kaspersky

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 de Kaspersky Security Center

Instalar y desinstalar la aplicación

- Kit de distribución
- Requisitos de hardware y software
- Preparativos para la instalación
- Instalación de Kaspersky Endpoint Security
- Preparación de la aplicación para su uso
- Desinstalación de Kaspersky Endpoint Security

Iniciar la aplicación por primera vez

Interfaz de la aplicación Kaspersky Endpoint Security

- Ventana principal de la aplicación
- Ícono de Kaspersky Endpoint Security
- Ventana de configuración 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
- Sobre el certificado de licencia
- Acerca de la clave
- Acerca del código de activación
- Acerca del archivo de claves
- Sobre la provisión de datos
- Activar Kaspersky Endpoint Security
- Ver información de licencia
- Administrar licencias y suscripciones
- Comparación de la funcionalidad de la aplicación según el tipo de licencia para estaciones de trabajo

Realizar las tareas más usuales

- Iniciar y cerrar la aplicación
- Ver el estado de la protección del equipo
- Ver el estado operativo de los componentes instalados
- Deshabilitar y reanudar la protección del equipo
- Usar el Centro de protección
- Realizar tareas de análisis
- Configurar el inicio automático de una tarea de análisis programado
- Actualizar las bases de datos de la aplicación
- Pasos a seguir si se bloquea el acceso a archivos
- Restaurar un objeto que ha sido eliminado o desinfectado por la aplicación
- Ver el informe de funcionamiento de la aplicación
- Qué se debe hacer si aparecen ventanas de notificaciones

Configuración avanzada de la aplicación
- Alcance de la protección del equipo
- Protección contra archivos peligrosos
- Protección contra amenazas web
- Protección contra amenazas de correo
- Protección contra amenazas de red
- Firewall
- Detección de comportamiento
- Análisis
- Tareas de actualización
- Tareas locales
  - Tarea Análisis de discos externos
- Copias de seguridad
- Informes
- Managed Detection and Response
- Endpoint Detection and Response Expert (on-premise)
- Endpoint Detection and Response Optimum
  - Integración con Endpoint Detection and Response Optimum
  - Análisis en busca de indicadores de peligro
  - Poner archivo en cuarentena
  - Obtener archivo
  - Eliminar archivo
  - Iniciar proceso
  - Finalizar proceso
  - Prevención de ejecución
  - Aislamiento de la red informática
  - Cloud Sandbox
- Cifrado de disco FileVault
- Protección con contraseña
- Prevención de exploits
- Motor de reparación
- Control Web
- Control de dispositivos

Participar en Kaspersky Security Network

Comprobar la integridad de los componentes de la aplicación

Administración de la aplicación a través de la Consola de administración de Kaspersky Security Center
- Implemente Kaspersky Endpoint Security en una red corporativa
- Actualice Kaspersky Endpoint Security versión 11.1 o posterior a la versión 12.2.1
- Prepárese para la instalación remota de Kaspersky Endpoint Security
  - Instale el complemento de administración de Kaspersky Endpoint Security
  - Instale el Agente de red localmente
  - Instale el Agente de red con Apple Remote Desktop
  - Instale el Agente de red con Kaspersky Security Center
  - Instale el Agente de red con el protocolo SSH
  - Desinstale el Agente de red localmente

- Administre el Agente de red desde la línea de comandos
  - Iniciar/detener el Agente de red en equipo remoto
  - Compruebe la conexión entre un equipo cliente y el Servidor de administración manualmente. Utilidad Klnagchk
  - Conecte un equipo remoto al Servidor de administración manualmente. Utilidad Klmover
  - Desinstalación del Agente de red
- Instalar y desinstalar Kaspersky Endpoint Security
  - Instale la aplicación con el protocolo SSH
  - Instale la aplicación con Kaspersky Security Center
  - Cree un paquete de instalación
  - Desinstale la aplicación con Kaspersky Security Center
- Inicie y detenga la aplicación a través de Kaspersky Security Center
- Cree y administre tareas
  - Crear tareas
  - Iniciar y detener tareas manualmente
  - Importar y exportar tareas
  - Ver tareas
  - Administrar configuraciones específicas de tareas
- Cree y administre políticas
  - Cree una directiva
  - Vea la lista de directivas
  - Edite la configuración de directivas
  - Cambie el estado de una directiva
  - Exporte una directiva a un archivo KLP
  - Importe una directiva desde un archivo KLP
- Cree y administre perfiles de directivas.
- Genere un informe sobre objetos detectados
- Obtener una clave de recuperación para una unidad cifrada

