxy**.

Nombre de usuario

Nombre de usuario de conexión al servidor proxy.

Este campo está disponible si se seleccionan las casillas de verificación **Usar la siguiente configuración de servidor proxy** y **Usar autenticación**.

Contraseña

Contraseña para el nombre de usuario especificado.

Este campo está disponible si se seleccionan las casillas de verificación **Usar la siguiente configuración de servidor proxy** y **Usar autenticación**.

Mostrar

Al hacer clic en este botón, se muestran los caracteres de la contraseña que introdujo en el campo **Contraseña**.

No usar servidor proxy para direcciones locales

Esta casilla de verificación activa o desactiva el uso de un servidor proxy al actualizar los módulos y las bases de datos de la aplicación desde una carpeta de red o local.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security no utilizará un servidor proxy al actualizar los módulos y las bases de datos de la aplicación desde una carpeta de red o local.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security utilizará un servidor proxy al actualizar los módulos y las bases de datos de la aplicación en una carpeta de red o local.

Esta casilla de verificación está seleccionada de forma predeterminada.

Esta casilla de verificación está disponible si se selecciona la opción **Usar la siguiente configuración de servidor proxy**.

En la sección **Comprobar conexiones seguras**, puede definir si Kaspersky Endpoint Security analiza las conexiones seguras (HTTPS).

Comprobación de conexiones seguras (HTTPS)

El conmutador **Comprobación de conexiones seguras (HTTPS)** activa o desactiva el análisis de conexiones seguras mediante el protocolo HTTPS y muestra notificaciones cuando el Control Web bloquea el acceso del usuario a recursos web peligrosos.

Si el conmutador **Comprobación de conexiones seguras (HTTPS)** está activado, Kaspersky Endpoint Security hace lo siguiente:

- El componente Protección frente a amenazas web analizará los datos entrantes y salientes de su equipo a través del protocolo HTTPS en Safari, Google Chrome o Firefox.

- La aplicación muestra notificaciones cuando el usuario accede a recursos web bloqueados mediante el Control web en el equipo remoto.

Si el conmutador **Comprobación de conexiones seguras (HTTPS)** está desactivado, Kaspersky Endpoint Security hace lo siguiente:

- El componente Protección frente a amenazas web no analizará los datos entrantes y salientes de su equipo a través del protocolo HTTPS.
- La aplicación no muestra notificaciones cuando el usuario accede a recursos web bloqueados mediante el Control Web en el equipo remoto.

Este conmutador está activado de forma predeterminada.

En la sección **Elija la tienda de certificados que Firefox utilizará**, puede seleccionar el almacén de certificados para comprobar el tráfico HTTPS cifrado en el navegador Mozilla Firefox.

Llavero Raíz del sistema (recomendado)

Si se selecciona esta opción, Kaspersky Endpoint Security usa un certificado raíz del llavero Raíz del sistema para analizar el tráfico HTTPS cifrado en el navegador Mozilla Firefox.

Esta opción está seleccionada de forma predeterminada.

Ajustes de la tienda de certificados del navegador Mozilla Firefox

Si se selecciona esta opción, Kaspersky Endpoint Security utiliza el certificado del almacén de certificados del navegador.

En este caso, debe añadir manualmente el certificado de Kaspersky Endpoint Security al almacén de certificados del navegador Mozilla Firefox. Para obtener más información, consulte Cómo añadir el certificado de Kaspersky Endpoint Security al almacenamiento de certificados de Mozilla Firefox.

En la sección **Certificados raíz de confianza**, puede administrar la lista de certificados raíz de confianza.

Administrar certificados raíz de confianza

Al hacer clic en este vínculo, se abre una ventana en la que puede crear una lista de certificados raíz de confianza para que se conecten a los servidores correspondientes sin notificaciones.

En la sección **Puertos supervisados**, puede configurar qué puertos supervisa Kaspersky Endpoint Security.

Puertos seleccionados

Al hacer clic en este vínculo, se abrirá una ventana donde puede configurar la lista de puertos que supervisará Kaspersky Endpoint Security.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Administrar certificados raíz de confianza”

Expandir todo | Contraer todo

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede añadir los certificados que se considerarán de confianza.

Eliminar

Al hacer clic en este botón, elimina el certificado seleccionado en la lista de equipos de confianza.

Lista de certificados de confianza

Una lista que muestra los nombres de los certificados raíz de confianza.

La lista está vacía de manera predeterminada.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana "Puertos supervisados"

Expandir todo | Contraer todo

Lista de puertos supervisados

Una lista de puertos para los que puede configurar la supervisión de los datos transmitidos.

En forma predeterminada, la lista de puertos contiene los puertos más usados por los servicios más comunes.

Agregar

Al hacer clic en este botón, se abrirá un cuadro de diálogo donde puede agregar un puerto que desee que Kaspersky Endpoint Security supervise.

Eliminar

Al hacer clic en este botón, se elimina de la lista el puerto seleccionado.

Este botón está disponible si se selecciona la casilla de verificación situada junto al puerto.

Puerto

Esta columna contiene los números de puerto.

Estado

Esta columna contiene un conmutador que indica el estado de supervisión de los datos transmitidos a través del puerto.

Si el estado es **Supervisado**, Kaspersky Endpoint Security analizará el tráfico transmitido a través del puerto correspondiente.

Si el estado es **No supervisado**, Kaspersky Endpoint Security no analizará el tráfico transmitido a través del puerto correspondiente.

Descripción

Esta columna contiene una descripción del puerto.

El cuadro de diálogo "Agregar puerto"

Expandir todo | Contraer todo

Campo de entrada Puerto

El número de un puerto cuyos datos transmitidos desea que Kaspersky Endpoint Security analice.

Campo de entrada Descripción

Información adicional sobre el puerto, como por ejemplo, el tipo de puerto.

La ventana "Zona de confianza": la sección "Archivos y carpetas"

Expandir todo | Contraer todo

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede agregar un archivo o carpeta a la Zona de confianza.

Eliminar

Al hacer clic en este botón, se eliminará el archivo o la carpeta seleccionados de la lista de exclusiones.

Este botón está disponible si se selecciona la casilla de verificación situada junto al archivo o carpeta.

Archivo o carpeta

Esta columna contiene los archivos o carpetas agregados a la Zona de confianza.

Estado

El conmutador de esta columna activa o desactiva el análisis del archivo o carpeta agregado a la Zona de confianza.

Si el conmutador está activado, Kaspersky Endpoint Security no analiza el archivo o carpeta correspondiente.

Si el conmutador está desactivado, Kaspersky Endpoint Security analiza el archivo o carpeta correspondiente.

Comentario

Información sobre el archivo o carpeta agregado a la Zona de confianza.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo "Agregar exclusión"

Expandir todo | Contraer todo

Campo de entrada Escriba el nombre del archivo, carpeta o máscara

La ruta a un archivo o carpeta, o una máscara de archivo o carpeta que se excluirá de la cobertura de protección.

Incluir subcarpetas

Esta casilla de verificación activa o desactiva el análisis de las subcarpetas de la carpeta especificada en el campo **Escriba el nombre del archivo, carpeta o máscara**.

Si se selecciona esta casilla, Kaspersky Endpoint Security no analizará las subcarpetas de la carpeta especificada durante los análisis de software malicioso.

Si la casilla no está seleccionada, Kaspersky Endpoint Security solo excluye los archivos que se encuentran directamente en la carpeta especificada en **Escriba el nombre del archivo, carpeta o máscara** durante los análisis de software malicioso. Las subcarpetas de la carpeta especificada sí se analizarán.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Componentes**, puede seleccionar componentes que no analizarán el archivo o carpeta especificado.

Cualquiera

Ni el Análisis ni el componente Protección frente a amenazas en archivos analizarán el archivo o carpeta especificado.

De la lista

Esta opción le permite seleccionar los componentes.

Protección frente a amenazas en archivos

Si se selecciona esta casilla de verificación, el componente Protección frente a amenazas en archivos no analizará el archivo o carpeta especificado.

Esta casilla de verificación está disponible si se selecciona la opción **De la lista**.

Análisis

Si se selecciona esta casilla de verificación, el componente Análisis no analizará el archivo o carpeta especificado.

Esta casilla de verificación está disponible si se selecciona la opción **De la lista**.

Campo de entrada Comentario

Información sobre el archivo o carpeta agregado a la Zona de confianza.

En la sección **Estado**, puede seleccionar si la exclusión está activa o no.

Desactivado

Kaspersky Endpoint Security analiza el archivo o carpeta correspondiente.

Activada

Kaspersky Endpoint Security no analiza el archivo o carpeta correspondiente.

La ventana “Zona de confianza”: la sección “Aplicaciones de confianza”

Expandir todo | Contraer todo

Lista de aplicaciones de confianza

Una lista de aplicaciones de confianza cuya actividad de red Kaspersky Endpoint Security no supervisará.

Agregar

Al hacer clic en este botón, se abrirá un cuadro de diálogo en el que puede introducir una ruta a una aplicación cuya actividad de red Kaspersky Endpoint Security no supervisará.

Eliminar

Al hacer clic en este botón, se elimina de la lista la aplicación de confianza seleccionada.

Este botón está disponible si se selecciona la casilla de verificación situada junto a la aplicación de confianza.

Aplicación

Esta columna contiene el nombre de la aplicación o el último segmento de la ruta a una aplicación.

Estado

Esta columna contiene un conmutador que indica el estado de supervisión de la actividad de red de la aplicación.

Si el estado es **Activado**, Kaspersky Endpoint Security no supervisa la actividad de red de la aplicación correspondiente.

Si el estado es **Desactivado**, Kaspersky Endpoint Security supervisa la actividad de red de la aplicación correspondiente.

Ruta

Esta columna contiene la ruta de la aplicación en el equipo cliente, que debe agregar de forma manual.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo "Agregar aplicación"

Expandir todo | Contraer todo

Campo de entrada Ruta

La ruta a una aplicación cuya actividad de red o archivo no será supervisada por la aplicación Kaspersky Endpoint Security.

Requisito de firma de código

Requisitos para la firma del código de la aplicación cuya actividad Kaspersky Endpoint Security no supervisará.

Este es un parámetro opcional.

Opciones

En esta sección, puede seleccionar los tipos de actividad que no desea que la aplicación Kaspersky Endpoint Security supervise.

No supervisar la actividad de archivos

Esta casilla de verificación activa o desactiva la supervisión de las operaciones con archivos de una aplicación en un equipo cliente.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security no supervisa la actividad de archivos de la aplicación.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security supervisa la actividad de archivos de la aplicación.

Esta casilla de verificación está seleccionada de forma predeterminada.

No supervisar la actividad de red

Esta casilla activa o desactiva la supervisión del tráfico de Internet entrante y saliente en un equipo cliente.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security no supervisa la actividad de red de la aplicación.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security supervisa la actividad de red de la aplicación.

Esta casilla de verificación está seleccionada de forma predeterminada.

La sección Configuración adicional

Expandir todo | Contraer todo

Protección

Al hacer clic en este vínculo, se abrirá la ventana **Protección** en la que puede administrar los ajustes generales de Kaspersky Endpoint Security instalada en los equipos de los usuarios y seleccionar los tipos de archivos que Kaspersky Endpoint Security detectará.

Informes y copias de seguridad

Al hacer clic en este vínculo, se abrirá la ventana **Informes y copias de seguridad** en la que puede administrar los ajustes de los informes y el depósito de copias de seguridad.

Interacción con el usuario

Al hacer clic en este vínculo, se abrirá la ventana **Interacción con el usuario** en la que puede configurar las notificaciones que mostrará Kaspersky Endpoint Security, el idioma de visualización de los eventos que mostrará Kaspersky Security Center y los ajustes adicionales de Kaspersky Endpoint Security.

Red

Al hacer clic en este enlace, se abre la ventana **Red**, donde puede administrar la configuración del servidor proxy, activar o desactivar el análisis de conexiones cifradas (HTTPS), seleccionar el almacenamiento del certificado para comprobar el tráfico HTTPS cifrado en el navegador Mozilla Firefox y configurar los puertos supervisados.

Zona de confianza

Al hacer clic en este enlace, se abrirá la ventana **Zona de confianza** en la que puede añadir exclusiones para el componente Protección frente a amenazas en archivos o tareas de análisis y configurar las aplicaciones de confianza.

La ventana "Protección"

Expandir todo | Contraer todo

En la sección **General**, puede activar o desactivar la protección de los archivos en un equipo remoto y configurar el inicio automático de la aplicación cuando se encienda el equipo o se reinicie el sistema operativo.

Iniciar aplicación cuando se encienda el equipo

Esta casilla de verificación activa o desactiva el inicio automático de Kaspersky Endpoint Security cuando se enciende un equipo remoto o después de que se reinicie su sistema operativo.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security se iniciará de forma automática cuando se encienda el equipo remoto o se reinicie su sistema operativo.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security no se iniciará de forma automática cuando se encienda el equipo remoto o se reinicie su sistema operativo.

Esta casilla de verificación está seleccionada de forma predeterminada.

Importante: Si selecciona esta casilla mientras Kaspersky Endpoint Security no está en ejecución, se aplicarán los cambios cuando inicie la aplicación o use Kaspersky Security Center.

Activar protección

Esta casilla de verificación activa o desactiva la protección de un equipo remoto en el que esté instalado Kaspersky Endpoint Security.

Si se selecciona la casilla de verificación, se activará la protección del equipo remoto.

Si no se selecciona la casilla de verificación, esta se desactivará.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Tipos de objetos que deben detectarse**, puede seleccionar los tipos de archivos que Kaspersky Endpoint Security detectará.

Virus, gusanos, programas troyanos, herramientas maliciosas, software publicitario y automarcadores

Esta casilla de verificación activa o desactiva la detección de los siguientes tipos de programas:

- Todos los tipos de software malicioso.
- Aplicaciones que muestran anuncios (como banners) en su equipo o sustituyen los resultados de búsqueda de su navegador por sitios web de publicidad.
- Aplicaciones que establecen conexiones telefónicas mediante un módem del equipo en modo oculto.

La casilla de verificación está seleccionada de forma predeterminada y no se puede desactivar.

Software legítimo que puede ser utilizado por intrusos con el fin de dañar el equipo o los datos personales del usuario

Esta casilla de verificación activa o desactiva la detección de aplicaciones que no son maliciosas o peligrosas, pero que pueden usarse para dañar el equipo de un usuario en determinadas circunstancias.

Si la casilla está selecciona, Kaspersky Endpoint Security detecta el software legítimo que pueden utilizar los intrusos para dañar el equipo o los datos personales de un usuario.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no detecta el software legítimo que pueden utilizar los intrusos para dañar el equipo o los datos personales de un usuario.

Esta casilla de verificación no está seleccionada de forma predeterminada.

La sección **Avanzado** le permite activar el modo ahorro de energía.

Omitir las tareas programadas cuando se utilice la alimentación de la batería

Esta casilla de verificación activa o desactiva el inicio de las tareas de análisis programadas en equipos que funcionen con batería.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security no iniciará tareas de análisis programadas en equipos que funcionen con batería.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security sí las iniciará en estos equipos.

Esta casilla de verificación está seleccionada de forma predeterminada.

Limitar el uso de las tareas de análisis de la CPU

Kaspersky Endpoint Security limita el uso de la CPU del dispositivo protegido durante las tareas de análisis bajo demanda al valor especificado en el campo de entrada correspondiente.

Activar esta opción puede afectar negativamente al rendimiento de Kaspersky Endpoint Security.

De manera predeterminada, esta opción está desactivada.

Límite máximo (en porcentajes)

Valor máximo permitido de uso de CPU para las tareas de análisis de Kaspersky Endpoint Security.

El campo de entrada estará disponible si se seleccionó la opción **Limitar el uso de las tareas de análisis de la CPU**.

Nota: Este es un límite acumulativo entre todos los núcleos de la CPU. El uso de la CPU que se muestra en Supervisión de actividad es el total del uso de cada núcleo de la CPU y, por lo tanto, puede superar el cien por ciento.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana "Informes y copias de seguridad"

Expandir todo | Contraer todo

En la sección **Informes**, puede definir la configuración de generación y almacenamiento de los informes sobre eventos que ocurren mientras se está ejecutando Kaspersky Endpoint Security.

Eliminar informes después de <valor> días

Esta casilla de verificación activa o desactiva la eliminación de los informes después del período especificado.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security eliminará los informes después del período especificado. De forma predeterminada, Kaspersky Endpoint Security almacena los informes durante 30 días.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security almacenará todos los informes de manera indefinida.

Esta casilla de verificación está seleccionada de forma predeterminada.

Registrar eventos no críticos

Esta casilla de verificación activa o desactiva el registro de eventos no críticos (por ejemplo, los eventos informativos) en el informe. Los eventos no críticos no afectan a la seguridad.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security registrará los eventos informativos en el informe.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security no los registrará en el informe.

Esta casilla de verificación no está seleccionada de forma predeterminada.

Mantener solamente los eventos recientes

Esta casilla de verificación activa o desactiva la función de almacenar únicamente la información sobre eventos importantes de la ejecución anterior de la tarea.

Si se selecciona esta casilla de verificación, cada vez que se inicie la tarea, Kaspersky Endpoint Security eliminará la información sobre eventos no críticos de la ejecución anterior de la tarea, pero guardará la información importante (por ejemplo, sobre software malicioso detectado) en el informe.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security mantendrá toda la información de la ejecución anterior de la tarea.

Esta casilla de verificación no está seleccionada de forma predeterminada.

En la sección **Copia de seguridad**, puede especificar el período durante el cual los objetos se pueden almacenar en el Depósito de copias de seguridad.

Eliminar objetos después de <valor> días

Esta casilla de verificación activa o desactiva la eliminación de los objetos del Depósito de copias de seguridad tras finalizar el período especificado.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security eliminará los objetos del Depósito de copias de seguridad tras finalizar el período especificado. El período de almacenamiento predeterminado es de 30 días.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security almacenará los objetos del Depósito de copias de seguridad de manera indefinida.

Esta casilla de verificación está seleccionada de forma predeterminada.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Interacción con el usuario”

Expandir todo | Contraer todo

En la sección **Interfaz de la aplicación**, puede configurar si el icono de la aplicación se mostrará en la barra de menús de un equipo remoto y si un usuario puede abrir la ventana principal de Kaspersky Endpoint Security y usar la interfaz de la aplicación.

Mostrar el icono de la aplicación en la barra de menús

Esta casilla de verificación activa o desactiva que se muestre el icono de la aplicación en la barra de menús de un equipo remoto.

Si se selecciona la casilla de verificación, se mostrará el icono de la aplicación en la barra de menús.

Si no se selecciona la casilla de verificación, se ocultará el icono de la aplicación en la barra de menús.

Esta casilla de verificación está seleccionada de forma predeterminada.

Permitir al usuario abrir la aplicación

Esta casilla de verificación activa o desactiva la capacidad de un usuario de abrir la ventana principal de Kaspersky Endpoint Security y usar la interfaz de la aplicación en un equipo remoto.

Si se selecciona esta casilla de verificación, un usuario puede abrir la ventana principal de Kaspersky Endpoint Security y usar la interfaz de la aplicación en un equipo remoto.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security impide que un usuario abra la ventana principal de la aplicación y oculta la interfaz de la aplicación en un equipo remoto.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Notificaciones**, puede activar notificaciones sobre eventos de Kaspersky Endpoint Security y elegir el tipo de notificación.

Notificaciones

El conmutador **Notificaciones** activa o desactiva las notificaciones sobre eventos de Kaspersky Endpoint Security.

Si el conmutador **Notificaciones** está activado, Kaspersky Endpoint Security mostrará notificaciones sobre eventos que ocurren mientras se están ejecutando los componentes de Kaspersky Endpoint Security.

Si el conmutador **Notificaciones** está desactivado, Kaspersky Endpoint Security no mostrará notificaciones sobre eventos que ocurren mientras se están ejecutando los componentes de Kaspersky Endpoint Security.

Este conmutador está activado de forma predeterminada.

Notificaciones de usuario

Al hacer clic en este vínculo, se abrirá una ventana en la que podrá seleccionar los tipos de notificación que se utilizarán para todos los tipos de eventos.

En la sección **Permitir al usuario salir de la aplicación**, puede configurar si un usuario desde un equipo remoto puede apagar Kaspersky Endpoint Security.

Mostrar la función Salir en el menú contextual del icono de la aplicación

Esta casilla de verificación activa o desactiva la disponibilidad del elemento **Salir** en el menú contextual del icono de la aplicación mostrado en la barra de menús.

Si se selecciona esta casilla de verificación, se mostrará el elemento **Salir** en el menú contextual del icono de la aplicación. El usuario de un equipo remoto puede salir de Kaspersky Endpoint Security en dicho equipo.

Si no se selecciona la casilla de verificación, el elemento **Salir** no se encuentra disponible en el menú contextual del icono de la aplicación. El usuario de un equipo remoto no puede salir de Kaspersky Endpoint Security en dicho equipo.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Eventos en Kaspersky Security Center**, puede seleccionar el idioma de visualización de los eventos de Kaspersky Endpoint Security en Kaspersky Security Center.

Idioma de visualización

En esta lista desplegable, puede seleccionar el idioma de visualización de los eventos de Kaspersky Endpoint Security en Kaspersky Security Center.

En la sección **Restricciones**, puede permitir la gestión local de las claves y actualizaciones de Kaspersky Endpoint Security en un equipo remoto.

Permitir que el usuario administre las actualizaciones de forma local

Esta casilla de verificación activa o desactiva la gestión local de las actualizaciones de Kaspersky Endpoint Security en un equipo remoto.

Si se selecciona la casilla de verificación, se activará la gestión local de las actualizaciones de Kaspersky Endpoint Security en un equipo remoto.

Si no se selecciona la casilla de verificación, las actualizaciones de Kaspersky Endpoint Security en un equipo remoto solo se podrán gestionar con el complemento de administración de Kaspersky Endpoint Security a través de Kaspersky Security Center.

Esta casilla de verificación está seleccionada de forma predeterminada.

Permitir que el usuario administre las claves de forma local

Esta casilla de verificación activa o desactiva la gestión local de las claves de Kaspersky Endpoint Security en un equipo remoto.

Si se selecciona la casilla de verificación, se activará la gestión local de las claves de Kaspersky Endpoint Security en un equipo remoto.

Si no se selecciona la casilla de verificación, las claves de Kaspersky Endpoint Security en un equipo remoto solo se podrán gestionar con el complemento de administración de Kaspersky Endpoint Security a través de Kaspersky Security Center.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Protección con contraseña**, puede establecer y configurar la contraseña para limitar las acciones no deseadas en los dispositivos de los usuarios.

Protección con contraseña

El interruptor **Protección con contraseña** activa o desactiva la protección con contraseña de acciones no deseadas en los dispositivos de los usuarios.

Si el interruptor **Protección con contraseña** está activado, puede establecer y configurar una contraseña para limitar las acciones del usuario en sus dispositivos.

Si el interruptor **Protección con contraseña** está desactivado, un usuario puede realizar una acción no deseada sin introducir una contraseña.

Este conmutador está desactivado de forma predeterminada.

Si activa este interruptor, se abre una ventana donde puede configurar la contraseña para limitar las acciones no deseadas en los dispositivos de los usuarios.

Configuración

Al hacer clic en este botón, se abre una ventana donde puede configurar la contraseña para limitar las acciones no deseadas en los dispositivos de los usuarios.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana "Notificaciones de usuario"

Expandir todo | Contraer todo

Eventos

Esta columna enumera los eventos que podrían ocurrir mientras Kaspersky Endpoint Security se está ejecutando:

- **Eventos críticos**. Eventos de crucial importancia desde el punto de vista de la seguridad.
- **Error de funcionamiento**. Eventos que hacen que falle el sistema.
- **Eventos importantes**. Eventos de los que el usuario se debería ocupar.
- **Eventos informativos**. Los eventos que son informativos.

Notificaciones

Una notificación es un mensaje emergente que informa al usuario sobre un evento.

La casilla de verificación de la columna **Notificaciones** activa o desactiva las notificaciones emergentes sobre eventos de una categoría en concreto.

Sonido

Un sonido de notificación asociado con un evento.

La casilla de verificación de la columna **Sonido** activa o desactiva las notificaciones de sonido sobre eventos de una categoría en concreto.

La sección "Actualización"

Expandir todo | Contraer todo

Actualizar módulos de aplicación

Esta casilla de verificación activa o desactiva las actualizaciones de los módulos de aplicación. Las bases de datos de la aplicación siempre están actualizadas.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security actualizará los módulos de aplicación.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security no actualizará los módulos de aplicación.

Esta casilla de verificación está seleccionada de forma predeterminada.

Orígenes de actualizaciones

Esta lista contiene las direcciones de los recursos desde los que Kaspersky Endpoint Security descarga e instala actualizaciones de los módulos y las bases de datos de la aplicación. Puede especificar una carpeta local o de red, o un servidor FTP o HTTP como un origen de actualizaciones.

De forma predeterminada, la lista de orígenes de actualizaciones contiene los servidores de actualización de Kaspersky.

Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console, la lista de orígenes de actualizaciones también incluye los servidores de Kaspersky Security Center de forma predeterminada.

Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la lista de orígenes de actualizaciones también incluye los puntos de distribución de forma predeterminada. Para obtener información detallada sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

No se puede eliminar los orígenes de actualizaciones predeterminados de la lista.

Agregar

Al hacer clic en este botón, se abrirá un diálogo en el que podrá especificar la ruta a una carpeta local o de red, o a una dirección web para agregarlas a la lista de orígenes de actualizaciones.

Eliminar

Al hacer clic en este botón, se elimina de la lista el origen de actualizaciones seleccionado.

Este botón está disponible si se selecciona la casilla de verificación situada junto al origen de actualizaciones.

Origen de actualizaciones

Esta columna contiene los orígenes de actualizaciones de Kaspersky Endpoint Security.

Estado

Si el conmutador de esta columna está activado, Kaspersky Endpoint Security usa el origen de actualizaciones correspondiente de la columna **Origen de actualizaciones** para recibir actualizaciones.

Si el conmutador de esta columna está desactivado, Kaspersky Endpoint Security no usa el origen de actualizaciones correspondiente de la columna **Origen de actualizaciones** para recibir actualizaciones.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar origen de actualizaciones”

Expandir todo | Contraer todo

Introduzca una ruta a una carpeta local o de red o a un campo de entrada de la dirección web

Dirección del recurso desde la que Kaspersky Endpoint Security copia las actualizaciones.

Puede especificar una ruta a una carpeta local o de red, o la dirección web o IP de un servidor FTP o HTTP, como la dirección del recurso.

Puede especificar la dirección web de un servidor FTP con el siguiente formato: ftp://<nombre de usuario>:<contraseña>@<host>:<puerto>.

En la sección **Estado**, puede definir si Kaspersky Endpoint Security usa la dirección web especificada como origen de actualizaciones.

Desactivado

La dirección web se agrega a la lista de orígenes de actualizaciones, pero Kaspersky Endpoint Security no usa esta dirección web como origen de actualizaciones.

Activado

La dirección web se agrega a la lista de orígenes de actualizaciones y Kaspersky Endpoint Security usa esta dirección web como origen de actualizaciones.

En la sección "Cifrado de datos"

Expandir todo | Contraer todo

Cifrado de disco de FileVault

El conmutador **Cifrado de disco de FileVault** activa o desactiva la administración de cifrado de disco de FileVault.

Si el conmutador **Cifrado de disco de FileVault** está activado, el cifrado de disco de FileVault se puede aplicar a los equipos cliente de Kaspersky Security Center.

Si el conmutador **Cifrado de disco de FileVault** está desactivado, el cifrado de disco de FileVault no se puede aplicar a los equipos cliente de Kaspersky Security Center.

Este conmutador está desactivado de forma predeterminada.

Nota: Si el conmutador **Cifrado de disco de FileVault** está desactivado, los usuarios con derechos de administrador pueden cifrar o descifrar los discos de inicio de su Mac desde Ajustes del sistema. Para obtener más información sobre FileVault, consulte la documentación de Apple.

Cifrar disco

Kaspersky Endpoint Security muestra una solicitud de credenciales de cuenta de equipo en los equipos cliente a los cuales se aplica la directiva. Cuando el usuario introduce las credenciales, Kaspersky Endpoint Security comienza a cifrar el disco de inicio del usuario.

Si el conmutador **Cifrado de disco de FileVault** está activado y la opción **Cifrar disco** está seleccionada, los usuarios con derechos de administrador no pueden descifrar el disco de inicio de sus Mac desde Ajustes del sistema.

Descifrar disco

Kaspersky Endpoint Security muestra una solicitud de credenciales de cuenta de equipo en los equipos cliente a los cuales se aplica la directiva. Cuando el usuario introduce las credenciales, Kaspersky Endpoint Security comienza a descifrar el disco de inicio del usuario.

Si el conmutador **Cifrado de disco de FileVault** está activado y la opción **Descifrar disco** está seleccionada, los usuarios con derechos de administrador no pueden cifrar el disco de inicio de sus Mac desde Ajustes del sistema.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La sección Detection and Response

Expandir todo | Contraer todo

Managed Detection and Response

Al hacer clic en este enlace, se abre una ventana en la que puede configurar los ajustes de Managed Detection and Response.

Endpoint Detection and Response

Al hacer clic en este enlace, se abre una ventana en la que puede configurar los ajustes de Endpoint Detection and Response.

Endpoint Detection and Response (KATA)

Al hacer clic en este enlace, se abre una ventana donde puede configurar los ajustes de Endpoint Detection and Response (KATA).

La ventana “Managed Detection and Response”

Expandir todo | Contraer todo

Managed Detection and Response

El interruptor de **Managed Detection and Response** activa o desactiva el componente Managed Detection and Response, que interactúa con el servicio de Kaspersky Managed Detection and Response. Este servicio detecta y elimina constantemente las amenazas de seguridad que se dirigen a su organización.

Si el interruptor de **Managed Detection and Response** está activado y el archivo de configuración MDR está importado, esto significa que el componente Managed Detection and Response está activado.

Si el interruptor de **Managed Detection and Response** está desactivado, el componente Managed Detection and Response está desactivado.

Este conmutador está desactivado de forma predeterminada.

Importar

Al hacer clic en este botón, se abre una ventana que permite importar el archivo de configuración MDR en la directiva de Kaspersky Endpoint Security.

Eliminar archivo de configuración

Haga clic en este botón para eliminar el archivo de configuración MDR de la política de Kaspersky Endpoint Security.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Endpoint Detection and Response

Expandir todo | Contraer todo

Endpoint Detection and Response

El conmutador **Endpoint Detection and Response** activa o desactiva el componente Endpoint Detection and Response, que interactúa con la solución Kaspersky Endpoint Detection and Response. Esta solución protege los equipos frente a amenazas complejas, incluidos nuevos exploits, ransomware y ataques sin archivos.

Si el interruptor de **Endpoint Detection and Response** está activado, el componente Endpoint Detection and Response está habilitado.

Si el interruptor de **Endpoint Detection and Response** está desactivado, el componente Endpoint Detection and Response está deshabilitado.

Este conmutador está desactivado de forma predeterminada.

En la sección **Aislamiento de red**, puede establecer los ajustes para aislar los equipos de la red en respuesta a la detección de un indicador de vulneración.

Configure los ajustes de desbloqueo de equipos

Al hacer clic en este enlace, se abre una ventana en la que puede especificar el retraso para desactivar automáticamente el Aislamiento de red.

Exclusiones

Al hacer clic en este enlace, se abre una ventana en la que puede especificar las conexiones de red que no se bloquean en el equipo después de que se activa automáticamente el Aislamiento de red.

En la sección **Prevención de ejecución**, puede establecer los ajustes para el funcionamiento de archivos ejecutables y scripts, y la apertura de archivos Office.

Prevención de ejecución

El conmutador **Prevención de ejecución** activa o desactiva la Prevención de ejecución.

Si el conmutador **Prevención de ejecución** está activado, puede crear y editar la lista de reglas de Prevención de ejecución y seleccionar una acción para realizar cuando se ejecutan o abren objetos prohibidos.

Si el conmutador **Prevención de ejecución** está desactivado, no puede administrar los objetos que los usuarios ejecutan o abren en sus dispositivos.

Este conmutador está desactivado de forma predeterminada.

Acción al ejecutar o abrir un objeto prohibido

Bloquear y escribirlo en el informe

Si este modo está seleccionado, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado.

Solo eventos del registro

Si este modo está seleccionado, Kaspersky Endpoint Security publica un evento sobre los intentos de iniciar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos de Kaspersky Security Center y en el sistema de registro unificado, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de manera predeterminada.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede crear una nueva regla de Prevención de ejecución.

Editar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede editar una regla de prevención existente.

Este botón está disponible si se selecciona una regla en la lista de reglas.

Eliminar

Al hacer clic en este botón, se elimina una regla de Prevención de ejecución de la lista de reglas.

Este botón está disponible si se selecciona una regla en la lista de reglas.

En la sección **Configuración de Sandbox en la nube**, puede activar o desactivar el componente Sandbox en la nube.

Sandbox en la nube

El conmutador **Sandbox en la nube** activa o desactiva la tecnología Cloud Sandbox que ayuda a detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados para analizarse a Sandbox en la nube. Sandbox en la nube ejecuta estos archivos en un entorno aislado para identificar la actividad maliciosa y decide su reputación. Luego, los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Sandbox en la nube detecta un archivo malicioso, Kaspersky Endpoint Security realizará la acción apropiada para eliminar la amenaza en todos los equipos en los que se detecte este archivo.

Si el conmutador **Sandbox en la nube** está activado, la tecnología Sandbox en la nube está activada.

Si el conmutador **Sandbox en la nube** está desactivado, la tecnología Sandbox en la nube está desactivada.

Este conmutador está desactivado de forma predeterminada.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana de ajustes de desbloqueo del equipo

Expandir todo | Contraer todo

Desbloquear automáticamente el equipo aislado en

Esta casilla activa o desactiva el apagado automático de Aislamiento de red después de un tiempo especificado.

Si esta casilla está seleccionada, puede especificar el retraso para desactivar automáticamente el Aislamiento de red de un equipo.

Si esta casilla está desactivada, Kaspersky Endpoint Security desactiva el Aislamiento de red 8 horas después de que comience el aislamiento.

Esta casilla de verificación está seleccionada de forma predeterminada.

Horas

El intervalo después del cual el Aislamiento de red se desactivará automáticamente.

Este campo solo se puede editar si la casilla **Desbloquear automáticamente el equipo aislado en** está seleccionada.

La ventana Exclusiones de aislamiento de red

Expandir todo | Contraer todo

Exclusiones de aislamiento de red

Esta lista contiene las conexiones de red que añadió como exclusiones de Aislamiento de red.

Añadir

Al hacer clic en este botón, se abre una ventana donde puede especificar manualmente los ajustes de la conexión de red que se añadirá como una exclusión.

Añadir desde el perfil

Al hacer clic en este botón, se abre una ventana donde puede seleccionar perfiles de red estándar para configurar las exclusiones.

Eliminar

Al hacer clic en este botón, se elimina una conexión de red de la lista de exclusiones de Aislamiento de red.

Este botón está disponible si se selecciona una conexión en la lista de exclusiones de Aislamiento de red.

La ventana de opciones de la regla

Expandir todo | Contraer todo

Nombre de la regla

Nombre de una regla de exclusión de Aislamiento de red.

Este es un ajuste opcional.

Dirección

Dirección del tráfico.

Protocolo

Tipo de protocolo.

Número

Número de protocolo.

El valor debe ajustarse a la lista de números de protocolo de Internet asignados de la IANA.

Este campo está disponible si se selecciona el tipo de protocolo **Personalizado**.

Puerto local o rango

Puerto local o rango del equipo para el que se configuran las exclusiones de Aislamiento de red.

Puerto o rango remoto

Puerto remoto o rango del equipo para el que se configuran las exclusiones de Aislamiento de red.

Dirección remota

Dirección de red del equipo para el que se están configurando las exclusiones de Aislamiento de red.

Aplicaciones

Esta casilla es para añadir una aplicación a la que se le permite iniciar una conexión de red añadida a las exclusiones de Aislamiento de red en el equipo aislado.

Si esta casilla está seleccionada, puede añadir una aplicación de este tipo.

Si esta casilla está desactivada, cualquier aplicación del equipo aislado puede iniciar una conexión de red añadida a las exclusiones de Aislamiento de red.

La casilla está desactivada de manera predeterminada.

Añadir

Al hacer clic en este botón, se abre una ventana en la que puede especificar una ruta a una aplicación que puede iniciar una conexión de red añadida a las exclusiones de Aislamiento de red.

Editar

Al hacer clic en este botón, se abre una ventana donde puede editar una ruta a una aplicación añadida.

Este botón está disponible si se elige una aplicación de la lista.

Eliminar

Al hacer clic en este botón, se elimina una aplicación añadida.

Este botón está disponible si se elige una aplicación de la lista.

La ventana de la regla de prevención

Nombre

El nombre de la regla.

Tipo

El tipo de objeto que desea bloquear.

En la sección **Ruta al objeto**, puede seleccionar si desea especificar la ruta completa al objeto que se prohibirá. Si selecciona especificar la ruta, introduzca su valor en el campo correspondiente.

En la sección **Suma de comprobación del objeto**, puede seleccionar si desea especificar la suma de comprobación para el objeto que se prohibirá. Si selecciona especificar la suma de verificación, seleccione su tipo e introduzca el valor en el campo correspondiente.

La ventana "Endpoint Detection and Response (KATA)"

Expandir todo | Contraer todo

Endpoint Detection and Response (KATA)

El interruptor de **Endpoint Detection and Response (KATA)** activa o desactiva el componente Endpoint Detection and Response (KATA) que interactúa con la solución Kaspersky Anti Targeted Attack Platform. Esta solución detecta de inmediato amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas y ataques de día cero, entre otras.

Si el interruptor de **Endpoint Detection and Response (KATA)** está activado, el componente Endpoint Detection and Response (KATA) está activado.

Si el interruptor de **Endpoint Detection and Response (KATA)**) está desactivado, el componente Endpoint Detection and Response (KATA) está desactivado.

Este conmutador está desactivado de forma predeterminada.

Configuración de conexión a servidor

Al hacer clic en este enlace, se abre un cuadro de diálogo donde puede configurar los ajustes para la conexión a los servidores KATA.

Servidores KATA

Esta lista contiene los servidores KATA que ha añadido.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede configurar una conexión a un servidor KATA.

Editar

Al hacer clic en este botón, se abre un cuadro de diálogo donde se puede editar una conexión existente a un servidor KATA.

Este botón está disponible si se selecciona un servidor en la lista de servidores.

Eliminar

Al hacer clic en este botón, se elimina un servidor KATA de la lista de servidores.

Este botón está disponible si se selecciona un servidor en la lista de servidores.

Dirección

Dirección IP de un servidor KATA.

Puerto

Número de puerto de un servidor KATA.

Enviar solicitud de sincronización al servidor KATA cada (min.)

El intervalo entre las solicitudes de sincronización enviadas a un servidor KATA.

El valor predeterminado es 5 minutos.

Usar TTL al enviar eventos

Esta casilla de verificación activa/desactiva TTL para paquetes enviados por Kaspersky Endpoint Security a un servidor KATA. El mecanismo TTL limita la vida útil de los paquetes de eventos al valor especificado en el campo **TTL (h)**.

Si esta casilla de verificación está seleccionada, TTL está activado.

Si esta casilla de verificación no está seleccionada, TTL está desactivado.

Esta casilla de verificación está seleccionada de forma predeterminada.

TTL (h)

La vida útil de los paquetes enviados por Kaspersky Endpoint Security a un servidor KATA.

El valor predeterminado es de 24 horas.

En la sección **Configuración de transmisión de datos**, puede configurar los ajustes para enviar datos a los servidores KATA.

Retraso máximo de transmisión de eventos (s)

El intervalo en el que Kaspersky Endpoint Security envía eventos a un servidor KATA.

El valor predeterminado es de 30 segundos.

Cantidad máxima de eventos por paquete

El número máximo de eventos enviados por Kaspersky Endpoint Security a un servidor KATA por paquete.

El valor predeterminado es 1024 eventos.

En la sección **Limitación de solicitudes**, puede restringir el número de eventos transmitidos.

Activar la limitación de solicitudes

Esta casilla de verificación activa o desactiva la restricción del número de eventos enviados por Kaspersky Endpoint Security a un servidor KATA.

Si esta casilla de verificación está seleccionada, se restringe el número de eventos enviados por la aplicación.

Si esta casilla de verificación está desactivada, el número de eventos enviados por la aplicación no se restringe.

Esta casilla de verificación está seleccionada de forma predeterminada.

Número máximo de eventos por hora

El número máximo de eventos que Kaspersky Endpoint Security envía a un servidor KATA por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora.

El valor predeterminado es 3000 eventos por hora.

Porcentaje de exceso de límite del evento

El umbral de eventos del mismo tipo (porcentaje).

Kaspersky Endpoint Security restringe la transmisión de eventos de un tipo particular si la proporción de eventos de ese tipo con respecto al número total de eventos supera el umbral configurado.

El valor predeterminado es 15 %.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Servidor KATA”

Expandir todo | Contraer todo

Dirección

Dirección IP de un servidor KATA.

Puerto

Número de puerto de un servidor KATA.

El valor predeterminado es 443.

La ventana “Configuración de la conexión al servidor”

Expandir todo | Contraer todo

Tiempo de espera (s)

Se agotó el tiempo de espera de respuesta del servidor KATA. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a otro servidor KATA.

El valor predeterminado es de 10 segundos.

En la sección **Certificado TLS del servidor**, puede añadir o eliminar un certificado TLS y ver información sobre el certificado que añadió.

Añadir certificado TLS

Al hacer clic en este botón, se abre una ventana en la que puede seleccionar un certificado de TLS que se utilizará para establecer una conexión de confianza con un servidor KATA.

Eliminar

Al hacer clic en este botón, se elimina el certificado de TLS actual.

Este botón está disponible si se ha añadido un certificado de TLS.

En la sección **Conexión de seguridad adicional**, puede configurar la protección mejorada para la conexión entre Kaspersky Endpoint Security y un servidor KATA.

Utilizar verificación bidireccional

Esta casilla de verificación activa o desactiva la verificación bidireccional que hace que la conexión entre Kaspersky Endpoint Security y un servidor KATA sea más segura. Para usar la verificación bidireccional, debe cargar un contenedor de cifrado.

Si esta casilla de verificación está seleccionada, Kaspersky Endpoint Security utiliza la verificación bidireccional para conectarse a un servidor KATA.

Si esta casilla está desactivada, Kaspersky Endpoint Security no utiliza la verificación bidireccional para conectarse a un servidor KATA.

Esta casilla de verificación no está seleccionada de forma predeterminada.

Cargar criptocontenedor

Al hacer clic en este botón, se abre una ventana en la que puede seleccionar un contenedor de cifrado que se utilizará para la verificación bidireccional. El archivo de contenedor de cifrado tiene la extensión .PFX.

Nota: El contenedor de cifrado debe estar protegido por contraseña. No es posible añadir un contenedor de cifrado sin una contraseña.

Contraseña de criptocontenedor

La contraseña del contenedor de cifrado utilizado para la verificación bidireccional.

En la sección “Controles de seguridad”

Control web

El conmutador **Control web** activa o desactiva el Control web.

Si el conmutador **Control web** está activado, puede crear reglas para administrar los sitios web que los usuarios visitan en equipos remotos.

Si el conmutador **Control web** está desactivado, no puede administrar los sitios web que los usuarios visitan en equipos remotos.

Este conmutador está desactivado de forma predeterminada.

Lista de reglas

Esta lista contiene las reglas que ha creado para administrar los sitios web que los usuarios visitan en equipos remotos.

El orden en el que se clasifican las reglas determina la prioridad de su aplicación en Kaspersky Endpoint Security.

Agregar

Al hacer clic en este botón, se abrirá una ventana donde puede crear una regla nueva para Control Web.

Eliminar

Hacer clic en este botón elimina la regla seleccionada de la lista de reglas.

Este botón está disponible si se selecciona la casilla de verificación situada junto a la regla.

Subir

Hacer clic en este botón sube la regla seleccionada en la lista de reglas y aumenta la prioridad de su aplicación en Kaspersky Endpoint Security.

Bajar

Hacer clic en este botón baja la regla seleccionada en la lista de reglas y disminuye la prioridad de su aplicación en Kaspersky Endpoint Security.

Nombre

El nombre de la regla.

Estado

El conmutador de esta columna define si la regla está activa o no.

Puede activar o desactivar el conmutador que se encuentra junto a la regla correspondiente para cambiar el estado de la regla.

Acción

La acción que realizará Kaspersky Endpoint Security cuando el usuario visite cierta dirección web, un grupo de direcciones web o la categoría de sitios web que contiene esa regla.

Puede cambiar la acción asignada al seleccionar otra opción en el menú de acceso directo correspondiente en esta columna.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Editar regla”

Introducir el campo de entrada del nombre de la regla

El nombre de la regla.

En la sección **Estado**, puede establecer la regla como activa o inactiva.

Activa

Si esta opción se selecciona, creará una regla activa. Se aplicará al equipo remoto directamente después de que la directiva entre en vigencia.

Inactiva

Si esta opción se selecciona, creará una regla inactiva. Estará pendiente cuando la directiva entre en vigencia.

En la sección **Acción**, puede seleccionar la acción que realizará Kaspersky Endpoint Security cuando el usuario visita cierta dirección web, un grupo de direcciones web o la categoría de sitios web que contiene esa regla.

Permitir

Si esta opción se selecciona, Kaspersky Endpoint Security permite al usuario visitar la dirección web, el grupo de direcciones web o la categoría de sitios web que contiene esa regla.

Nota: Kaspersky Endpoint Security permite visitar recursos web en el equipo remoto si el conmutador de alternancia **Verificación de conexiones seguras (HTTPS)** está activado en la ventana **Red** del Asistente de nueva directiva.

Esta opción está seleccionada de forma predeterminada.

Bloquear

Si esta opción se selecciona, Kaspersky Endpoint Security impide al usuario visitar la dirección web, el grupo de direcciones web o la categoría de sitios web que contiene esa regla.

Nota: Kaspersky Endpoint Security muestra notificaciones cuando el usuario accede a recursos web bloqueados por Control Web en el equipo remoto si se activa el conmutador **Comprobación de conexiones seguras (HTTPS)** en la ventana **Red** del asistente para una nueva directiva.

Mostrar advertencia

Si esta opción se selecciona, Kaspersky Endpoint Security muestra una advertencia cuando el usuario intenta ingresar a la dirección web, el grupo de direcciones web o la categoría de sitios web que contiene esa regla.

En la sección **Área de la regla**, puede decidir crear una regla para una dirección web específica o un grupo de direcciones web o categorías de sitio web.

Categorías

Si esta opción se selecciona, creará una regla para categorías de sitio web.

Seleccionar categorías

Al hacer clic en este vínculo, se abrirá un diálogo en el que puede seleccionar las categorías de sitio web que contiene la regla.

Dirección particular

Si esta opción se selecciona, creará una regla para una dirección web específica o un grupo de direcciones web.

Esta opción está seleccionada de forma predeterminada.

Agregar

Al hacer clic en este botón, se abrirá un diálogo en el que puede especificar una dirección web o una máscara de dirección web que contiene la regla.

Eliminar

Al hacer clic en este botón, se eliminará la dirección web o máscara de dirección web de la lista de direcciones web que contiene la regla.

Este botón está disponible si se selecciona la casilla de verificación situada junto a la dirección web o máscara de dirección web.

Dirección

Direcciones web o máscaras de dirección web que contiene la regla.

El cuadro de diálogo "Agregar dirección web"

Expandir todo | Contraer todo

Introduzca un campo de entrada de la dirección web

Dirección web o máscara de dirección web que contendrá la regla.

El cuadro de diálogo "Categorías de contenido"

Expandir todo | Contraer todo

Lista de categorías de contenido

Esta lista contiene las categorías de sitio web que puede agregar a la regla.

La casilla de verificación junto a un nombre de categoría de sitio web agrega o elimina sitios web que pertenecen a esta categoría en la regla.

Todas las casillas de verificación están desmarcadas de forma predeterminada.

La sección Protección frente a amenazas básicas

Expandir todo | Contraer todo

Protección frente a amenazas en archivos

Al hacer clic en este vínculo, se abrirá una ventana en la que puede configurar los ajustes del componente Protección frente a amenazas en archivos.

Protección frente a amenazas web

Al hacer clic en este vínculo, se abrirá una ventana en la que puede configurar los ajustes del componente Protección frente a amenazas web.

Protección frente a amenazas en la red

Al hacer clic en este vínculo, se abrirá una ventana en la que puede configurar los ajustes del componente Protección frente a amenazas en la red.

Protección frente a amenazas en el correo

Al hacer clic en este enlace, se abrirá una ventana en la que puede configurar los ajustes del componente Protección frente a amenazas en el correo.

Firewall

Al hacer clic en este enlace, se abrirá una ventana en la que puede ajustar la configuración del Firewall.

La ventana "Protección frente a amenazas en archivos"

Protección frente a amenazas en archivos

El conmutador **Protección frente a amenazas en archivos** activa o desactiva el componente Protección frente a amenazas en archivos.

Si el conmutador **Protección frente a amenazas en archivos** está activado, Kaspersky Endpoint Security realiza una supervisión en tiempo real del sistema de archivos de los equipos cliente a los cuales se aplica la directiva.

Si el conmutador **Protección frente a amenazas en archivos** está desactivado, Kaspersky Endpoint Security no protege el sistema de archivos de los equipos cliente a los cuales se aplica la directiva.

Este conmutador está activado de forma predeterminada.

En la sección **Cobertura de protección**, puede establecer una cobertura de protección al seleccionar uno de los elementos presentes o al agregar los archivos o carpetas que desee.

Agregar

Al hacer clic en este botón, se abre un diálogo en el que puede especificar un archivo, una carpeta o una máscara que se agregará a la lista de objetos incluidos en la cobertura de protección.

Eliminar

Al hacer clic en este botón, se elimina un objeto de la cobertura de protección.

Este botón está disponible si se selecciona un objeto en la lista de objetos protegidos.

No se pueden eliminar los objetos predeterminados incluidos en la cobertura de protección.

Cobertura de protección

Esta columna contiene los objetos que analiza Kaspersky Endpoint Security cuando el componente Protección frente a amenazas en archivos está activado.

De forma predeterminada, Kaspersky Endpoint Security analiza los siguientes objetos:

- **Todas los discos extraíbles**. Kaspersky Endpoint Security analiza todas las unidades extraíbles.
- **Todos los discos internos**. Kaspersky Endpoint Security analiza todas las unidades internas.
- **Todos los discos de red**. Kaspersky Endpoint Security analiza todas las unidades de red.

Estado

Si el conmutador en esta columna está activado, Kaspersky Endpoint Security analiza el objeto correspondiente de la columna **Cobertura de protección** cuando la Protección frente a amenazas en archivos está activada.

Si el conmutador en esta columna está desactivado, Kaspersky Endpoint Security no analiza el objeto correspondiente de la columna **Cobertura de protección** cuando la Protección frente a amenazas en archivos está activada.

Adicional

Esta columna indica si Kaspersky Endpoint Security analiza las subcarpetas de un objeto correspondiente.

En la sección **Si se detecta un objeto malicioso**, puede seleccionar la acción que desea que Kaspersky Endpoint Security realice al detectar un objeto malicioso.

Preguntar al usuario

Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el objeto malicioso que ha infectado el archivo y pregunta qué acción desea que lleve a cabo. Las acciones pueden variar en función del estado del objeto.

Esta opción está seleccionada de forma predeterminada.

Desinfectar; eliminar si la desinfección falla

Kaspersky Endpoint Security bloquea el acceso al archivo infectado e intenta desinfectarlo sin solicitar la confirmación del usuario.

Si el archivo está desinfectado, Kaspersky Endpoint Security lo guardará en su ubicación original con el nombre del archivo original. Si la desinfección falla, Kaspersky Endpoint Security elimina el archivo infectado.

Desinfectar; bloquear si la desinfección falla

Kaspersky Endpoint Security bloquea el acceso al archivo infectado e intenta desinfectarlo sin solicitar la confirmación del usuario.

Si el archivo está desinfectado, Kaspersky Endpoint Security lo guardará en su ubicación original con el nombre del archivo original. Si la desinfección falla, Kaspersky Endpoint Security mantiene el archivo infectado en un estado bloqueado en su ubicación original.

En la sección **Optimización**, puede configurar el rendimiento del análisis y seleccionar el algoritmo de análisis.

Analizar solo archivos nuevos y modificados

Esta casilla de verificación activa o desactiva el análisis solo de los archivos que Kaspersky Endpoint Security reconozca como nuevos o modificados desde el último análisis.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará solo los archivos que reconozca como nuevos o modificados desde el último análisis.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará todos los archivos.

Esta casilla de verificación está seleccionada de forma predeterminada.

Omitir el análisis del volumen de sistema de solo lectura

Esta casilla de verificación activa o desactiva el análisis del volumen del sistema de solo lectura por parte de Kaspersky Endpoint Security.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security omite el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el volumen del sistema de solo lectura.

Esta casilla de verificación está seleccionada de forma predeterminada.

Utilizar iSwift

Esta casilla de verificación activa o desactiva el uso de la tecnología iSwift durante el análisis. iSwift permite que Kaspersky Endpoint Security use un algoritmo especial para excluir algunos objetos del análisis, con objeto de aumentar la velocidad del análisis.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security utilizará iSwift durante el análisis.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security no utilizará iSwift durante el análisis.

Esta casilla de verificación está seleccionada de forma predeterminada.

En la sección **Tipos de archivos**, puede seleccionar qué archivos analizará Kaspersky Endpoint Security cuando el componente Protección frente a amenazas en archivos esté activado.

Analizar todos los archivos

Kaspersky Endpoint Security analiza todos los objetos del sistema de archivos que se ejecutan, abren o guardan.

Analizar aplicaciones y documentos (por contenido)

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados según su contenido.

Analizar aplicaciones y documentos (por extensión)

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados según su extensión de archivo.

Kaspersky define la lista de extensiones, que se incluye en las bases de datos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security siempre analiza los archivos sin extensiones.

En la sección **Archivos compuestos**, puede seleccionar los tipos de archivos compuestos que Kaspersky Endpoint Security analiza cuando el componente Protección frente a amenazas en archivos está activado.

Analizar archivos

Esta casilla de verificación activa o desactiva el análisis de archivos. Para ver la lista de extensiones, consulte la ayuda de Kaspersky Endpoint Security.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará los archivos.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los archivos durante el análisis.

Analizar paquetes de instalación

Esta casilla de verificación activa o desactiva el análisis de paquetes de instalación.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará los paquetes de instalación.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los paquetes de instalación durante el análisis.

Analizar los objetos OLE incrustados

Esta casilla activa o desactiva el análisis de los objetos incrustados en un archivo, como hojas de cálculo Excel, macros y archivos adjuntos a un correo electrónico.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security analizará objetos OLE incrustados.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los objetos OLE incrustados durante el análisis.

No extraer archivos que superen los <valor> MB

Esta casilla de verificación activa o desactiva el límite de tamaño de los archivos que se analizarán.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security omitirá los archivos superiores al valor especificado durante el análisis.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security extraerá y analizará los archivos independientemente de su tamaño.

Esta opción está disponible si se selecciona la casilla de verificación **Analizar archivos**.

Posponer la extracción de archivos que superan los <valor> MB

Una opción que limita el tamaño de los archivos que se analizarán.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará todos los archivos cuyo tamaño supere el límite establecido. Sin embargo, lo hará con una prioridad inferior a dos minutos después de detectar este tipo de archivo.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará todos los archivos con la misma prioridad.

Esta opción está disponible si se selecciona la casilla de verificación **Analizar archivos**.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar cobertura de protección”

Expandir todo | Contraer todo

Campo de entrada Escriba el nombre del archivo, carpeta o máscara

Ruta a un archivo, a una carpeta o a una máscara de archivos o carpetas.

El objeto es una carpeta

Esta casilla de verificación activa o desactiva el análisis de un objeto como carpeta.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el objeto que haya especificado en el campo **Escriba el nombre del archivo, carpeta o máscara** como una carpeta.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el objeto que haya especificado en el campo **Escriba el nombre del archivo, carpeta o máscara** como un archivo.

Esta casilla de verificación está seleccionada de forma predeterminada.

Incluir subcarpetas

Esta casilla de verificación activa o desactiva el análisis de las subcarpetas en la carpeta especificada en el campo **Escriba el nombre del archivo, carpeta o máscara**.

Si se selecciona la casilla, Kaspersky Endpoint Security analizará las subcarpetas durante los análisis de software malicioso.

Si no se selecciona esta casilla, Kaspersky Endpoint Security solo analizará los archivos contenidos directamente en la carpeta especificada en el campo **Escriba el nombre del archivo, carpeta o máscara** durante los análisis de software malicioso.

Esta casilla de verificación está seleccionada de forma predeterminada.

La ventana “Protección frente a amenazas web”

Expandir todo | Contraer todo

Protección frente a amenazas web

El conmutador **Protección frente a amenazas web** activa o desactiva el componente Protección frente a amenazas web.

Si el conmutador **Protección frente a amenazas web** está activado, el componente Protección frente a amenazas web analizará los datos entrantes y salientes de su equipo a través de los protocolos HTTP y HTTPS en Safari, Google Chrome o Firefox.

Si el conmutador **Protección frente a amenazas web** está desactivado, el componente Protección frente a amenazas web no analizará los datos entrantes y salientes de su equipo a través de los navegadores web.

Este conmutador está activado de forma predeterminada.

En la sección **Si se detecta un objeto malicioso**, puede seleccionar la acción que desea que Kaspersky Endpoint Security realice al detectar un objeto malicioso.

Preguntar al usuario

Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el tipo de software malicioso que ha infectado el objeto de tráfico web y le pide que elija la acción que desea que aplique este objeto. Las acciones disponibles pueden variar en función del estado del objeto.

Esta casilla acción está seleccionada de forma predeterminada.

Bloquear automáticamente

Kaspersky Endpoint Security bloquea automáticamente el acceso a los objetos de tráfico web peligrosos.

En la sección **Direcciones web de confianza**, puede crear o editar una lista de direcciones web de confianza y activar o desactivar el análisis de tráfico de las direcciones web de esta lista.

No analizar tráfico web de direcciones web de confianza

La casilla de verificación activa o desactiva el análisis del tráfico web de las direcciones web de confianza.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security no analizará el tráfico web de las direcciones web de confianza.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el tráfico web de las direcciones web de confianza.

Esta casilla de verificación no está seleccionada de forma predeterminada.

Lista de direcciones web

Esta lista contiene direcciones web de confianza.

Puede desactivar la casilla de verificación situada junto a una dirección web de la lista. Si no se selecciona la casilla de verificación, el componente Protección frente a amenazas web analizará el tráfico web de la dirección web.

La lista está disponible si se selecciona la casilla de verificación **No analizar tráfico web de direcciones web de confianza**.

Agregar

Al hacer clic en este botón, se abrirá un diálogo en el que puede introducir una dirección web o una máscara de dirección web que se agregará a la lista de direcciones web de confianza.

Eliminar

Al hacer clic en este botón, se eliminará la dirección web o máscara de dirección de la lista de direcciones web de confianza.

Este botón está disponible si se selecciona una dirección web o una máscara de dirección de la lista de direcciones web de confianza.

Dirección web

Esta columna contiene direcciones web de confianza.

Estado

Si el conmutador de esta columna está activado, Kaspersky Endpoint Security no analiza el objeto correspondiente de la columna de **Dirección web** cuando el componente Protección frente a amenazas web está activado y se ha seleccionado la casilla de verificación **No analizar tráfico web de direcciones web de confianza**.

Si el conmutador de esta columna está desactivado, Kaspersky Endpoint Security analiza el objeto correspondiente de la columna **Dirección web** cuando el componente Protección frente a amenazas web está activado y se ha seleccionado la casilla de verificación **No analizar tráfico web de direcciones web de confianza**.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo "Agregar dirección web"

Expandir todo | Contraer todo

Introduzca un campo de entrada de la dirección web

Una dirección web o máscara de dirección web cuyo tráfico no será analizado por el componente Protección frente a amenazas web.

En la sección **Estado**, puede definir si Kaspersky Endpoint Security analiza el tráfico de esta dirección web o grupo de direcciones web.

Desactivar

La dirección web o máscara de dirección web se agrega a la lista de **Direcciones web de confianza**, pero Kaspersky Endpoint Security analiza su tráfico.

Activar

La dirección web o máscara de dirección web se agrega a la lista de **Direcciones web de confianza** y Kaspersky Endpoint Security no analiza su tráfico.

La ventana "Protección frente a amenazas en la red"

Expandir todo | Contraer todo

Protección frente a amenazas en la red

El conmutador **Protección frente a amenazas en la red** activa o desactiva el componente Protección frente a amenazas en la red.

Si el conmutador **Protección frente a amenazas en la red** está activado, Kaspersky Endpoint Security protegerá el equipo remoto frente a ataques de red.

Si el conmutador **Protección frente a amenazas en la red** está desactivado, Kaspersky Endpoint Security no protegerá el equipo remoto frente a ataques de red.

Este conmutador está activado de forma predeterminada.

En la sección de **Configuración de Protección frente a amenazas en la red**, puede modificar el período durante el cual Kaspersky Endpoint Security bloqueará los equipos atacantes.

Bloquear equipos atacantes durante <valor> minutos

Esta casilla de verificación activa o desactiva la adición de equipos atacantes a la lista de equipos bloqueados durante el período especificado.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security agregará los equipos atacantes a la lista de equipos bloqueados durante el período especificado.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security no bloqueará los equipos atacantes.

Esta casilla de verificación está seleccionada de forma predeterminada.

De forma predeterminada, los equipos atacantes se bloquean durante 60 minutos.

En la sección **Exclusiones**, puede crear o editar una lista de las direcciones IP de los equipos remotos cuya actividad de red nunca bloquea Kaspersky Endpoint Security.

Lista de direcciones IP

Contiene las direcciones IP de los equipos remotos a los cuales Kaspersky Endpoint Security nunca bloquea su actividad de red.

Agregar

Al hacer clic en este botón, se abrirá un diálogo en el que puede introducir la dirección IP de un equipo remoto.

Eliminar

Al hacer clic en este botón, se eliminará la dirección IP seleccionada de la lista de direcciones IP.

Este botón está disponible si se selecciona la dirección IP de un equipo remoto de la lista de direcciones IP.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo "Agregar exclusión"

Expandir todo | Contraer todo

Introduzca un campo de entrada de la dirección IP

Dirección IP de un equipo remoto.

La sección "Protección frente a amenazas avanzadas"

Expandir todo | Contraer todo

En la sección **Configuración de KSN**, puede configurar el uso de Kaspersky Security Network.

Kaspersky Security Network

El conmutador **Kaspersky Security Network** activa o desactiva la participación en Kaspersky Security Network.

Si el conmutador **Kaspersky Security Network** está activado, los equipos cliente a los cuales se aplica la directiva participan en Kaspersky Security Network.

Si el conmutador **Kaspersky Security Network** está desactivado, los equipos cliente a los cuales se aplica la directiva no participarán en Kaspersky Security Network.

Este conmutador está desactivado de forma predeterminada.

Modo KSN extendido

El conmutador **Modo KSN extendido** activa o desactiva el envío de datos adicionales desde el equipo remoto a Kaspersky para mejorar la protección de equipos cliente y la utilidad de Kaspersky Endpoint Security.

Si se activa **Modo KSN extendido**, los equipos cliente que se rigen según la directiva proporcionan tanto los datos necesarios para el funcionamiento de los servicios de detección como datos adicionales a Kaspersky Security Network.

Si se desactiva **Modo KSN extendido**, los equipos cliente que se rigen según la directiva proporcionan solo los datos necesarios para el funcionamiento de los servicios de detección y no proporcionan datos adicionales a Kaspersky Security Network.

El conmutador **Modo KSN extendido** está desactivado en forma predeterminada.

El conmutador se activa automáticamente si activa el conmutador **Kaspersky Security Network**, pero se puede desactivar.

Datos proporcionados a Kaspersky cuando usa Kaspersky Security Network en la infraestructura de KSN global

Si el conmutador **Kaspersky Security Network** está activado y el conmutador **Modo KSN extendido** está desactivado, Kaspersky Endpoint Security que se ejecuta en los equipos cliente proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación

del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Versión completa del software instalado;

  tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. de dispositivo único; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

Si los conmutadores **Kaspersky Security Network** y **Modo KSN extendido** están activados, Kaspersky Endpoint Security que se ejecuta en los equipos cliente proporciona a Kaspersky los siguientes datos:

- Información sobre la versión del sistema operativo (SO) y los paquetes de servicios instalados en el ordenador, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo kernel del sistema operativo y los parámetros del modo de ejecución del sistema operativo; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO; versión de Service Pack del SO; fecha y hora de inicio del SO; tiempo de demora del procesamiento del evento acerca de la acción del SO en el subsistema de análisis de comportamiento; cantidad de eventos de acción del tipo actual demorados del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactiva; cantidad de eventos de acciones del SO procesados; cantidad de eventos de acción sincrónicos procesados del SO; demora total de todos los eventos de acción del tipo actual del SO; tiempo de demora de procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento de eventos persistentes; demora total de todos los eventos de acción del SO; cantidad de eventos de acción sincrónicos del SO en espera; fecha y hora del evento recibido por una acción en el SO.

- Información sobre el último reinicio fallido del sistema operativo: número de reinicios fallidos.

- Información sobre la aplicación instalada del Titular de los derechos y el estado de la protección antivirus: id. de instalación del software (PCID); versión del registro de la base de datos del software; el identificador único de la instancia de la instalación de la aplicación en el ordenador, el tipo de aplicación, id. del tipo de aplicación, la versión completa de la aplicación instalada, el identificador de la versión de configuración de la aplicación, el identificador del tipo de ordenador, el identificador único del ordenador en el que está instalada la aplicación, el identificador de Usuario único en los servicios del Titular de los derechos, el idioma regional y el estado de funcionamiento, la versión de los componentes de Software instalados y su estado de funcionamiento, la versión del protocolo utilizado para conectarse con los servicios del Titular de los derechos; versión completa del software instalado; tipo de software instalado; id. de actualización de software; ID del servicio de reputación; ID del tipo de protocolo; ID de un centro de activación regional; versión de la lista de decisiones del servicio de software revocadas; ID del registro activado en las bases de datos Antivirus del software; marca de tiempo del registro desencadenado en las bases de datos antivirus del software; tipo de registro desencadenado en las bases de datos antivirus del software; ID único de la instancia de la instalación de la aplicación en el equipo; fecha de activación de la licencia; fecha de caducidad de la licencia; el identificador de la licencia; estado de la licencia usada por el Software; Tipo de suma de comprobación del objeto que se procesa; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; suma de comprobación del objeto que se procesa; suma de comprobación del código de activación del software; versión completa del Software; id. del Software; suma de comprobación del archivo llave de software; ID del modelo de información utilizado para proveer la licencia del software; Identificador del certificado utilizado para firmar el encabezado del ticket de licencia de software; la fecha y hora de creación del ticket de licencia del software; la suma de comprobación del ticket de licencia del software; La versión del ticket de licencia de software; La versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; ID del ticket de la licencia actual; ID del componente del software; el resultado de la acción del Software; código de error; dirección del servicio web a la que se accedió (URL, IP); número del puerto; dirección web de la fuente de la solicitud del servicio web (origen de referencia); cantidad de ciclos de actualizar y aplicar para bases de datos antivirus; fecha y hora de la última actualización y aplicación de las bases de datos antivirus; Fecha y hora de lanzamiento de las bases de datos del software; versión del componente del Software; id. de actualización de software; tipo del software instalado; fecha y hora de inicio de System Watcher; fecha y hora de instalación del software; probabilidad de enviar estadísticas por medio de System Watcher; código del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por System watcher; tiempo máximo permitido para el procesamiento de un evento por parte de System watcher; tiempo de procesamiento del evento que tardó más tiempo del estándar en ser procesado por System Watcher; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por System Watcher.

- Información sobre todos los objetos y operaciones procesados: veredicto del software del objeto que se procesa; código de directorio; tamaño del objeto que se procesa; suma de control (SHA256) del objeto que se procesa; número del software detectado en el contexto de System Watcher; fecha y hora de detección de software por parte de System Watcher; detectar características; ID del registro activado en las bases de datos Antivirus del software; motivo de detección de software por System Watcher; suma de control (MD5) del objeto que se procesa; resultado de la comprobación de integridad del módulo; nombre del objeto que se procesa; tipo de registro en las bases de datos antivirus del software activado; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; la dirección URL y del referente desde las que se descargó; el tamaño de los archivos analizados y las rutas hasta ellos; la señal del archivo; la fecha y la hora de creación del archivo; el nombre, el tamaño y las sumas de control (MD5, SHA2-256) del compresor (si el

archivo estaba comprimido); la entropía del archivo; el tipo de archivo; el código de tipo de archivo; la señal, el ID y el formato del archivo ejecutable; la suma de control del objeto (MD5, SHA2-256); el tipo y el valor de la suma de control complementaria del objeto; datos sobre la firma digital (certificado) del objeto: datos sobre el editor del certificado, número de inicios del objeto desde el envío de la última estadística, ID de la tarea de análisis de la aplicación, los medios para recibir información sobre la reputación del objeto, el valor del filtro de destino, los parámetros técnicos de las tecnologías de detección aplicables; ruta hacia el objeto que se procesa; código de directorio.

- Para archivos ejecutables: la entropía de las secciones del archivo, la marca de verificación de reputación o la marca de la firma del archivo, el nombre, el tipo, el tipo de ID, la suma de comprobación (MD5) y el tamaño de la aplicación cargada por el objeto que se está validando, la ruta de la aplicación y las rutas de las plantillas, un atributo que indica la presencia de la lista de autoejecución, la fecha de entrada, la lista de atributos, el nombre del compresor e información sobre la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME y la fecha y hora de creación del archivo.

- Información sobre las aplicaciones iniciadas y sus módulos: sumas de comprobación (MD5, SHA2-256) de los archivos en ejecución, tamaño, atributos, fecha de creación, nombre del compresor (si el archivo estaba comprimido), nombres de los archivos, información sobre los procesos que se ejecutan en el sistema (identificación del proceso [PID]), nombre del proceso, información sobre la cuenta desde la que se inició el proceso, la aplicación y el comando que iniciaron el proceso, la ruta completa a los archivos del proceso y la línea de comandos de inicio, una descripción de la aplicación a la que pertenece el proceso (el nombre de la aplicación e información sobre el editor), así como los certificados digitales que se usan e información necesaria para verificar su autenticidad o información sobre la ausencia de firma digital de un archivo e información sobre los módulos cargados en los procesos: sus nombres, tamaños, tipos, fechas de creación, atributos, sumas de comprobación (MD5, SHA2-256, SHA1); las rutas a ellos; la información del encabezado de archivo PE; los nombres de los compresores (si se comprimió el archivo); la información sobre la disponibilidad y validez de estas estadísticas y el identificador del modo para generar las estadísticas que se envían.

- En caso de detectar una amenaza o vulnerabilidad, además de la información sobre el objeto escaneado se deberá proporcionar información sobre el identificador, la versión y el tipo de registro en la base de datos del antivirus; el nombre de la amenaza según la clasificación de Kaspersky, la fecha y la hora de la última actualización de la base de datos del antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de aplicación que solicitó la URL y en la cual ocurrió la detección; la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador del tipo de tráfico en el cual fue detectada la amenaza, el identificador de vulnerabilidad y el nivel de la amenaza recibida, la dirección URL y de referencia de la página web en la cual fue detectada la vulnerabilidad.

- Si se detectase un objeto potencialmente malicioso, se proveerá información sobre los datos contenidos en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo que realiza el ataque y número del puerto del equipo del usuario víctima del ataque de red, ID del protocolo de ataque, y nombre y tipo de ataque.

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

- El URL y la dirección IP del sitio web en el cual fue detectado el contenido malicioso o sospechoso; nombre, dimensión y suma de chequeo del archivo que solicitó dicho URL; identificador, peso y grado de aplicación de la norma establecida para dar el veredicto y objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: el estado de finalización de la tarea de actualización, el tipo de error que podría haber ocurrido durante el proceso de actualización, el número de actualizaciones fallidas y el identificador del componente de la aplicación que realiza las actualizaciones.

- Información acerca del uso de Kaspersky Security Network (KSN): el identificador de KSN, el identificador de la aplicación, la versión completa de la aplicación, la dirección IP impersonal del dispositivo del usuario, indicadores del nivel de satisfacción de las solicitudes de KSN, indicadores de la calidad de procesamiento de paquetes de KSN, indicadores del número de solicitudes de KSN e información sobre los tipos de solicitudes de KSN, fecha y hora en que se inició el envío de estadísticas, fecha y hora en que finalizó el envío de estadísticas, información sobre actualizaciones de configuración de KSN: identificador de la configuración activa, identificador de la configuración recibida y código de error de la actualización de la configuración.

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se ha detectado el evento, tipo y categoría de evento, nombre de la fuente del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la cual se solicita la reputación y el Referente, la conexión del tipo de protocolo de la conexión, el identificador interno del tipo de aplicación, el número del puerto usado, el identificador del Usuario, la suma de comprobación del archivo escaneado (MD5), el tipo de amenaza detectada, información sobre el registro usado para detectar una amenaza (el identificador del registro para las bases de datos antivirus, el registro de la marca de tiempo y el tipo); clave pública del certificado; huella digital del certificado del objeto analizado y algoritmo de hash.

- Datos sobre la distribución territorial de la aplicación: la fecha de la instalación y activación de la aplicación, el ID del partner que proporciona la licencia para la activación de la aplicación, el ID de la aplicación, el ID de localización de idioma de la aplicación, el número de serie de la licencia de activación de la aplicación y el indicio de participación en KSN.

- Información sobre la licencia usada: el tipo de licencia y el período de validez, el número de días hasta la fecha de caducidad de la licencia, el identificador del partner a quien se le compró la licencia, el identificador del centro de activación regional, la suma de comprobación del código de activación, el hash del cuerpo del resguardo calculado mediante el algoritmo SHA1, la fecha y hora de creación del resguardo de la licencia, el identificador de la información de licencia, el identificador del resguardo de la licencia, el identificador de la secuencia del resguardo de licencia, el identificador único del equipo del usuario, la fecha desde la que es válido el resguardo de la licencia, la fecha hasta la que es válido el resguardo de la licencia, el estado actual del resguardo de la licencia, la versión del encabezado del resguardo, la versión de la licencia, el identificador del certificado de la firma del encabezado del resguardo, la suma de comprobación del archivo de claves, el número de serie del firmante del encabezado del resguardo y el token de autenticación.

- Información sobre el hardware instalado en el equipo: tipo, nombre, nombre del modelo, versión de firmware y parámetros de los dispositivos integrados y conectados.
- Información sobre el dispositivo: ID de dispositivo.
- Información sobre el funcionamiento del componente Control web:

  la versión del componente, el motivo de la categorización, información adicional sobre el motivo de la categorización, la URL categorizada y la dirección IP de host de objeto bloqueado/categorizado.

Modo nube

El conmutador de alternancia del **modo nube** activa/desactiva el modo el modo operativo de la aplicación en el que Kaspersky Endpoint Security utiliza una versión ligera de las bases de datos antimalware. Este modo solo está disponible si la participación en Kaspersky Security Network está activada. La versión liviana de las bases de datos antimalware permite usar aproximadamente la mitad de la memoria RAM del equipo que se usaría con las bases de datos completas. Si no participa en Kaspersky Security Network o si el modo nube está desactivado, Kaspersky Endpoint Security descarga la versión completa de las bases de datos antimalware desde los servidores de Kaspersky.

Si el botón de alternancia está activado, Kaspersky Endpoint Security usa la versión liviana de las bases de datos antimalware, lo que reduce la carga de los recursos del sistema operativo.

Nota: Kaspersky Endpoint Security descarga la versión liviana de las bases de datos antimalware durante la siguiente actualización después de seleccionar la casilla.

Si el botón de alternancia está desactivado, Kaspersky Endpoint Security usa la versión completa de las bases de datos antimalware.

Nota: Kaspersky Endpoint Security descarga la versión completa de las bases de datos antimalware durante la siguiente actualización después de deseleccionar la casilla.

Declaración de KSN

Al hacer clic en este vínculo, se abre una ventana en la que puede leer el texto de la Declaración de Kaspersky Security Network y aceptar las condiciones de participación en Kaspersky Security Network.

Nota: Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console y según los ajustes de Kaspersky Security Center, puede participar en Kaspersky Private Security Network en lugar de Kaspersky Security Network. Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la participación en Kaspersky Private Security Network no está disponible. Para obtener información detallada sobre la participación en Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center.

En la sección **Configuración de proxy de KSN**, puede definir la configuración de proxy de KSN.

Utilizar el proxy de KSN

Esta casilla de verificación activa o desactiva el uso de un servidor proxy al conectarse a Kaspersky Security Network.

Si se selecciona la casilla de verificación, Kaspersky Endpoint Security usará un servidor proxy para conectarse a Kaspersky Security Network.

Si no se selecciona la casilla de verificación, Kaspersky Endpoint Security se conectará directamente a Kaspersky Security Network.

Esta casilla de verificación no está seleccionada de forma predeterminada.

Utilizar los servidores de Kaspersky cuando el proxy de KSN no esté disponible

Esta casilla de verificación activa o desactiva el uso de los servicios de Kaspersky si el proxy de KSN no está disponible.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security utilizará los servidores de Kaspersky cuando el proxy de KSN no esté disponible.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security no utilizará los servidores de Kaspersky cuando el proxy de KSN no esté disponible.

Esta casilla de verificación no está seleccionada de forma predeterminada.

La casilla está disponible si se selecciona la casilla de verificación **Utilizar el proxy de KSN**.

Aplicar

Cuando el conmutador **Aplicar** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador **Aplicar** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de configuración de tareas, la configuración de la aplicación, las políticas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana "Participación en Kaspersky Security Network/Kaspersky Private Security Network"

Expandir todo | Contraer todo

Más información

Al hacer clic en este vínculo, se abre una nueva ventana del navegador en la que puede leer el texto de la Declaración de Kaspersky Security Network o la Declaración de Kaspersky Private Security Network.

Acepto las condiciones de participación en Kaspersky Security Network/Kaspersky Private Security Network

Los equipos a los cuales se aplica la directiva participan en Kaspersky Security Network/Kaspersky Private Security Network.

No acepto las condiciones de participación en Kaspersky Security Network/Kaspersky Private Security Network

Los equipos a los cuales se aplica la directiva no participan en Kaspersky Security Network/Kaspersky Private Security Network.

Nota: Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la participación en Kaspersky Private Security Network no estará disponible. Para obtener información detallada sobre la participación en Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center.

El cuadro de diálogo "Conceder acceso"

Expandir todo | Contraer todo

Obtener clave de recuperación

Al hacer clic en este botón, se genera una clave de recuperación requerida para acceder a un disco cifrado en un equipo cliente.

Administrar la aplicación desde la línea de comandos

Puede administrar la aplicación Kaspersky Endpoint Security desde la línea de comandos.

Nota: Una vez instaladas las actualizaciones de módulos de Kaspersky Endpoint Security, la versión de la aplicación cliente en la línea de comandos puede diferir de la versión instalada de la aplicación.

Sintaxis de la línea de comandos:

```
kav <comando> <parámetros>
```

Cada comando tiene su propio rango de parámetros admitidos.

Ver la ayuda de la línea de comandos

Utilice el siguiente comando para ver información sobre la sintaxis de la línea de comandos de la aplicación:

```
kav -? | help
```

Ejecutar análisis de software malicioso

Sintaxis del comando:

```
kav scan <cobertura del análisis> <acción> <tipos de archivos> <exclusiones> <parámetros de informe> <parámetros avanzados>
```

Nota: Para hacer un análisis de software malicioso, también puede abrir la línea de comandos e iniciar una de las tareas creadas en la aplicación. La tarea se inicia con los parámetros especificados en la interfaz de Kaspersky Endpoint Security.

Descripciones de parámetros

`<cobertura del análisis>`: este parámetro especifica una lista de objetos que se analizarán en busca de código malicioso. Puede incluir varios parámetros separándolos por un espacio.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Son posibles los siguientes valores:

- `<archivos>`: lista de las rutas de archivos o carpetas que deben analizarse. Puede especificar rutas absolutas o relativas a los archivos. Los elementos de la lista están separados por un espacio.

  Nota: Si el nombre de un objeto o su ruta incluye un espacio o caracteres especiales (como $, & o @), el nombre debe enmarcarse entre comillas simples (' '), o bien debe agregarse una barra invertida inmediatamente antes de cada uno de los caracteres especiales. Si se incluye una referencia a una carpeta específica, se analizan todos los archivos y carpetas que contenga.

- `-all`: análisis completo del equipo.
- `-remdrives`: todas las unidades extraíbles.
- `-fixdrives`: todas las unidades locales.
- `-netdrives`: todas las unidades de red.
- `-@:<filelist.lst>`: ruta del archivo con una lista de objetos y carpetas dentro de la cobertura del análisis. El archivo debe estar en formato de texto y cada objeto de análisis debe enumerarse en una línea aparte. Solo puede introducirse una ruta absoluta al archivo.

`<acción>`: este parámetro determina la acción que debe realizarse con los objetos maliciosos que se detecten durante el análisis. Si no se define este parámetro, la acción predeterminada es la que corresponda con el valor `-i8`.

Son posibles los siguientes valores:

- `-i0`: no realizar ninguna acción con el objeto; tan solo registrar información sobre el objeto en un informe.
- `-i1`: desinfectar los objetos infectados; ignorarlos si no pueden desinfectarse.
- `-i2`: desinfectar los objetos infectados; eliminarlos si no pueden desinfectarse; no eliminar los contenedores, excepto aquellos con encabezados ejecutables (archivos comprimidos .sfx).
- `-i3`: desinfectar los objetos infectados; eliminarlos si no pueden desinfectarse; eliminar los contenedores por completo si no pueden eliminarse los archivos infectados que contengan.
- `-i4`: eliminar los objetos infectados; eliminar los contenedores por completo si no pueden eliminarse los archivos infectados que contengan.
- `-i8`: preguntar al usuario qué acción llevar a cabo en caso de detectar un objeto infectado (predeterminado).
- `-i9`: preguntar al usuario qué acción llevar a cabo cuando se haya finalizado el análisis.

`<tipos de archivo>`: este parámetro define los tipos de archivos que se someten a análisis de software malicioso. De forma predeterminada, si este parámetro no está definido, solo se analizan los archivos que podrían estar infectados (según el contenido de los archivos).

Son posibles los siguientes valores:

- `-fe`: analizar solo los archivos que podrían estar infectados (según la extensión de archivo).
- `-fi`: analizar solo los archivos que podrían estar infectados (según el contenido del archivo). Este parámetro se utiliza de forma predeterminada.
- `-fa`: analizar todos los archivos.

<exclusiones>: este parámetro define los objetos que se excluirán del análisis. Puede incluir varios parámetros separándolos por un espacio.

Son posibles los siguientes valores:

- -e:a: no analizar los archivos comprimidos.
- -e:b: no analizar las bases de datos de correo electrónico.
- -e:m: no analizar mensajes de correo electrónico en formato de texto.
- -e:<máscara>: no analizar objetos por máscara.
- -e:<segundos>: ignorar los objetos cuyo análisis se prolongue más tiempo del especificado (en segundos).
- -es:<tamaño>: ignorar objetos con un tamaño que supere el valor especificado (en megabytes).

<parámetros de informe>: estos parámetros definen el formato del informe que contiene los resultados del análisis. Puede especificar una ruta al archivo absoluta o relativa del archivo de informe. Si este parámetro no está definido, los resultados del análisis se muestran en pantalla, junto con todos los eventos.

Son posibles los siguientes valores:

- -r:<archivo de informe>: registrar solo los eventos importantes en el archivo de informe especificado.
- -ra:<archivo de informe>: registrar todos los eventos en el archivo de informe especificado.

<parámetros avanzados>: parámetros que definen el uso de las tecnologías de análisis de software malicioso y los archivos de configuración:

- -iSwift=<on|off>: activar/desactivar el uso de iSwift.
- -c:<configuración del archivo>: define la ruta del archivo de configuración que contiene la configuración de la aplicación para realizar las tareas de análisis software malicioso. Puede especificar una ruta al archivo absoluta o relativa. Si este parámetro no está especificado, los valores establecidos en la interfaz de la aplicación se utilizan junto con los valores ya especificados en la línea de comandos.

Ejemplo:

Inicie un análisis de las carpetas ~/Documentos, /Aplicaciones y el archivo denominado my test.exe:

```
kav scan ~/Documentos/Aplicaciones 'my test.exe'
```

Analizar los objetos listados en el archivo objects2scan.txt. Utilizar el archivo de configuración scan_settings.txt. Cuando el análisis concluya, cree un informe para registrar todos los eventos:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Archivo de configuración de ejemplo:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Actualizar la aplicación

Sintaxis del comando:

```
kav update <origen de actualizaciones> <parámetros del informe> <parámetros avanzados>
```

Descripciones de parámetros

<origen de actualizaciones>: un servidor HTTP o una red o carpeta local desde donde descargar actualizaciones. Si no se elige una ruta, el origen de actualizaciones se tomará de la configuración de actualización de la aplicación.

<parámetros del informe>: estos parámetros definen el formato del informe de resultados del análisis. Puede especificar una ruta al archivo absoluta o relativa del archivo de informe. Si el parámetro no está definido, los resultados de actualización se muestran en pantalla, junto con todos los eventos.

Son posibles los siguientes valores:

- -r:<archivo de informe>: registrar solo los eventos importantes en el archivo de informe especificado.
- -ra:<archivo de informe>: registrar todos los eventos en el archivo de informe especificado.

<parámetros avanzados>: parámetro que define el uso de un archivo de configuración.

-c:<archivo de configuración>: define la ruta de un archivo de configuración que contiene la configuración de la aplicación para actualizarla. Puede especificar una ruta al archivo absoluta o relativa. Si no se define este parámetro, se utilizan los valores configurados en la interfaz de la aplicación.

Ejemplo:

Actualice las bases de datos de la aplicación desde el origen predeterminado y registre todos los eventos en el informe:

```
kav update -ra:avbases_upd.txt
```

Actualice los módulos de Kaspersky Endpoint Security con los parámetros del archivo de configuración updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

Anular la última actualización

Sintaxis del comando:

```
kav rollback <parámetros de informe>
```

Importante: Se requieren derechos de administrador para ejecutar este comando.

Descripciones de parámetros

`<parámetros del informe>`: este parámetro define el formato del informe que contiene los resultados de la tarea de deshacer la actualización. Puede especificar una ruta al archivo absoluta o relativa del archivo de informe. Si el parámetro no está definido, los resultados de deshacer se muestran en pantalla, junto con todos los eventos.

Son posibles los siguientes valores:

- `-r:<archivo de informe>`: registrar solo los eventos importantes en el archivo de informe especificado.
- `-ra:<archivo de informe>`: registrar todos los eventos en el archivo de informe especificado.

Ejemplo:

```
kav rollback -ra:rollback.txt
```

Iniciar/detener un componente o una tarea

Sintaxis del comando START:

```
kav start <nombre de la tarea o del componente> <parámetros de informe>
```

Sintaxis del comando STOP:

```
kav stop <nombre de tarea o componente>
```

Importante: Se requieren derechos de administrador para ejecutar el comando de detención.

Descripciones de parámetros

`<nombre de tarea o componente>`: especifica uno de los valores siguientes:

- `fm` o `file_monitoring`: Protección frente a amenazas en archivos
- `wm` o `web_monitoring`: Protección frente a amenazas web
- `ids`: Protección frente a amenazas en la red
- `full` o `scan_my_computer`: tarea de Análisis completo
- `scan_objects`: tarea de Análisis personalizado
- `quick` o `scan_critical_areas`: tarea de Análisis rápido
- `updater`: tarea de actualización

- `rollback`: tarea Deshacer

`<parámetros del informe>`: estos parámetros definen el formato del informe de los resultados de la tarea o del componente. Puede especificar una ruta al archivo absoluta o relativa del archivo de informe. Si este parámetro no está definido, Kaspersky Endpoint Security muestra resultados de acuerdo con parámetros configurados en la interfaz gráfica del usuario.

Nota: `<parámetros de informe>` solo está disponible para los valores `scan_objects`, `updater` y `rollback`.

Son posibles los siguientes valores:

- `-r:<archivo de informe>`: Kaspersky Endpoint Security registra solo los eventos importantes en el archivo de informe especificado.
- `-ra:<archivo de informe>`: Kaspersky Endpoint Security registra todos los eventos en el archivo de informe especificado.

Nota: Los componentes y tareas que se inician desde la línea de comandos se ejecutan con los parámetros definidos desde la interfaz gráfica del usuario.

Ejemplo:

Para activar el componente Protección frente a amenazas en archivos, introduzca el siguiente comando en la línea de comandos:

```
kav start fm
```

Para detener una tarea de análisis completo desde la línea de comandos, escriba el siguiente comando:

```
kav stop scan_my_computer
```

Ver el estado y las estadísticas de un componente o una tarea

Esta es la sintaxis del comando de estado:

```
kav status <nombre de tarea o componente>
```

Esta es la sintaxis del comando de estadísticas:

```
kav statistics <nombre de tarea o componente>
```

Descripciones de parámetros

`<nombre de tarea o componente>`: especifica uno de los valores siguientes:

- `fm` o `file_monitoring`: Protección frente a amenazas en archivos
- `wm` o `web_monitoring`: Protección frente a amenazas web
- `mail_monitoring`: Protección frente a amenazas en el correo
- `ids`: Protección frente a amenazas en la red
- `firewall`: firewall
- `behaviordetection`: detección de comportamiento
- `exploitprevention`: prevención de exploits
- `remediationengine`: motor de reparación
- `devicecontrol`: control de dispositivos
- `webcontrol`: control web
- `full` o `scan_my_computer`: tarea de Análisis completo
- `scan_objects`: tarea de Análisis personalizado
- `quick` o `scan_critical_areas`: tarea de Análisis rápido
- `externalstoragesscanner`: tarea de análisis de disco extraíble

- `updater`: tarea de actualización
- `rollback`: tarea Deshacer
- `diskencryption`: cifrado de disco FileVault
- `edroptimum`: Endpoint Detection and Response Optimum
- `edrkata`: Endpoint Detection and Response (KATA)
- `cloudsandbox`: Sandbox en la nube
- `mdr`: Managed Detection and Response

Nota: Si se ejecuta el comando de estado sin especificar ningún valor para el parámetro `<nombre de tarea o componente>`, se muestra el estado de todas las tareas y componentes de la aplicación. En el caso del comando de estadísticas, debe especificarse un valor para el parámetro `<nombre de tarea o componente>`.

Exportar configuración de protección

Sintaxis del comando:

```
kav export <nombre de tarea o componente> <archivo de exportación>
```

Descripciones de parámetros

`<nombre de tarea o componente>`: especifica uno de los valores siguientes:

- `fm` o `file_monitoring`: Protección frente a amenazas en archivos
- `wm` o `web_monitoring`: Protección frente a amenazas web
- `ids`: Protección frente a amenazas en la red
- `full` o `scan_my_computer`: tarea de Análisis completo
- `scan_objects`: tarea de Análisis personalizado
- `quick` o `scan_critical_areas`: tarea de Análisis rápido
- `updater`: tarea de actualización
- `rollback`: tarea Deshacer

`<archivo de exportación>`: ruta del archivo al que se exporta la configuración de la aplicación. Puede especificar una ruta al archivo absoluta o relativa.

Ejemplo:

```
kav export fm fm_settings.txt
```

Activar la aplicación

Puede activar Kaspersky Endpoint Security aplicando un archivo de claves.

Sintaxis del comando:

```
kav license /add <archivo de claves o código de activación clave>
```

Descripciones de parámetros

`<archivo de claves>`: archivo de claves de la aplicación con la extensión .key.

`<código de activación clave>`: código de activación en formato XXXX-XXXX-XXXX-XXXX.

Ejemplo:

```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

Instalar la extensión de sistema

Sintaxis del comando:

```
kav activatesystemextension /sysext
```

Nota: Debe conceder permisos a Kaspersky Endpoint Security en la configuración de **Privacidad y seguridad** para terminar de instalar la extensión.

Configurar las conexiones de red

Puede configurar las conexiones de red para los componentes Protección frente a amenazas web y Protección frente a amenazas en la red.

Sintaxis del comando:

```
kav activatesystemextension /webav
```

Nota: Debe conceder permisos para el filtrado de contenido de red a Kaspersky Endpoint Security para finalizar la configuración.

Eliminar claves de licencia

Puede eliminar todas las claves de licencia actualmente agregadas a la aplicación.

Sintaxis del comando:

```
kav license /del
```

Importante: Se requieren derechos de administrador para ejecutar este comando.

Devolver códigos de la línea de comandos

Los códigos generales puede devolverlos cualquier comando de la línea de comandos. Los códigos devueltos incluyen códigos generales, así como códigos específicos de tareas concretas.

Sintaxis del comando para recibir el código devuelto:

```
echo $?
```

Códigos devueltos generales:

- `0`: operación finalizada con éxito
- `1`: valor de parámetro no válido
- `2`: error desconocido
- `3`: la tarea devolvió un error
- `4`: tarea cancelada

Códigos devueltos de tareas de análisis de software malicioso:

- `101`: todos los objetos maliciosos procesados
- `102`: objetos maliciosos detectados

Salir de la aplicación

Sintaxis del comando:

```
kav exit
```

Importante: Se requieren derechos de administrador para ejecutar este comando.

Desinstalar la aplicación

Utilice la siguiente secuencia de comandos para desinstalar Kaspersky Endpoint Security desde la línea de comandos:

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

Importante: Se requieren privilegios de administrador para desinstalar la aplicación.

Comandos de administración de Detection and Response

Puede usar la línea de comandos para administrar la funcionalidad integrada de la solución Detection and Response. Puede administrar las soluciones de Detection and Response si la administración mediante la consola de Kaspersky Security Center no es posible.

Administrar Prevención de ejecución

Puede ver los ajustes de Prevención de ejecución del equipo cliente y desactivar la Prevención de ejecución en el equipo cliente.

Sintaxis del comando:

```
kav prevention </disable | /show>
```

Descripciones de los comandos

`/disable`: el comando para desactivar la Prevención de ejecución en el equipo cliente.

`/show`: El comando para mostrar la configuración de Prevención de ejecución actual, incluido el modo y la lista de reglas de Prevención de ejecución.

Administrar Aislamiento de red

Puede ver la configuración de Aislamiento de red del host y desactivar Aislamiento de red en el host.

Sintaxis del comando:

```
kav isolation </off | /status>
```

Descripciones de los comandos

`/off`: El comando para desactivar Aislamiento de red.

Importante: Se requieren derechos de administrador para ejecutar este comando.

`/status`: El comando para mostrar el estado de Aislamiento de red y las exclusiones.

Nota: Estos comandos deben ejecutarse simultáneamente.

Ponerse en contacto con el Servicio de soporte técnico

En esta sección se describe cómo obtener soporte técnico y las condiciones de disponibilidad de dicho servicio.

Cómo obtener soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Endpoint Security o en otras fuentes de información de Kaspersky Endpoint Security, póngase en contacto con el Servicio de soporte técnico de Kaspersky. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas acerca de la instalación y el uso de Kaspersky Endpoint Security.

Nota: Kaspersky proporciona soporte técnico para Kaspersky Endpoint Security durante su ciclo de vida (consulte la página del ciclo de vida de soporte técnico de la aplicación). Antes de ponerse en contacto con el Servicio de Soporte Técnico, lea las normas de soporte .

Puede ponerse en contacto con el Servicio de soporte técnico de una de las siguientes formas:

- Visitando el sitio web del Servicio de soporte técnico
- Enviando una solicitud al Servicio de soporte técnico desde el portal Kaspersky CompanyAccount

Servicio de soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal dirigido a empresas que utilizan aplicaciones de Kaspersky. El portal de Kaspersky CompanyAccount está diseñado para que los usuarios puedan interactuar con los especialistas de Kaspersky mediante el envío de solicitudes en línea. Puede utilizar Kaspersky CompanyAccount para realizar un seguimiento del estado de sus solicitudes en línea, así como guardar un historial.

Puede registrar a todos los empleados de su organización en una única cuenta de Kaspersky CompanyAccount. Una única cuenta permite administrar de forma centralizada las solicitudes electrónicas que envíen los empleados registrados a Kaspersky, así como administrar los privilegios de dichos 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.

Recopilar información para el Servicio de soporte técnico

Para que el soporte y la solución de problemas de la aplicación sean más efectivos, los especialistas del Servicio de soporte técnico pueden pedirle que cambie temporalmente la configuración de la aplicación con el fin de realizar depuraciones durante los diagnósticos. Esta solicitud puede requerir que lleve a cabo lo siguiente:

- Activación de la funcionalidad que reúne información de diagnóstico detallada.
- Ajuste de la configuración de componentes individuales de la aplicación que no están disponibles a través de los elementos estándar de la interfaz de usuario.
- Modificación de la configuración de transmisión de la información de diagnóstico reunida.

Los especialistas del Servicio de soporte técnico le proporcionarán toda la información necesaria para realizar las operaciones y le informarán sobre el alcance los datos que se reunirán con objeto de realizar depuraciones. Después de que se reúna la información de diagnóstico detallada, esta se guardará en el equipo del usuario. Esta información no se envía automáticamente a Kaspersky.

Utilizar un archivo de rastreo

Después de notificar un problema a los especialistas del Servicio de soporte técnico de Kaspersky, puede que le pidan que genere un informe con datos sobre el funcionamiento de Kaspersky Endpoint Security y que lo envíe al Servicio de soporte técnico de Kaspersky. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky también le soliciten que genere un *archivo de rastreo*. El archivo de rastreo permite realizar un examen paso a paso de la ejecución de los comandos de la aplicación y determinar cuándo se producen errores.

Crear un archivo de rastreo

El rastreo es un modo eficaz de registrar información detallada sobre la actividad en las aplicaciones. Los especialistas del Servicio de soporte técnico utilizan archivos de rastreo para solucionar problemas.

Crear un archivo de rastreo

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Seguimientos**, seleccione la casilla **Activar rastreo**.

Importante: Se recomienda que únicamente utilice esta opción cuando se lo indique un especialista del Servicio de soporte técnico de Kaspersky.

Los archivos de rastreo pueden requerir mucho espacio de disco. Cuando ya no necesite rastrear los archivos, desactive el rastreo.

Desactivar rastreo

1. En la barra de menús, haga clic en el icono de la aplicación y elija **Ajustes**.
   Se abre la ventana de ajustes de la aplicación.
2. En la pestaña **Interfaz** de la sección **Seguimientos**, desmarque la casilla de verificación **Activar rastreo**.

Kaspersky Endpoint Security guarda la siguiente información en un archivo de rastreo:

- Información sobre el dispositivo y el sistema operativo (ID exclusivo del dispositivo, tipo de dispositivo, direcciones MAC de dispositivos de red, tipo de sistema operativo, versión del sistema operativo).
- Información sobre la operación de la aplicación y sus módulos.
- Información sobre la suscripción (tipo de suscripción, región).
- Información sobre la configuración regional del idioma, ID de la aplicación, personalización de la aplicación, versión de la aplicación, ID exclusivo de instalación de la aplicación, ID exclusivo del equipo.
- Información sobre el estado de protección contra software malicioso del equipo, así como sobre todos los objetos detectados y procesados (el nombre del objeto detectado, la fecha y hora de la detección, la dirección web de descarga, los nombres y tamaños de los archivos infectados y sus rutas, la dirección IP del equipo atacante y el número de puerto del equipo al que se dirige el ataque de red, la lista de actividad de software malicioso y las direcciones web no deseadas) y las acciones relevantes y decisiones tomadas por la aplicación y el usuario.
- Información sobre las aplicaciones descargadas por el usuario (dirección web, cualidades, tamaño de archivo e información sobre el proceso de descarga del archivo).
- Información sobre las aplicaciones iniciadas y sus módulos (tamaño, tributos, fecha de creación, detalles del encabezado del PE, región, nombre, ubicación y compresores).
- Información sobre los errores de interfaz y el uso de la interfaz de la aplicación de Kaspersky instalada.
- Información sobre conexiones de red: la dirección IP del equipo remoto y del equipo del usuario, los números de puertos a través de los que se estableció la conexión y el protocolo de red de la conexión.
- Información sobre los paquetes de red recibidos y enviados por el equipo sobre las redes de TI y de telecomunicaciones.
- Información sobre los mensajes de correo electrónico e instantáneos enviados y recibidos.
- Información sobre las direcciones web visitadas: la hora en que se estableció la conexión con un protocolo abierto, los datos de inicio de sesión y la contraseña del sitio web, y el contenido de las cookies.
- Certificado público del servidor.

Los archivos de rastreo solo contienen la información necesaria para corregir defectos de la aplicación. Kaspersky utiliza los archivos de rastreo para investigar los incidentes asociados a errores en el funcionamiento de la aplicación Kaspersky Endpoint Security.

De forma predeterminada, la creación de archivos de rastreo está desactivada. Puede activar la generación de archivos de rastreo en los ajustes de la aplicación.

Los archivos de rastreo se pueden enviar a Kaspersky solo de forma manual. La aplicación no envía los archivos de rastreo a Kaspersky de manera automática.

Puede elegir cómo se envían los archivos de rastreo a Kaspersky.

Antes de enviar archivos de rastreo a Kaspersky, examine los datos que contienen.

Importante: Los archivos de rastreo pueden contener información personal o confidencial. Al enviar archivos de rastreo a Kaspersky, acepta proporcionarle a Kaspersky todos los datos almacenados en los archivos de rastreo que envía y también acepta el método usado para enviarlos.

Fuentes de información sobre la aplicación

La página de Kaspersky Endpoint Security en el sitio web de Kaspersky

En la página de Kaspersky Endpoint Security del sitio web de Kaspersky, puede consultar información general sobre la aplicación, sus funciones y sus características.

La página de Kaspersky Endpoint Security en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web del Servicio de soporte técnico de Kaspersky.

En la página de Kaspersky Endpoint Security en la Base de conocimientos puede leer artículos que ofrecen información útil, recomendaciones y respuestas a preguntas frecuentes sobre cómo comprar, instalar y utilizar la aplicación.

Los artículos de la Base de conocimientos pueden proporcionar respuestas a preguntas relacionadas con Kaspersky Endpoint Security, así como con otras aplicaciones de Kaspersky. También pueden contener novedades del Servicio de soporte técnico de Kaspersky.

Ir a la Base de conocimientos desde el menú desplegable Ayuda

1. Elija **Ayuda** > **Soporte**.
2. Haga clic en **Servicio de soporte técnico**.

Hable sobre las aplicaciones de Kaspersky en el Foro de soporte de Kaspersky

Si su pregunta no requiere una respuesta inmediata, puede compartirla con los expertos de Kaspersky y el resto de los usuarios en nuestro Foro.

En el Foro, podrá consultar los temas de debate, publicar comentarios y crear nuevos temas.

Ir al Foro desde el menú desplegable Ayuda

1. Elija **Ayuda** > **Soporte**.
2. Haga clic en **Comunidad**.

Nota: Se requiere una conexión a Internet para acceder a los recursos del sitio web.

Si no encuentra una solución a un problema que tenga, póngase en contacto con Servicio de soporte técnico de Kaspersky.

Materiales de ayuda incluidos con la aplicación

La aplicación incluye la ayuda completa y la ayuda contextual.

La ayuda completa proporciona información acerca de cómo configurar y usar Kaspersky Endpoint Security.

La ayuda contextual proporciona información sobre las ventanas de Kaspersky Endpoint Security, describe la configuración de Kaspersky Endpoint Security y contiene enlaces a descripciones de tareas en las que se utiliza dicha configuración.

La ayuda se puede incluir en el kit de distribución o se puede encontrar en el sitio web de Kaspersky. Se requiere una conexión a Internet para ver la ayuda en línea.

Ayuda en línea (esta ayuda)

En esta ayuda, puede encontrar información sobre cómo llevar a cabo los siguientes procedimientos:

- Preparación para la instalación de la aplicación, instalación y activación de la aplicación.
- Configuración y uso de la aplicación.
- Administración remota de la aplicación mediante Kaspersky Security Center.

Apéndices

Sección que ofrece información complementaria del texto del documento.

Problemas conocidos y limitaciones

Kaspersky Endpoint Security tiene los siguientes problemas y limitaciones conocidos:

- Si se instala en el ordenador una aplicación que recopila información y la envía para ser procesada, la aplicación Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis configurando la aplicación Kaspersky Endpoint Security como se describe en este documento.
- La configuración funcional de la aplicación se pueden modificar editando los archivos de configuración.
- En Kaspersky Security Center, las tareas locales pueden aparecer dos veces en las propiedades de los dispositivos administrados.
- Cambiar el origen de actualizaciones de una tarea de actualización local desactiva automáticamente la ejecución de la tarea de actualización.
- Si inicia una tarea de reinicio del ordenador a través de la Consola de administración con un mensaje para el usuario que contiene un punto y coma (;), la tarea se muestra como completada pero no se le solicita al usuario que reinicie el Mac.
- Para excluir el tráfico de red de Safari del análisis de Kaspersky Endpoint Security, debe añadir las siguientes rutas a la lista de exclusiones:
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.apple.Safari.SearchHelper.xpc`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit.networking.xpc/contents/macc`
- Para excluir el tráfico de red de Google Chrome del análisis de Kaspersky Endpoint Security, debe añadir la siguiente ruta a la lista de exclusiones:
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- Después de crear un perfil de directiva para una directiva de Kaspersky Endpoint Security mediante Kaspersky Security Center Web Console y Cloud Console, deberá verificar que la configuración se aplique correctamente en los ordenadores cliente.
- Al activar el cifrado de disco FileVault en la configuración de las directivas, los usuarios con derechos de administrador pueden descifrar el disco de inicio de su Mac desde Configuración del sistema (Preferencias del Sistema).
- Los cambios en las opciones del servidor proxy se aplicarán solo después de que se reinicie Kaspersky Endpoint Security.
- Es posible que Safari no se conecte a un sitio web que tenga un certificado no fiable. Puede añadir este sitio web a las exclusiones o utilizar otro navegador.
- Después de desinstalar Kaspersky Endpoint Security 11.2 o versiones posteriores de manera remota mediante Kaspersky Security Center, es posible que una de las extensiones del sistema de la aplicación quede en la memoria del ordenador. Después de eso, en raras ocasiones, puede ocurrir un problema con el permiso acceso total al disco al instalar Kaspersky Endpoint Security. En este caso, recomendamos desinstalar la aplicación localmente y volver a instalarla.
- Es posible que las aplicaciones que necesitan Rosetta no se instalen si Kaspersky Endpoint Security se está ejecutando. Para resolver el problema, salga de Kaspersky Endpoint Security e intente volver a instalar la aplicación.
- Los detalles de alerta para amenazas detectadas dentro de objetos compuestos contienen información únicamente sobre el objeto detectado en sí, sin un gráfico de la cadena de desarrollo de la amenaza.
- Al guardar una contraseña para la protección con contraseña, puede haber un error. En este caso, recomendamos desinstalar y volver a instalar la aplicación.
- Kaspersky Endpoint Security no analiza archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.
- No se puede analizar un objeto puesto en cuarentena como resultado de la tarea Mover archivo a cuarentena.
- En Kaspersky Security Center, el nombre del dispositivo se muestra correctamente solo si el nombre NetBIOS, el nombre del ordenador y el nombre del host son los mismos.

Lista de objetos analizados por extensión

Si al crear una tarea de análisis en Kaspersky Security Center, en la configuración de análisis ha seleccionado la opción **Analizar aplicaciones y documentos (por extensión)**, Kaspersky Endpoint Security realiza análisis de software malicioso en objetos sin extensiones y objetos con las siguientes extensiones:

Formatos generales:

- txt
- csv
- htm
- html

Archivos multimedia (audio/vídeo):

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg
- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape
- ogg
- aac

- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

Archivos de imagen:

- jpg
- jpe
- jpeg
- jff
- gif
- png
- bmp
- tif
- tiff
- emf
- wmf
- eps
- psd
- cdr
- swf

Archivos ejecutables y del sistema:

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o

- so
- elf
- prx
- vb
- vbs
- js
- bat
- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

Documentos y plantillas:

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx
- potx
- pptm
- potm
- ppsx

- ppsm
- rtf
- pdf
- msg
- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde
- accdr
- accdc
- chm
- mht

Archivos:

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz

- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

Nota: El formato real de un archivo puede no corresponderse con el formato indicado por su extensión.

Máscaras en rutas a archivos y carpetas

Una *máscara de nombre de archivo* o *máscara de nombre de carpeta* representa el nombre y la extensión de un archivo o el nombre de una carpeta mediante el uso de símbolos comunes.

Puede utilizar estos símbolos para especificar la cobertura de la protección, la cobertura del análisis y la zona de confianza:

- El símbolo de la virgulilla (`~`) sustituye `/Usuarios/<nombre de usuario>` en la ruta a un archivo o una carpeta. Por ejemplo, la ruta `~/Escritorio` significa que la cobertura de protección incluye las carpetas del escritorio de todos los usuarios en los equipos que desea proteger.
- El símbolo del asterisco (`*`) sustituye cualquier conjunto de caracteres en el nombre de archivo o carpeta, excepto los caracteres `\` y `/` (que delimitan los nombres de archivos y carpetas en las rutas a archivos y carpetas). Por ejemplo, la máscara `/*/*.txt` incluirá todas las rutas a los archivos con la extensión TXT ubicados en las carpetas del disco interno, pero no en las subcarpetas.
- Dos símbolos consecutivos de asterisco (`**`) sustituyen cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre de archivo o carpeta, incluidos los caracteres `\` y `/` (que delimitan los nombres de archivos y carpetas en las rutas a archivos y carpetas). Por ejemplo, la máscara `/Carpeta/**/*.txt` incluirá todas las rutas a los archivos con extensión TXT ubicados en la carpeta denominada Carpeta y sus subcarpetas. La máscara debe incluir al menos un nivel de anidamiento. La máscara `/**/*.txt` no es una máscara válida.
- El signo de interrogación (`?`) sustituye cualquier carácter del nombre de archivo o carpeta, excepto los caracteres `\` y `/` (que delimitan los nombres de archivos y carpetas en las rutas a archivos y carpetas). Por ejemplo, la máscara `/Carpeta/???.txt` incluirá las rutas a todos los archivos ubicados en la carpeta denominada Carpeta que tengan la extensión TXT y un nombre formado por tres caracteres.

Requisitos del archivo de IOC

Al crear tareas de Análisis de IOC, tenga en cuenta los siguientes requisitos y limitaciones del archivo de IOC:

- La aplicación admite archivos de IOC con las extensiones IOC, XML y JSON en las versiones 1.0 y 1.1 del estándar abierto OpenIOC, o las versiones 2.0 y 2.1 de STIX, para describir indicadores de vulneración.
- Si, al momento de crear una tarea de Análisis de IOC en la línea de comandos, carga archivos de IOC, algunos de los cuales no son compatibles, cuando se ejecuta la tarea, la aplicación usa solo los archivos de IOC compatibles. Si, al momento de crear una tarea de análisis de IOC en la línea de comandos, todos los archivos de IOC que carga resultan no compatibles, la tarea aún se puede ejecutar, pero no detectará ningún indicador de peligro. No es posible cargar archivos de IOC no compatibles mediante Web Console o Cloud Console.
- Los errores semánticos y los términos y etiquetas de IOC no compatibles en los archivos de IOC no provocan un error en la ejecución de la tarea. En dichas secciones de los archivos de IOC, la aplicación no detecta ninguna coincidencia.
- Los identificadores de todos los archivos de IOC utilizados en una única tarea de análisis de IOC deben ser únicos. Si hay archivos de IOC con el mismo identificador, puede afectar los resultados de la ejecución de la tarea.
- Un archivo de IOC único no debe tener un tamaño mayor que 2 MB. El uso de archivos más grandes hará que las tareas del análisis de IOC finalicen con un error. El tamaño total de todos los archivos añadidos a la colección de IOC no debe exceder los 10 MB. Si el tamaño total de todos los archivos supera los 10 MB, debe dividir la colección de IOC y crear varias tareas de Análisis de IOC.
- Se recomienda crear un archivo de IOC por amenaza. Esto facilita el análisis de los resultados de la tarea de Análisis de IOC.

Las características y limitaciones de la compatibilidad de la aplicación con los archivos de IOC se muestran en la siguiente tabla.

Características y limitaciones de la compatibilidad con los documentos del IOC.

Condiciones admitidas	OpenIOC 1.0:
	`is`
	`isnot` (como excepción del conjunto)
	`contains`
	`containsnot` (como excepción del conjunto)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	STIX 2.0 y 2.1:
	`=`
	`!=`
	`>`
	`<`
	`=>`
	`<=`
	`in`
	`like`
	`matches`

Atributos de condición admitidos	OpenIOC 1.1:
	`preserve-case`
	`negate`

Operadores compatibles	`AND` `OR`
Tipos de datos compatibles	`"date"`: fecha (condiciones aplicables: `is`, `greater-than`, `less-than`) `"int"`: entero (condiciones aplicables: `is`, `greater-than`, `less-than`) `"string"`: cadena (condiciones aplicables: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duración en segundos (condiciones aplicables: `is`, `greater-than`, `less-than`)

Características de la interpretación de tipos de datos	Los tipos de datos `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` se interpretan como cadenas.
	La aplicación admite la interpretación de la configuración de `Content` para los tipos de datos `int` y `date` cuando se establece en forma de intervalos:
	OpenIOC 1.0:
	Usar el operador `TO` en el campo `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`

`<Content type="int">[154192 TO 154192]</Content>`

OpenIOC 1.1:

Usar las condiciones `greater-than` y `less-than`

Usar el operador `TO` en el campo `Content`

La aplicación admite la interpretación de los tipos de datos `date` y `duration` si los indicadores se configuran en `ISO 8601`, `Zulu Time Zone`, `UTC format`.

Intérpretes de scripts admitidos para Prevención de ejecución

Prevención de ejecución admite los siguientes intérpretes de scripts:

- PkgUtil
- PkgInstaller
- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

Importante: Si los intérpretes de scripts PkgUtil o PkgInstaller ya iniciados abrieron el script especificado en la regla de Prevención de ejecución, la ejecución de este script no se bloqueará.

Cómo añadir el certificado de Kaspersky Endpoint Security al almacenamiento de certificados de Mozilla Firefox

Si el navegador utiliza el almacenamiento de certificados de Mozilla Firefox, debe exportar y añadir el certificado de Kaspersky a este almacenamiento de certificados de manera manual. De lo contrario, el navegador no podrá abrir páginas HTTPS.

Exporte el certificado de Kaspersky

1. Abra **Launchpad** > **Otro** > **Acceso a llaveros** en su Mac.
2. En el panel izquierdo de la ventana, haga clic en **Sistema** y abra la pestaña **Certificados**.
3. En la lista de certificados, busque **Autoridad de certificación de Kaspersky Web Anti-Virus**.
4. Haga clic con el botón derecho en este certificado y escoja **Exportar "Autoridad de certificación de Kaspersky Web Anti-Virus"**.
5. Seleccione una ubicación donde guardar el certificado y haga clic en **Guardar**.

Se guardó el certificado de Kaspersky.

Añada el certificado de Kaspersky al almacenamiento de certificados de Mozilla Firefox

1. Abra Mozilla Firefox
2. En la esquina superior derecha, haga clic en el botón de menú y seleccione **Ajustes**.
3. En el panel izquierdo de la ventana, seleccione **Privacidad y seguridad**.
4. Desplácese hacia abajo hasta la sección **Certificados**.
5. Haga clic en **Ver certificados**.
6. En la ventana que se abre, haga clic en **Importar**.
7. Escoja el archivo de certificado de Kaspersky y haga clic en **Abrir**.
8. Seleccione las casillas **Confiar en esta CA para identificar sitios web** y **Confiar en esta CA para identificar a los usuarios de correo electrónico**. Haga clic en **Aceptar**.

   El certificado de Kaspersky se importa al almacenamiento de certificados de Mozilla Firefox. Se muestra en la lista de certificados en la ventana **Administrador de certificados**.

Importante: Cada vez que se reinstala la aplicación de Kaspersky Endpoint Security, se genera un nuevo certificado raíz de Kaspersky. Esto significa que debe completar este procedimiento después de cada reinstalación de la aplicación de Kaspersky Endpoint Security.

Información sobre código de terceros

La información sobre código de terceros se incluye en el archivo legal_notices.txt en la carpeta donde se instaló la aplicación.

Avisos sobre las marcas comerciales

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

App Store, Apple, Apple Remote Desktop, FileVault, iCloud, Keychain, Launchpad, Mac, Mac Pro, macOS, Rosetta, Safari y Xcode son marcas comerciales de Apple Inc.

IOS es una marca comercial o una marca comercial registrada de Cisco Systems, Inc. o sus filiales en Estados Unidos y en otros países.

Android, Chrome, Chromium, Google y Google Chrome son marcas comerciales de Google LLC.

Intel es una marca comercial de Intel Corporation o sus subsidiarias.

Linux es la marca comercial registrada de Linus Torvalds en los Estados Unidos y otros países.

Excel, IIS, Internet Explorer, Microsoft, Microsoft Edge, Windows, Windows Installer, Windows Phone y WMI son marcas comerciales del grupo de empresas Microsoft.

Firefox y Mozilla son marcas comerciales de Mozilla Foundation en EE. UU. y otros países.

Java y JavaScript son marcas comerciales registradas de Oracle y/o sus empresas afiliadas.

Parallels, el logotipo de Parallels y Coherence son marcas comerciales o marcas comerciales registradas de Parallels International GmbH.

VMware y VMware Fusion es una marca comercial o una marca comercial registrada de VMware, Inc. en Estados Unidos y otros países.

JAMF y Composer son marcas comerciales registradas o de derecho consuetudinario de JAMF SOFTWARE, LLC en los EE. UU. y otros países.

La ventana “Archivo comprimido protegido por contraseña detectado”

Si Kaspersky Endpoint Security debe analizar un archivo protegido por contraseña mientras se está ejecutando el componente Protección frente a amenazas en archivos o una tarea de análisis, aparecerá una ventana de notificación.

Archivo

Ruta al archivo.

Contraseña

Campo para introducir la contraseña.

Si introduce la contraseña, Kaspersky Endpoint Security analiza el archivo comprimido en busca de software malicioso y otras amenazas de seguridad informática.

Omitir archivos protegidos

Al hacer clic en este botón, se ignora el objeto, así como todos los objetos de ese mismo tipo.

Omitir

Al hacer clic en este botón, se ignora el objeto.

El cuadro de diálogo El servidor proxy requiere autenticación

Nombre de usuario

Campo para introducir el nombre de usuario de conexión al servidor proxy.

Contraseña

Campo para introducir la contraseña.

Recordar contraseña

Esta casilla de verificación activa o desactiva el uso del nombre de usuario y contraseña especificados para la autenticación futura en el servidor proxy.

Esta casilla no está seleccionada de forma predeterminada.

Cuadro de diálogo "Objeto detectado"

Cuando Kaspersky Endpoint Security detecta un virus u otra amenaza de seguridad, aparece una ventana de notificación en la pantalla.

Detectado

El nombre del objeto según la clasificación de la Enciclopedia de virus de Kaspersky.

Detalles

Al hacer clic en este botón, se abre una página de la Enciclopedia de virus de Kaspersky con información sobre el objeto detectado.

Objeto

Ruta a la carpeta con el objeto detectado o la dirección web en la que este se ha detectado.

Aplicar a todo

Esta casilla de verificación activa o desactiva la acción seleccionada para todos los objetos del mismo tipo durante la sesión actual de Protección frente a amenazas en archivos, Protección frente a amenazas web o una tarea de análisis de software malicioso.

Esta casilla está desmarcada de forma predeterminada.

La sesión actual de Protección frente a amenazas en archivos o Protección frente a amenazas web se define como el período desde que se inicia el componente hasta que se detiene, o bien hasta que se sale de la aplicación o esta vuelva a iniciarse. La sesión actual de tareas de análisis de software malicioso se define como el período que va desde el inicio de una tarea de análisis de software malicioso hasta su finalización.

Los botones con las acciones que puede ejecutar sobre los objetos detectados varían en función del tipo de objeto detectado.

Puede seleccionar una de las siguientes acciones:

- **Desinfectar**. Desinfecta el objeto. Antes de ejecutar la desinfección Kaspersky Endpoint Security crea una copia de seguridad del archivo por si necesitara restaurar el archivo original.
- **Eliminar**. Elimina el objeto. Antes de eliminar el objeto Kaspersky Endpoint Security crea una copia de seguridad del archivo por si necesitara restaurar el archivo original.
- **No bloquear**. Permite el acceso a un sitio web considerado objeto de tráfico web peligroso.
- **Bloquear**. Deniega el acceso a un sitio web considerado objeto de tráfico web peligroso.
- **Eliminar archivo**. Elimina el archivo comprimido que contiene el objeto detectado.
- **Omitir archivos protegidos**. Ignora archivos comprimidos protegidos con contraseña durante los análisis de software malicioso.
- **Omitir**. Bloquea el acceso al objeto, pero no realiza ninguna otra acción con él.

La ventana Análisis



Al hacer clic en este botón, volverá a la ventana anterior de Kaspersky Endpoint Security.



Al hacer clic en este botón, avanzará hasta la siguiente ventana de Kaspersky Endpoint Security.



Al hacer clic en este botón, se eliminan todos los registros de todas las tareas de análisis de software malicioso de la ventana **Análisis**.

Planificar análisis

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede planificar tareas de Análisis completo o Análisis rápido.

Análisis rápido

Al hacer clic en el botón de inicio ( ) en esta sección se ejecuta una tarea de Análisis rápido.

Análisis completo

Al hacer clic en el botón de inicio ( ) en esta sección se ejecuta una tarea de Análisis completo.

Al hacer clic en este botón se detiene la tarea de análisis de software malicioso seleccionada.

Este botón aparece si una tarea de análisis de software malicioso se está ejecutando.

Ajustes

Al hacer clic en este botón, se abre la pestaña **Análisis** en la que puede establecer los ajustes de las tareas de análisis.

Seleccionar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede elegir el archivo o carpeta que quiera analizar.

En la parte inferior de la sección **Archivos y carpetas**, puede ver los registros de todas las tareas de análisis de software malicioso realizadas en los archivos o las carpetas seleccionados.

Detalles

Al hacer clic en este botón, se abre la ventana del informe de la tarea de análisis de software malicioso.

Esto botón aparece al mantener el puntero sobre la tarea de análisis.

Borrar historial de análisis

Al hacer clic en este botón, se eliminan todos los registros de todas las tareas de análisis de software malicioso.

Mostrar todo

Al hacer clic en este botón, se abre la ventana **Objetos detectados**, donde puede ver todos los objetos detectados.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

La ventana Objetos detectados

La sección **Objetos detectados** contiene los objetos maliciosos detectados por la aplicación.

Desinfectar todo

Al hacer clic en este botón, se inicia la desinfección de todos los objetos maliciosos que se hayan detectado.

Ignorar todo

Al hacer clic en este botón se eliminan todos los objetos maliciosos de la lista de objetos maliciosos en la sección **Objetos detectados**.

Al hacer clic en este botón, se abre un menú emergente en el que puede seleccionar una de las acciones siguientes que puede llevar a cabo con un objeto malicioso:

- **Desinfectar**. Desinfecta el objeto. Antes de la desinfección, la aplicación Kaspersky Endpoint Security crea una copia de seguridad del archivo para poder restaurarlo o desinfectarlo posteriormente sin riesgo de pérdida de datos.
- **Ignorar**. Eliminar el objeto de la lista de objetos detectados.

La sección **Otros objetos** contiene objetos detectados que no son maliciosos, pero que los piratas podrían usar para hacerle daño a su equipo o datos.

Eliminar todo

Al hacer clic en este botón se eliminan de su equipo todos los objetos detectados.

Ignorar todo

Al hacer clic en este botón se eliminan todos los objetos detectados de la lista de objetos detectados en la sección **Otros objetos**.

Al hacer clic en este botón, se abre un menú emergente en el que puede seleccionar una de las acciones siguientes para llevar a cabo con un objeto detectado:

- **Eliminar**. Eliminar el objeto detectado de su equipo.
- **Ignorar**. Eliminar el objeto de la lista de objetos detectados.

La sección **Copia de seguridad** contiene copias de seguridad de objetos detectados.

Eliminar todo

Al hacer clic en el botón, se eliminan todas las copias de seguridad en cuarentena de objetos detectados de su equipo.

Al hacer clic en este botón, se abre un menú emergente en el que puede seleccionar una de las acciones siguientes para llevar a cabo con un objeto con copia de seguridad:

- **Eliminar copia de seguridad**. Elimine de su equipo la copia de seguridad en cuarentena del objeto detectado.
- **Restaurar archivo**. Restaurar la copia de seguridad del archivo seleccionado en la lista a su ubicación original con el mismo nombre que tenía antes de la desinfección o eliminación. Si ya existe un objeto con el mismo nombre en la ubicación original (por ejemplo, si Kaspersky Endpoint Security

creó una copia del archivo original antes de la desinfección o si desinfectó el archivo original), se muestra una advertencia. Puede modificar la ubicación del objeto que desea restaurar o cambiarle el nombre a este.

La ventana Licencia



Al hacer clic en este botón, volverá a la ventana anterior de Kaspersky Endpoint Security.



Al hacer clic en este botón, avanzará hasta la siguiente ventana de Kaspersky Endpoint Security.

Nota: Esta ventana varía si se activa Kaspersky Endpoint Security y por el tipo de la licencia o suscripción utilizada.

Esta ventana puede contener la siguiente información:

- Estado de la licencia o suscripción
- Claves activas
- Claves de reserva (si existen)
- El tipo de licencia y el número de equipos en los que puede utilizar la aplicación con la licencia o la suscripción actuales
- Funciones de la aplicación que están disponibles con la licencia o suscripción actuales
- Fecha y hora de vencimiento de la licencia
- Número de días hasta la caducidad de la licencia

En esta ventana, puede realizar las siguientes acciones:

- Activar la aplicación mediante un código de activación.
- Vaya a un sitio web con información sobre cómo comprar una licencia en la tienda en línea de Kaspersky.
- Abra el sitio web del proveedor de Kaspersky Endpoint Security que contiene información sobre la renovación de la suscripción.
- Actualizar el estado de su suscripción.

Para obtener más información sobre la licencia de Kaspersky Endpoint Security, comuníquese con el administrador del sistema en su organización.

La pestaña Protección

En la sección **General**, puede activar o desactivar la protección del equipo contra software malicioso y otras amenazas de seguridad.

Activar protección

Esta casilla de verificación activa o desactiva la protección en tiempo real contra software malicioso y otras amenazas de la seguridad informática.

Esta casilla está seleccionada de forma predeterminada.

Comprobar conexiones seguras (HTTPS)

Esta casilla de verificación activa o desactiva el análisis de conexiones cifradas (HTTPS) de Kaspersky Endpoint Security y muestra notificaciones cuando el Control Web bloquea el acceso del usuario a recursos web peligrosos.

Esta casilla no está seleccionada de forma predeterminada.

Zona de confianza

Al hacer clic en este botón, se abre una ventana en la que puede editar la Zona de confianza creando una lista de objetos en los que confía y que no desea analizar en busca de software malicioso.

Ajustes

Al hacer clic en este botón, se abre una ventana en la que puede administrar la lista de certificados raíz de confianza y seleccionar el almacén de certificados para verificar el tráfico HTTPS cifrado en el navegador Mozilla Firefox.

En la sección **Protección frente a amenazas en archivos**, puede activar o desactivar el componente Protección frente a amenazas en archivos y seleccionar la acción que deberá realizar Kaspersky Endpoint Security cuando detecte un archivo infectado.

Activar Protección frente a amenazas en archivos

Esta casilla de verificación activa o desactiva Protección frente a amenazas en archivos.

Esta casilla está seleccionada de forma predeterminada.

Cobertura de protección

Al hacer clic en este botón, se abrirá una ventana donde puede crear la cobertura de protección.

Desinfectar o eliminar objetos maliciosos automáticamente

Kaspersky Endpoint Security bloquea el acceso al archivo infectado e intenta desinfectarlo sin solicitar la confirmación del usuario. Antes de realizar la desinfección, Kaspersky Endpoint Security guarda una copia de seguridad del archivo en el Depósito de copias de seguridad. Si se ha desinfectado el archivo, Kaspersky Endpoint Security lo guarda en su ubicación original con el nombre del archivo original. Si la desinfección falla, Kaspersky Endpoint Security mantiene el archivo infectado en un estado bloqueado en su ubicación original. En el informe **Objetos procesados**, se registra la información sobre la detección del objeto infectado.

Preguntar al usuario

Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el posible objeto malicioso que infectó el archivo y pregunta qué acción desea que lleve a cabo. Las acciones pueden variar en función del estado del objeto.

Esta casilla acción está seleccionada de forma predeterminada.

En la sección **Protección frente a amenazas web**, puede activar o desactivar el componente Protección frente a amenazas web y seleccionar la acción que realizará Kaspersky Endpoint Security al detectar objetos de tráfico web peligrosos.

Activar Protección frente a amenazas web

Esta casilla de verificación activa o desactiva Protección frente a amenazas web.

Esta casilla está seleccionada de forma predeterminada.

Bloquear automáticamente el tráfico web peligroso

Kaspersky Endpoint Security bloquea el acceso al sitio web donde se detectó un objeto de tráfico web peligroso sin solicitar confirmación.

Preguntar al usuario

Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el objeto de tráfico web peligroso detectado y le pide que elija la acción que desea que Kaspersky Endpoint Security lleve a cabo. Las acciones pueden variar en función del estado del objeto.

Esta casilla acción está seleccionada de forma predeterminada.

En la sección **Protección frente a amenazas en el correo**, puede activar o desactivar el componente Protección frente a amenazas en el correo y seleccionar la acción que deberá realizar Kaspersky Endpoint Security cuando detecte un archivo infectado.

Activar Protección frente a amenazas en el correo

Esta casilla de verificación activa o desactiva Protección frente a amenazas en el correo.

Esta casilla está seleccionada de forma predeterminada.

Eliminar objetos maliciosos de forma automática

Cuando Kaspersky Endpoint Security detecta un objeto infectado en un mensaje de correo electrónico, elimina el objeto infectado y reemplaza el contenido del objeto con el texto "The requested file infected with <nombre del virus> has been deleted".

Bloquear objetos maliciosos de forma automática

Cuando Kaspersky Endpoint Security detecta un objeto infectado en un mensaje de correo electrónico, reemplaza el asunto del mensaje de correo electrónico con "Message is infected: <asunto original>", donde <asunto original> es el asunto original. El asunto del mensaje de correo electrónico se reemplaza solo para el protocolo POP3.

En la sección **Protección frente a amenazas en la red**, puede activar o desactivar la protección contra los ataques de red.

Activar Protección frente a amenazas en la red

Esta casilla de verificación activa o desactiva Protección frente a amenazas en la red.

Esta casilla está seleccionada de forma predeterminada.

Ajustes

Al hacer clic en este botón, se abre una ventana en la que puede crear una lista de equipos de confianza o consultar y modificar la lista de equipos bloqueados.



Al hacer clic en este botón, se evita que los usuarios sin privilegios de administrador cambien la configuración de la aplicación de Kaspersky Endpoint Security.



Al hacer clic en este botón, se le solicitan las credenciales del administrador. Después de introducir las credenciales de administrador, la configuración de la aplicación se puede editar.

La ventana Cobertura de la protección

En la sección **Cobertura de protección**, puede visualizar y editar la cobertura de protección.

Todas los discos extraíbles

Esta casilla de verificación activa o desactiva en tiempo real la protección de todos los discos extraíbles.

Esta casilla está seleccionada de forma predeterminada.

Todos los discos internos

Esta casilla de verificación activa o desactiva en tiempo real la protección de todos los discos internos.

Esta casilla está seleccionada de forma predeterminada.

Todos los discos de red

Esta casilla de verificación activa o desactiva en tiempo real la protección de todos los discos de red.

Esta casilla está seleccionada de forma predeterminada.

+

Al hacer clic en este botón, se abre una lista donde puede seleccionar elementos para crear la cobertura de protección:

- **Archivos y carpetas**. Al seleccionar este archivo, se abre un cuadro de diálogo para agregar un archivo o una carpeta a la cobertura de protección.
- **Todos los discos**. Si selecciona este elemento, se añaden todos los discos extraíbles, internos y de red del equipo a la cobertura de protección.
- **Todas los discos extraíbles**. Si selecciona este elemento, se añaden todos los discos extraíbles del equipo a la cobertura de protección.
- **Todos los discos internos**. Si selecciona este elemento, se añaden todos los discos internos del equipo a la cobertura de la protección.
- **Todos los discos de red**. Si selecciona este elemento, se añaden todos los discos de red del equipo a la cobertura de la protección.
- **Memoria**. Si selecciona este elemento, se agrega la memoria del equipo a la cobertura de protección.
- **Objetos de inicio**. Si selecciona este elemento, se agregan a la cobertura de protección todos los archivos ejecutables que se iniciaron al poner en marcha el sistema operativo. El análisis de los objetos de inicio permite detectar rootkits.

La casilla de verificación que se encuentra junto al elemento de una lista activa o desactiva la protección en tiempo real de los objetos asociados a este elemento.

–

Al hacer clic en este botón, se elimina el elemento seleccionado de la lista de cobertura de protección.

No se pueden quitar los elementos incluidos en la lista de cobertura de protección de forma predeterminada.

En la sección **Optimización**, puede configurar si Kaspersky Endpoint Security analiza el volumen del sistema de solo lectura.

Omitir el análisis del volumen de sistema de solo lectura

Esta casilla de verificación activa o desactiva el análisis de volumen del sistema de solo lectura por parte de Kaspersky Endpoint Security.

Esta casilla está seleccionada de forma predeterminada.

Importante: Es posible que la optimización esté desactivada por motivos de seguridad.

La ventana “Configuración”

En la pestaña **Equipos de confianza**, puede crear una lista de equipos de confianza. La aplicación Kaspersky Endpoint Security no bloquea de manera automática las direcciones IP de estos equipos, ni siquiera cuando se detecta actividad de red peligrosa en estos.

La lista de equipos de confianza está vacía de forma predeterminada.

+

Al hacer clic en este botón, se agrega un campo para introducir la dirección IP de un equipo de confianza.

–

Al hacer clic en este botón, elimina la dirección IP seleccionada en la lista de equipos de confianza.

Editar

Al hacer clic en este botón, se puede editar la dirección IP seleccionada en la lista.

En la pestaña **Equipos bloqueados**, puede consultar y modificar la lista de equipos bloqueados.

La aplicación Kaspersky Endpoint Security bloquea el equipo con esta dirección IP durante una hora después de detectar una actividad de red peligrosa procedente de este equipo.

Dirección IP

Esta columna muestra la dirección IP del equipo bloqueado.

Hora del incidente

En esta columna se muestra la fecha y la hora en que se detectó la actividad de red peligrosa en el equipo.

Desbloquear

Al hacer clic en este botón, se elimina la dirección IP seleccionada de la lista de equipos bloqueados.

La pestaña “Análisis”

Lista de las tareas de análisis de software malicioso

Contiene tareas de análisis de software malicioso predefinidas:

- **Análisis completo**. Un análisis de software malicioso de la memoria del equipo, de los objetos de inicio y de todos los discos internos del equipo.
- **Análisis rápido**. Un análisis de software malicioso solamente de áreas críticas del equipo: memoria, objetos de inicio y carpetas de sistema.

- **Análisis personalizado**. Análisis de software malicioso de un objeto específico (archivo, carpeta, disco interno o extraíble).
- **Análisis de discos externos**. Un análisis de software malicioso de los discos externos que se realiza al conectar un disco externo al ordenador.

Nota: Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

En la sección **Cobertura del análisis**, puede consultar y editar la cobertura del análisis de la tarea de Análisis rápido.

Editar

Al hacer clic en este botón, se abre una ventana en la que podrá consultar y editar la cobertura del análisis.

Este botón solo aparece cuando se ha seleccionado la tarea de Análisis rápido en la lista.

En la sección **Acción**, puede seleccionar la acción que desea que Kaspersky Endpoint Security realice cuando se detecte un archivo infectado y programar una tarea.

Desinfectar o eliminar objetos maliciosos automáticamente

Kaspersky Endpoint Security bloquea el acceso al archivo infectado e intenta desinfectarlo sin solicitar la confirmación del usuario. Antes de realizar la desinfección, Kaspersky Endpoint Security guarda una copia de seguridad del archivo en el Depósito de copias de seguridad. Si se ha desinfectado el archivo, Kaspersky Endpoint Security lo guarda en su ubicación original con el nombre del archivo original. Si la desinfección falla, Kaspersky Endpoint Security mantiene el archivo infectado en un estado bloqueado en su ubicación original. En el informe **Objetos procesados**, se registra la información sobre la detección del objeto infectado.

Preguntar al usuario al terminar el análisis

Kaspersky Endpoint Security pospone el procesamiento de los archivos infectados que ha detectado hasta la finalización del análisis. Cuando se completa el análisis, Kaspersky Endpoint Security muestra ventanas de notificación que le informan de cada objeto infectado detectado y le ofrece la opción de elegir las acciones que desea realizar a continuación. Las acciones pueden variar en función del estado del objeto.

Esta casilla acción está seleccionada de forma predeterminada.

En la sección **Cuando un disco externo se conecta** en la pestaña **Análisis de discos externos**, puede seleccionar la acción que Kaspersky Endpoint Security debe realizar cuando se conecta un disco externo.

Análisis

Si se selecciona esta opción, Kaspersky Endpoint Security inicia una tarea de análisis de software malicioso para el disco externo conectado.

Esta opción está seleccionada de forma predeterminada.

No hacer nada

Si se selecciona esta opción, Kaspersky Endpoint Security no analiza el disco externo que se conecta.

En la sección **Optimización**, puede configurar si Kaspersky Endpoint Security analizará el volumen del sistema de solo lectura al realizar una tarea de Análisis rápido o Análisis completo.

Omitir el análisis del volumen de sistema de solo lectura

Esta casilla de verificación activa o desactiva el análisis de volumen del sistema de solo lectura por parte de Kaspersky Endpoint Security.

Esta casilla de verificación está seleccionada de forma predeterminada para una tarea de Análisis rápido y no está seleccionada de forma predeterminada para una tarea de Análisis completo.

Importante: Es posible que la optimización esté desactivada por motivos de seguridad.

Uso de CPU

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede activar o desactivar la limitación del uso de la CPU del dispositivo protegido por parte de la aplicación para tareas de análisis. Si se selecciona la opción **Limitar el uso de la CPU con análisis a**, puede especificar el uso máximo permitido de la CPU en el campo correspondiente.

Nota: Este es un límite acumulativo entre todos los núcleos de la CPU. El uso de la CPU que se muestra en Supervisión de actividad es el total del uso de cada núcleo de la CPU y, por lo tanto, puede superar el cien por ciento.

Activar esta opción puede afectar negativamente al rendimiento de Kaspersky Endpoint Security.

De manera predeterminada, esta opción está desactivada.

Planificar

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede planificar tareas de Análisis completo o Análisis rápido.



Al hacer clic en este botón, se evita que los usuarios sin privilegios de administrador cambien la configuración de la aplicación de Kaspersky Endpoint Security.



Al hacer clic en este botón, se le solicitan las credenciales del administrador. Después de introducir las credenciales de administrador, la configuración de la aplicación se puede editar.

La ventana “Cobertura del análisis”

En esta ventana, puede ver y editar la cobertura del análisis para la tarea de Análisis rápido.

La casilla de verificación situada al lado de un objeto en la lista habilita/deshabilita el análisis de ese objeto.

+

Al hacer clic en este botón, se abre una lista para ajustar la cobertura del análisis:

- **Archivos y carpetas**. Al seleccionar este archivo, se abre un cuadro de diálogo para agregar un archivo o una carpeta a la cobertura del análisis.
- **Todos los discos**. Si selecciona este elemento, se añaden todos los discos extraíbles, internos y de red del equipo a la cobertura del análisis.
- **Todos los discos externos**. Si selecciona este elemento, se añaden todos los discos extraíbles del equipo a la cobertura del análisis.
- **Todos los discos internos**. Si selecciona este elemento, se añaden todos los discos internos del equipo a la cobertura del análisis.
- **Todos los discos de red**. Si selecciona este elemento, se añaden todos los discos de red del equipo a la cobertura del análisis.
- **Memoria**. Si selecciona este elemento, se agrega la memoria del equipo a la cobertura del análisis.
- **Objetos de inicio**. Si selecciona este elemento, se agregan todos los archivos ejecutables que se iniciaron al poner en marcha el sistema operativo a la cobertura del análisis. El análisis de los objetos de inicio permite detectar rootkits.

–

Al hacer clic en este botón, se elimina el elemento seleccionado en la lista de cobertura del análisis.

No se pueden quitar los elementos incluidos en la lista de cobertura del análisis de forma predeterminada.

En la sección **Optimización**, puede configurar si la aplicación Kaspersky Endpoint Security analiza el volumen del sistema de solo lectura al realizar una tarea de Análisis rápido o Análisis completo.

Omitir el análisis del volumen de sistema de solo lectura

Esta casilla de verificación activa o desactiva el análisis del volumen del sistema de solo lectura por parte de Kaspersky Endpoint Security.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security omite el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security analizará el volumen del sistema de solo lectura.

Esta casilla de verificación está seleccionada de forma predeterminada.

> **Nota:** Kaspersky Endpoint Security no analiza los archivos que se encuentran en el almacenamiento de OneDrive o iCloud, u otros almacenamientos en la nube. Excluya estos archivos de la cobertura del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

La pestaña “Amenazas”

En la sección **Objetos a detectar** puede configurar la lista de objetos que han de ser detectados.

Virus, gusanos, programas troyanos, herramientas maliciosas, software publicitario y automarcadores

Esta categoría incluye los siguientes tipos de programas:

- Todos los tipos de software malicioso.
- Aplicaciones que muestran anuncios (como banners) en su equipo o sustituyen los resultados de búsqueda de su navegador por sitios web de publicidad.
- Aplicaciones que establecen conexiones telefónicas mediante un módem del equipo en modo oculto.

Kaspersky Endpoint Security siempre controla los programas de este tipo.

La casilla de verificación está siempre seleccionada y no se puede desmarcar.

Los intrusos pueden utilizar software legítimo para dañar su equipo o sus datos personales

Esta casilla de verificación activa o desactiva el control de aplicaciones legítimas que puede utilizar un intruso para dañar el equipo o los datos del usuario, como las aplicaciones remotas de administración.

Esta casilla está desmarcada de forma predeterminada.

En la sección **Copia de seguridad**, puede especificar el período máximo de almacenamiento de los objetos en el Depósito de copias de seguridad.

Eliminar copias de seguridad de los objetos luego de <número> días

Esta casilla de verificación activa o desactiva la eliminación de los objetos del Depósito de copias de seguridad una vez transcurrido el período de almacenamiento especificado.

Si se selecciona la casilla de verificación, la aplicación elimina los objetos del Depósito de copias de seguridad cuando finaliza el plazo especificado en el campo de número situado junto a la casilla de verificación. Si la casilla no está seleccionada, los objetos se almacenan en el Depósito de copias de seguridad de forma indefinida.

De forma predeterminada, esta casilla está seleccionada y los objetos se almacenan en el Depósito de copias de seguridad durante 30 días.

En la sección **Exclusiones**, puede crear una lista de archivos, carpetas, aplicaciones y sitios web en los que confíe y que no desee analizar en busca de software malicioso.

Zona de confianza

Al hacer clic en este botón, se abre una ventana donde puede editar una zona de confianza.

Nota: Cuando un administrador configura la directiva para prohibir la edición de la Zona de confianza, los usuarios no pueden acceder a los ajustes de la Zona de confianza.



Al hacer clic en este botón, se evita que los usuarios sin privilegios de administrador cambien la configuración de la aplicación de Kaspersky Endpoint Security.



Al hacer clic en este botón, se le solicitan las credenciales del administrador. Después de introducir las credenciales de administrador, la configuración de la aplicación se puede editar.

La ventana Configurar contraseña de administrador

Contraseña

Campo para introducir una contraseña que limita las acciones no deseadas en el dispositivo.

Confirmar contraseña

Campo para introducir la contraseña por segunda vez a fin de confirmarla.

Opciones

La lista de acciones que se pueden proteger con la contraseña. Seleccione las casillas necesarias para proteger las acciones correspondientes en el dispositivo. Debe seleccionar al menos una casilla.

Cancelar

Al hacer clic en este botón, se cierra la ventana sin guardar los cambios.

Aceptar

Al hacer clic en este botón, se guarda la configuración de la contraseña de administrador y se cierra la ventana. Una vez guardados los cambios, se le solicitará que introduzca la contraseña cuando intente realizar una acción no deseada en el dispositivo.

La ventana Ajustes de protección con contraseña

Contraseña

Campo para introducir una contraseña que limite las acciones no deseadas en los dispositivos de los usuarios.

Haga clic en **Mostrar** para ver los símbolos introducidos.

Confirmar contraseña

Campo para introducir una contraseña por segunda vez a fin de confirmarla.

Haga clic en **Mostrar** para ver los símbolos introducidos.

Solicitar contraseña para

La lista de acciones que se pueden proteger con la contraseña. Seleccione las casillas de verificación necesarias para proteger las acciones correspondientes en el dispositivo del usuario.

La pestaña Aplicaciones de confianza

En la pestaña **Aplicaciones de confianza**, puede crear una lista de aplicaciones que no desee que la aplicación Kaspersky Endpoint Security supervise.

De forma predeterminada, la lista de objetos de la Zona de confianza está vacía.

+

Si hace clic en este botón, se abre una ventana donde puede introducir la ruta a una aplicación, especificar su requisito de firma de código y elegir los tipos de actividad que Kaspersky Endpoint Security no supervisará.

–

Al hacer clic en este botón, se elimina la aplicación seleccionada de la Zona de confianza.

Editar

Al hacer clic en este botón, se abre una ventana donde puede editar los parámetros de la aplicación de confianza.

La ventana Añadir aplicación de confianza

Ruta

La ruta a una aplicación cuya actividad Kaspersky Endpoint Security no supervisará.

Nota: Los enlaces simbólicos no se pueden usar para especificar rutas en este campo.

Seleccionar

Al hacer clic en este botón, se abre una ventana en la que puede seleccionar una aplicación cuya actividad no se supervisará a través de Kaspersky Endpoint Security. En este caso, los valores de los campos **Ruta** y **Requisito de firma de código** se insertan automáticamente.

Requisito de firma de código

Requisitos para la firma del código de la aplicación cuya actividad Kaspersky Endpoint Security no supervisará.

Este es un parámetro opcional.

En la sección **Opciones**, puede seleccionar el tipo de actividad que no desea que la aplicación Kaspersky Endpoint Security supervise.

No supervisar la actividad de archivos

Esta casilla de verificación activa o desactiva la supervisión de las operaciones con archivos de una aplicación en un equipo cliente.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security no supervisa la actividad de archivos de la aplicación.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security supervisa la actividad de archivos de la aplicación.

Esta casilla de verificación está seleccionada de forma predeterminada.

No supervisar la actividad de red

Esta casilla activa o desactiva la supervisión del tráfico de Internet entrante y saliente en un equipo cliente.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security no supervisa la actividad de red de la aplicación.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security supervisa la actividad de red de la aplicación.

Esta casilla de verificación está seleccionada de forma predeterminada.

Cancelar

Al hacer clic en este botón, se cierra la ventana sin guardar los cambios.

Aceptar

Al hacer clic en este botón, se guardan los parámetros de la aplicación de confianza y se cierra la ventana.

Pestaña Archivos y carpetas de confianza

En la pestaña **Archivos y carpetas**, puede crear una lista de archivos y carpetas que no desee que la aplicación Kaspersky Endpoint Security supervise.

De forma predeterminada, la lista de objetos de la Zona de confianza está vacía.

+

Al hacer clic en este botón se abre un cuadro de diálogo para seleccionar un archivo o carpeta.

–

Al hacer clic en este botón, se elimina el objeto seleccionado de la Zona de confianza.

Pestaña Direcciones web de confianza

En la pestaña **Direcciones web**, puede crear una lista de direcciones web que no desee que la aplicación Kaspersky Endpoint Security supervise.

De forma predeterminada, la lista de objetos de la Zona de confianza está vacía.

+

Al hacer clic en este botón, se agrega un campo para introducir una dirección web.

Puede utilizar los siguientes símbolos cuando especifique la dirección del sitio web:

- El símbolo de asterisco (*) toma el lugar de cualquier conjunto de caracteres, excepto los caracteres \ y / .
- Dos símbolos de asterisco consecutivos (**) toman el lugar de cualquier conjunto de caracteres (incluido un conjunto vacío), incluidos los caracteres \ y / .
- El signo de interrogación (?) toma el lugar de cualquier carácter individual en el nombre del archivo o de la carpeta, excepto los caracteres \ y / .

–

Al hacer clic en este botón, se elimina la dirección web seleccionada de la Zona de confianza.

Pestaña Avanzado

En la sección **KSN**, puede leer los términos de la Declaración de Kaspersky Security Network y decidir si participar o no en Kaspersky Security Network.

Mostrar la Declaración de KSN

Al hacer clic en este botón, se abre una ventana que muestra el texto de la Declaración de Kaspersky Security Network.

Kaspersky Endpoint Security puede utilizar una infraestructura KSN global o privada. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security utiliza información sobre la reputación de los archivos, los recursos web y las aplicaciones recibidas de Kaspersky Security Network y proporciona los datos necesarios para que los servicios de detección funcionen en Kaspersky Security Network.

Participar en Kaspersky Security Network

Esta casilla de verificación activa o desactiva la participación en Kaspersky Security Network.

Participar en Kaspersky Private Security Network

Esta casilla de verificación activa o desactiva la participación en Kaspersky Private Security Network. Para obtener más información sobre la participación en Kaspersky Private Security Network, comuníquese con el administrador del sistema en su organización.

Activar modo KSN extendido

Esta casilla de verificación activa o desactiva la provisión de datos adicionales a Kaspersky Security Network para mejorar la protección de su equipo y la utilidad de Kaspersky Endpoint Security. Puede encontrar la lista de datos en la Declaración de Kaspersky Security Network y en la Ayuda de Kaspersky Endpoint Security.

Esta casilla de verificación se seleccionará automáticamente si se selecciona la casilla **Participar en Kaspersky Security Network**, pero no podrá desmarcarla.

Activar modo nube

El modo nube hace referencia al modo de funcionamiento de la aplicación en el que Kaspersky Endpoint Security usa una versión liviana de las bases de datos antimalware. Este modo solo está disponible si la participación en Kaspersky Security Network está activada. La versión liviana de las bases de datos antimalware permite usar aproximadamente la mitad de la memoria RAM del equipo que se usaría con las bases de datos completas. Si no participa en Kaspersky Security Network o si el modo nube está desactivado, Kaspersky Endpoint Security descarga la versión completa de las bases de datos antimalware desde los servidores de Kaspersky.

Si el botón de alternancia está activado, Kaspersky Endpoint Security usa la versión liviana de las bases de datos antimalware, lo que reduce la carga de los recursos del sistema operativo.

> **Nota:** Kaspersky Endpoint Security descarga la versión liviana de las bases de datos antimalware durante la siguiente actualización después de seleccionar la casilla.

Si el botón de alternancia está desactivado, Kaspersky Endpoint Security usa la versión completa de las bases de datos antimalware.

Nota: Kaspersky Endpoint Security descarga la versión completa de las bases de datos antimalware durante la siguiente actualización después de deseleccionar la casilla.

En la sección **Detección de comportamiento**, puede activar/desactivar el componente Detección de comportamiento y seleccionar una acción para realizar cuando se detecta actividad de software malicioso.

Activar Detección de comportamiento

Esta casilla activa/desactiva el componente Detección de comportamiento, que recibe información sobre las acciones de las aplicaciones en su ordenador y la proporciona a otros componentes de protección para mejorar su rendimiento.

Bloquear la actividad de software malicioso

Si se selecciona esta opción, Kaspersky Endpoint Security cierra una aplicación al detectar actividad maliciosa.

Eliminar objeto peligroso detectado

Si se selecciona esta opción, Kaspersky Endpoint Security elimina el archivo ejecutable de una aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad cuando se detecta actividad maliciosa.

Preguntar al usuario

Si se selecciona esta opción, cuando se detecta actividad de malware, la aplicación Kaspersky Endpoint Security muestra una ventana de notificación con información sobre el objeto malicioso y solicita al usuario que elija la acción que debe realizar la aplicación Kaspersky Endpoint Security. Las acciones disponibles pueden variar en función del estado del objeto.



Al hacer clic en este botón, se evita que los usuarios sin privilegios de administrador cambien la configuración de la aplicación de Kaspersky Endpoint Security.



Al hacer clic en este botón, se le solicitan las credenciales del administrador. Después de introducir las credenciales de administrador, la configuración de la aplicación se puede editar.

Pestaña Actualizar

En la sección **Bases de datos**, puede configurar el modo de las actualizaciones de la base de datos de Kaspersky Endpoint Security.

Descargar actualizaciones automáticamente

Esta casilla activa/desactiva actualizaciones automáticas de las bases de datos de la aplicación.

Esta casilla está seleccionada de forma predeterminada.

En la sección **Proxy**, puede configurar la utilización de un servidor proxy para actualizar Kaspersky Endpoint Security.

Utilizar servidor proxy

Esta casilla de verificación activa o desactiva la utilización de un servidor proxy para la conexión a Internet al efectuar la actualización de las bases de datos antimalware o de los módulos de aplicación.

Esta casilla está seleccionada de forma predeterminada.

Ajustes

Al hacer clic en este botón, se abrirá una ventana en la que podrá establecer la configuración de conexión del servidor proxy.

En la sección **Deshacer** puede volver a la versión anterior de las bases de datos de la aplicación. Puede ser necesario deshacer actualizaciones cuando la nueva versión de las bases de datos de la aplicación contiene una firma incorrecta que provoca que Kaspersky Endpoint Security bloquee una aplicación segura.

Deshacer actualización

Al hacer clic en este botón se deshace la actualización de las bases de datos de la aplicación.



Al hacer clic en este botón, se evita que los usuarios sin privilegios de administrador cambien la configuración de la aplicación de Kaspersky Endpoint Security.



Al hacer clic en este botón, se le solicitan las credenciales del administrador. Después de introducir las credenciales de administrador, la configuración de la aplicación se puede editar.

La ventana “Configuración del servidor proxy”

Usar ajustes de sistema para el servidor proxy

Kaspersky Endpoint Security utiliza la configuración del servidor proxy especificada en los ajustes del sistema de su Mac.

Esta casilla acción está seleccionada de forma predeterminada.

Usar ajustes específicos para el servidor proxy

Kaspersky Endpoint Security utiliza la configuración del servidor proxy especificada en esta ventana.

Dirección

Campo para introducir la dirección IP o el nombre de dominio de un servidor proxy.

Este campo está disponible si se selecciona la opción **Usar ajustes específicos para el servidor proxy**.

Puerto

Campo de entrada del número del puerto del servidor proxy utilizado para actualizar Kaspersky Endpoint Security.

Este campo está disponible si se selecciona la opción **Usar ajustes específicos para el servidor proxy**.

El valor predeterminado es 8080.

Usar autenticación

La *autenticación* es el proceso de comprobación de la conexión del nombre de usuario y la contraseña a un servidor proxy.

Esta casilla de verificación activa o desactiva la autenticación al conectarse a un servidor proxy.

Esta casilla está desmarcada de forma predeterminada.

Nombre de usuario

Campo para introducir el nombre de usuario de autenticación al conectarse al servidor proxy.

El campo está disponible si la casilla de verificación **Usar autenticación** está seleccionada.

Contraseña

Campo para introducir la contraseña de autenticación al conectarse al servidor proxy.

El campo está disponible si la casilla de verificación **Usar autenticación** está seleccionada.

Si no ha especificado el nombre de usuario y la contraseña, o si el servidor proxy rechaza el nombre de usuario y la contraseña introducidos, se abre una ventana donde debe introducir el nombre de usuario y la contraseña para autenticarse en el servidor proxy. Si la autenticación se realiza correctamente y la casilla de verificación **Recordar contraseña** de la ventana solicitada está seleccionada, el nombre de usuario y la contraseña que haya especificado se aplicarán siempre a partir de ese momento. Si no está seleccionada la casilla de verificación **Recordar contraseña** en la ventana de introducción del nombre de usuario y la contraseña, la próxima vez que se conecte al servidor proxy se le solicitará de nuevo el nombre de usuario y la contraseña.

Omitir servidor proxy con direcciones locales

Esta casilla activa o desactiva la utilización de un servidor proxy cuando se actualiza la aplicación desde una carpeta local o de red.

Esta casilla está seleccionada de forma predeterminada.

Pestaña Interfaz

En la sección **Notificaciones**, puede configurar las notificaciones sobre distintos eventos que desea recibir de Kaspersky Endpoint Security.

Activar notificaciones

Esta casilla de verificación activa o desactiva notificaciones sobre eventos de aplicación.

Esta casilla está seleccionada de forma predeterminada.

Activar sonidos de alerta cuando se detecte software malicioso

Esta casilla de verificación activa o desactiva las alertas de sonido cuando Kaspersky Endpoint Security detecta un objeto malicioso.

Esta casilla está seleccionada de forma predeterminada.

En la sección **Icono de aplicación** puede configurar que el icono de la aplicación se muestre en la barra de menús.

Mostrar en barra de menús

Esta casilla de verificación activa o desactiva que el icono de la aplicación se muestre en la barra de menús.

En la sección **Informes** puede activar o desactivar el registro de eventos no críticos en los informes de Kaspersky Endpoint Security.

Registrar eventos no críticos

Esta casilla activa/desactiva el registro de eventos informativos en informes. Como regla general, estos eventos no son importantes para la seguridad de su equipo.

En la sección **Seguimientos**, puede activar o desactivar el rastreo.

El rastreo es un modo de registrar información detallada sobre la actividad de la aplicación. Los especialistas del Servicio de soporte técnico de Kaspersky utilizan archivos de rastreo para solucionar problemas. Puede activar el registro de eventos de la aplicación para crear archivos de rastreo y enviarlos al Soporte técnico si los solicitan. De forma predeterminada, el registro de eventos de la aplicación está desactivado.

Importante: Active el rastreo solamente cuando el Servicio de soporte técnico se lo pida.

Activar rastreo

Esta casilla de verificación activa o desactiva la creación de archivos de rastreo.

Esta casilla no está seleccionada de forma predeterminada.

En la sección **Protección con contraseña**, puede activar la protección con contraseña de acciones no deseadas en su ordenador.

Activar la protección con contraseña

Esta casilla activa/desactiva la protección con contraseña de acciones no deseadas.

Esta casilla no está seleccionada de forma predeterminada.

Al seleccionar esta casilla, se abre una ventana en la que puede establecer y configurar la contraseña de administrador.

Ajustes

Al hacer clic en este botón, se abre una ventana en la que puede editar los parámetros de una contraseña de administrador.



Al hacer clic en este botón, se evita que los usuarios sin privilegios de administrador cambien la configuración de la aplicación de Kaspersky Endpoint Security.



Al hacer clic en este botón, se le solicitan las credenciales del administrador. Después de introducir las credenciales de administrador, la configuración de la aplicación se puede editar.

La ventana de ajustes de Protección frente a amenazas en el correo

Omitir los archivos más grandes que N MB

Si esta casilla de verificación está seleccionada, Protección frente a amenazas en el correo excluye del análisis los archivos adjuntos de los mensajes de correo electrónico si su tamaño supera el valor especificado.

Si esta casilla está desactivada, Protección frente a amenazas en el correo analiza los archivos comprimidos adjuntos en correos electrónicos de cualquier tamaño.

El valor predeterminado es 8 MB.

Esta casilla está seleccionada de forma predeterminada.

No comprobar archivos durante más de N s

Si esta casilla de verificación está seleccionada, el tiempo que se asigna para analizar los archivos comprimidos adjuntos de los mensajes de correo electrónico se limita al período especificado.

Si esta casilla de verificación está desactivada, el tiempo que se asigna para analizar los archivos comprimidos no está limitado.

El valor predeterminado es de 5 segundos.

Esta casilla está seleccionada de forma predeterminada.

La ventana Regla de paquetes de red

Nombre de la regla

Nombre de la regla de paquetes de red.

En la sección **Acción**, puede elegir la acción que realizará Kaspersky Endpoint Security cuando detecte la actividad de red.

En la sección **Protocolo**, puede especificar el protocolo al que se aplica la regla de red.

En la sección **Dirección**, puede especificar la dirección de la actividad de red que se supervisa.

En la sección **TTL**, puede especificar la vida útil de los paquetes de red que se supervisan.

En la sección **Adaptadores de red**, puede especificar los adaptadores de red a los que se aplica la regla de red.

En la sección **Dirección remota**, puede especificar las direcciones de red de los dispositivos remotos que pueden enviar y recibir paquetes de red.

En la sección **Dirección local**, puede especificar las direcciones de red local de los dispositivos que pueden enviar y recibir paquetes de red.

Registrar eventos

Esta casilla activa/desactiva el registro de eventos de Firewall.

Si se selecciona esta casilla de verificación, Kaspersky Endpoint Security registrará los eventos de Firewall en el informe.

Si no se selecciona esta casilla de verificación, Kaspersky Endpoint Security no registrará eventos de Firewall en el informe.

Esta casilla no está seleccionada de forma predeterminada.

La ventana Adaptador de red

Nombre del adaptador

El nombre del adaptador de red.

Tipo de interfaz

En esta lista desplegable, puede elegir el tipo de interfaz del adaptador de red.

Direcciones IP

La lista de direcciones IP.

Direcciones MAC

La lista de direcciones MAC.

La ventana Adaptadores de red

Nombre

Esta columna contiene el nombre del adaptador de red.

Tipo de interfaz

Esta columna contiene el tipo de interfaz del adaptador de red.

Direcciones IP

Esta columna contiene las direcciones IP del adaptador de red.

Direcciones MAC

Esta columna muestra la dirección MAC del adaptador de red.

La ventana Direcciones locales

Direcciones locales

Esta columna contiene las direcciones locales.

La ventana Dirección local

Tipo

Esta lista desplegable le permite especificar el tipo de entrada de IP local al que desea que se aplique la regla de red.

Dirección IP

Campo de entrada de la dirección IP. Este campo está disponible solo si selecciona **Dirección IP** en la lista desplegable **Tipo**.

Inicio del rango

Campo de entrada de inicio del rango de direcciones IP. Este campo está disponible solo si selecciona **Rango de direcciones IP** en la lista desplegable **Tipo**.

Final del rango

Campo de entrada de final del rango de direcciones IP. Este campo está disponible solo si selecciona **Rango de direcciones IP** en la lista desplegable **Tipo**.

La ventana Direcciones remotas

Direcciones remotas

Esta columna contiene las direcciones remotas.

La ventana Dirección remota

Tipo

Esta lista desplegable le permite especificar el tipo de entrada de dirección remota al que desea que se aplique la regla de red.

Dirección

Campo de entrada de dirección IP o nombre DNS. Este campo está disponible solo si selecciona **Dirección IP o nombre DNS** en la lista desplegable **Tipo**.

Inicio del rango

Campo de entrada de inicio del rango de direcciones IP. Este campo está disponible solo si selecciona **Rango de direcciones IP** en la lista desplegable **Tipo**.

Final del rango

Campo de entrada de final del rango de direcciones IP. Este campo está disponible solo si selecciona **Rango de direcciones IP** en la lista desplegable **Tipo**.

La ventana Plantillas

Plantillas de regla de red

Esta columna contiene las plantillas de regla de red.

La pestaña Regla de paquete de red

Servicio de red

Nombre de la regla de red.

Acción

Acción que debe realizar Firewall al detectar el tipo de actividad de red.

Dirección

Direcciones de red a las que se aplica la regla de red.

La pestaña Redes disponibles

Nombre

Esta columna contiene el nombre de la red.

Estado de red

Esta columna contiene el estado de red.

Dirección IP

Esta columna contiene las direcciones IP de la red.

La ventana Red disponible

Nombre de red

El nombre de la red.

Estado de red

La lista desplegable de estado de red.

Dirección IP

La dirección IP de la red.

La ventana Dirección MAC

Tipo

Esta lista desplegable le permite especificar el tipo de entrada de dirección MAC al que desea que se aplique la regla de red.

Dirección MAC

Campo de entrada de la dirección MAC. Este campo está disponible solo si selecciona **Dirección MAC** en la lista desplegable **Tipo**.

Máscara

Campo de entrada de la máscara de dirección MAC. Este campo está disponible solo si selecciona **Máscara de dirección MAC** en la lista desplegable **Tipo**.

Inicio del rango

Campo de entrada de inicio del rango de direcciones MAC. Este campo está disponible solo si selecciona **Rango de direcciones MAC** en la lista desplegable **Tipo**.

Final del rango

Campo de entrada de final del rango de direcciones MAC. Este campo está disponible solo si selecciona **Rango de direcciones MAC** en la lista desplegable **Tipo**.

El informe Eventos del sistema

El panel derecho de la ventana contiene un informe sobre el funcionamiento de Kaspersky Endpoint Security.

Hora

En esta columna, se muestra la fecha y la hora del evento.

Evento

En esta columna se muestra el estado del evento.

Nombre del programa

Esta columna muestra el nombre del programa en el que ocurrió el evento.

Usuario

Esta columna muestra el nombre del usuario que inició este evento.

Tipo de usuario

Esta columna muestra el tipo de usuario que inició este evento.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

Informe de Objetos procesados

En el panel derecho de la ventana se muestra la lista de todos los objetos infectados y objetos de tráfico web peligrosos detectados por la aplicación Kaspersky Endpoint Security.

Hora

Esta columna muestra el momento en que el objeto fue descubierto.

Objeto

En esta columna se muestra la ruta a la ubicación donde se detectó el objeto o la dirección web de este.

Estado

Esta columna muestra la acción que ha realizado la aplicación después de detectar el objeto.

Detectado

En esta columna se muestra el tipo de objeto detectado según la clasificación de la Enciclopedia de virus de Kaspersky.

Nombre

En esta columna se muestra el nombre del objeto detectado según la clasificación de la Enciclopedia de virus de Kaspersky.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Actualización de base de datos

El panel derecho de la ventana contiene informes sobre las tareas de actualización realizadas por la aplicación.

Iniciado

En esta columna, se muestra la fecha y la hora de inicio de cada tarea de actualización. Si se expande la lista de operaciones, esta columna también enumera las operaciones realizadas al actualizar la aplicación y la hora en que se realizaron.

Estado

En esta columna, se muestra el estado de una tarea de actualización.

Tamaño

En esta columna, se muestra el tamaño de los archivos de actualización descargados.

Velocidad promedio

En esta columna, se muestra la velocidad de descarga de los archivos de actualización.

Hora de finalización

En esta columna, se muestra la hora de finalización de una tarea de actualización.

Al hacer clic en este botón, se expande la lista de operaciones incluidas en la tarea de actualización.

Al hacer clic en este botón, se contrae la lista de operaciones incluidas en la tarea de actualización.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El Informe de Análisis

El panel derecho de la ventana contiene informes sobre tareas de análisis que realiza Kaspersky Endpoint Security.

Tarea

En esta columna, se muestra el nombre de una tarea de análisis.

Estado

En esta columna, se muestra el estado de una tarea de análisis o el estado de los objetos analizados.

Fecha

En esta columna, se muestran la fecha y hora de una tarea de análisis.

Iniciador

En esta columna, se muestra el usuario, la aplicación o el proceso que inició una tarea de análisis.

Al hacer clic en este botón, se amplía la lista de objetos analizados.

Al hacer clic en este botón, se contrae la lista de objetos analizados.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Protección frente a amenazas en archivos

El panel derecho de la ventana contiene un informe sobre el funcionamiento del componente Protección frente a amenazas en archivos.

Fecha

En esta columna se muestra la fecha y hora del acceso de la aplicación al objeto analizado.

Ruta

En esta columna se muestra la ruta a la ubicación original del objeto analizado.

Estado

En esta columna se muestra el estado de un objeto analizado.

Nombre del programa

En esta columna se muestra la aplicación que accedió al objeto analizado.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

Informe de Protección frente a amenazas web

El panel derecho de la ventana contiene un informe sobre el funcionamiento del componente Protección frente a amenazas web.

Fecha

Esta columna muestra la fecha y hora de detección de los objetos de tráfico web.

URL

En esta columna se muestran los objetos de tráfico de web que el componente Protección frente a amenazas web ha detectado. La columna especifica la dirección web donde se detectó cada objeto de tráfico web.

Estado

En esta columna se muestra el estado de los objetos de tráfico web detectados.

Nombre del programa

En esta columna se muestra el programa que accedió a los objetos de tráfico web detectados.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Protección frente a amenazas en el correo

El panel derecho de la ventana contiene un informe sobre el funcionamiento del componente Protección frente a amenazas en el correo.

Fecha

En esta columna se muestra la fecha y la hora en que se detectó un objeto infectado en el mensaje de correo electrónico.

Ruta

Esta columna muestra información sobre el mensaje de correo electrónico donde se detectó el objeto infectado.

Estado

En esta columna se muestran las medidas tomadas por Kaspersky Endpoint Security después de detectar un objeto infectado.

Nombre del programa

Esta columna muestra el nombre del cliente de correo electrónico.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

Informe de Protección frente a amenazas en la red

El panel derecho de la ventana contiene un informe sobre el funcionamiento de Protección frente a amenazas en la red.

Fecha

En esta columna se muestra la fecha y la hora en que se detectó la actividad de red peligrosa en el equipo.

Dirección IP

Esta columna muestra la dirección IP del equipo desde el que Kaspersky Endpoint Security ha detectado actividad de red peligrosa.

Estado

En esta columna se muestran las medidas tomadas por Kaspersky Endpoint Security después de detectar una actividad de red peligrosa.

Tipo de ataque

En esta columna se muestra el tipo de ataque de red detectado.

Puerto local

Esta columna muestra el número del puerto local a través del que se intentó cometer una intrusión.

Protocolo

En esta columna se muestra el tipo de protocolo empleado para cometer el ataque.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Endpoint Detection and Response

El panel derecho de la ventana contiene un informe sobre el funcionamiento del componente Endpoint Detection and Response.

Fecha

En esta columna, se muestra la fecha y hora de los eventos.

Evento

En esta columna se muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Firewall

El panel derecho de la ventana contiene un informe sobre el funcionamiento de Firewall.

Fecha

En esta columna, se muestra la fecha y hora de los eventos.

Evento

En esta columna se muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Prevención de exploits

El panel derecho de la ventana contiene un informe sobre el funcionamiento de Prevención de exploits.

Fecha

En esta columna, se muestra la fecha y hora de los eventos.

Evento

En esta columna se muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe de Control de dispositivos

El panel derecho de la ventana contiene un informe sobre el funcionamiento de Control de dispositivos.

Fecha

En esta columna, se muestra la fecha y hora de los eventos.

Evento

En esta columna se muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

El informe System Watcher

El panel derecho de la ventana contiene un informe sobre el funcionamiento del componente System Watcher.

Fecha

En esta columna, se muestra la fecha y hora de los eventos.

Evento

En esta columna se muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana en la que puede guardar el informe como un archivo TXT.

La ventana de soporte al usuario

Esta ventana incluye la siguiente información:

- Versión de Kaspersky Endpoint Security
- Fecha de lanzamiento de las bases de datos utilizadas actualmente por Kaspersky Endpoint Security
- Versión del sistema operativo instalado en el equipo

Servicio de soporte técnico

Al hacer clic en este botón, se abre la Base de conocimientos de Servicio de soporte técnico, donde encontrará artículos sobre Kaspersky Endpoint Security publicados por especialistas de Kaspersky.

Comunidad

Al hacer clic en este botón, se abre la comunidad donde puede debatir sobre Kaspersky Endpoint Security con los expertos de Kaspersky y otros usuarios.

Cerrar

Al hacer clic en este botón, se cierra la ventana de soporte del usuario.

La ventana Ajustes del certificado

En la pestaña **General**, puede seleccionar el almacenamiento del certificado para comprobar el tráfico HTTPS cifrado en el navegador Mozilla Firefox:

- **Llavero Raíz del sistema (recomendado)**
- **Ajustes de la tienda de certificados del navegador Mozilla Firefox**

  En este caso, debe añadir manualmente el certificado de Kaspersky Endpoint Security al almacenamiento de certificados del navegador Mozilla Firefox. Para obtener más información, consulte Cómo añadir el certificado de Kaspersky Endpoint Security al almacenamiento de certificados de Mozilla Firefox.

En la pestaña **Certificados de confianza**, puede crear una lista de certificados raíz de confianza para que se conecten a los servidores correspondientes sin emitir notificación.

La lista de certificados raíz de confianza está vacía de manera predeterminada.

+

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede añadir los certificados que se considerarán de confianza.

–

Al hacer clic en este botón, elimina el certificado seleccionado en la lista de equipos de confianza.

Nombre de certificado

La columna muestra los nombres de los certificados raíz de confianza.

Cancelar

Al hacer clic en este botón, se cierra la ventana sin guardar los cambios.

Guardar

Al hacer clic en este botón, se guarda la lista de certificados raíz de confianza actual y se cierra la ventana.

La ventana Comprobar certificado

Mostrar certificado

Al hacer clic en este botón, se abre una ventana de sistema con la información sobre el certificado.

Cancelar

Al hacer clic en este botón, se cierra la ventana.

Añadir a la lista de confianza

Al hacer clic en este botón, se añade el certificado a la lista de certificados de confianza. Como resultado, podrá conectarse al servidor correspondiente sin notificaciones.

Conectar

Al hacer clic en este botón, se conecta al servidor.

Nota: Los botones disponibles pueden variar según el tipo de certificado.

La ventana Seleccionar certificado

Lista de certificados disponibles

Seleccione la casilla junto a un certificado para utilizarlo al conectarse al servidor.

Mostrar certificado

Al hacer clic en este botón, se abre una ventana de sistema con la información sobre el certificado.

Cancelar

Al hacer clic en este botón, se cierra la ventana.

Continuar

Al hacer clic en este botón, se continúa conectando al servidor utilizando el certificado seleccionado.