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

- Instale el complemento web de Kaspersky Endpoint Security
- Cree una directiva
  - Protección contra amenazas del host
    - Configurar el componente Protección contra amenazas de archivo
    - Configurar el Análisis de unidades extraíbles
    - Configurar la detección de comportamiento
    - Configurar Anti-Cryptor
    - Configuración del componente Prevención de exploits
    - Configuración del componente Motor de reparación
  - Comunicación y protección web
    - Configurar la protección contra amenazas de correo
    - Configurar el componente Protección contra amenazas web
    - Configurar la Protección contra amenazas de red
    - Configure el componente Firewall
  - Controles de seguridad
    - Configurar el componente Control de dispositivos
    - Configurar el componente Control web
  - Cifrado de datos

- Configuración general
  - Configuración de detección
  - Kaspersky Security Network
  - Interacción con el usuario
  - Autoprotección
  - Rendimiento
  - Informes y repositorios
  - Configuración de red
  - Configuración de telemetría
  - Configuración de eventos
  - Configuración de actualización
- Agentes incorporados
  - Configurar Managed Detection and Response
  - Configurar Endpoint Detection and Response
  - Configurar Endpoint Detection and Response Expert (on-premise)
- Crear tareas
  - Configuración de la tarea Analizar
  - Configuración de la tarea Agregar clave
  - Configuración de la tarea Actualizar
- 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 malware
- Actualizar la aplicación
- Revertir la última actualización
- Iniciar/detener un componente o tarea
- Ver estado y estadísticas de un componente o tarea
- Exportar la configuración de la protección
- Activar la aplicación
- Instalar la extensión del sistema
- Configurar las conexiones de red
- Eliminar claves de licencia
- Códigos de retorno 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 la red

Contactarse con el Soporte Técnico

- Cómo obtener soporte técnico
- Soporte técnico mediante Kaspersky CompanyAccount
- Obtener información para el Soporte técnico
- Usar un archivo de rastreo
- Crear un archivo de seguimiento

Fuentes de información sobre la aplicación

Apéndices
Problemas y limitaciones conocidas
Problemas solucionados
Lista de objetos analizados por extensión
Máscaras en rutas de archivos y carpetas
Requisitos del archivo de IOC
Intérpretes de scripts compatibles con Prevención de ejecución
Cómo agregar el certificado de Kaspersky Endpoint Security al almacenamiento de certificados de Mozilla Firefox
Configuración de red para la interacción con servicios externos
Información acerca de código de terceros
Avisos de marca registrada

Descripción general de Kaspersky Endpoint Security

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

Protección contra archivos peligrosos

La Protección contra archivos peligrosos protege el sistema de archivos del equipo en tiempo real, ya que intercepta y analiza los intentos de acceder a los archivos. Más información.

Protección contra amenazas web

La Protección frente a amenazas en la web protege la información que el equipo envía y recibe a través de los protocolos HTTP y HTTPS en Safari, Chrome™ y Firefox™. Más información.

Protección contra amenazas de correo

Protección contra amenazas de 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 equipo con la ayuda de bases de datos antimalware, el servicio en la nube de Kaspersky Security Network y el análisis heurístico. Más información.

Protección contra amenazas de red

La Protección contra amenazas de red evita intrusiones en el sistema operativo. Este componente lo protege contra atacantes informáticos (que usan el análisis de puertos y ataques de fuerza bruta) y el malware que instalan (incluido un tipo de malware que intenta enviar datos personales a los delincuentes). Más información.

Firewall

Firewall bloquea conexiones no autorizadas al equipo mientras se trabaja en Internet o en una red local. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. El componente proporciona protección al equipo 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 equipo y la proporciona a otros componentes de protección para mejorar su rendimiento. También realiza la acción seleccionada como respuesta a la actividad del malware. Más información.

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. Más información.

Motor de reparación

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

Análisis

La aplicación Kaspersky Endpoint Security detecta y neutraliza los malware y otras amenazas de seguridad informática bajo demanda en el alcance del análisis especificado. Kaspersky Endpoint Security puede ejecutar un análisis completo del equipo, un análisis rápido de las áreas críticas y un análisis con un alcance especificado. Más información.

Actualización

Kaspersky Endpoint Security actualiza las bases de datos y los módulos de la aplicación desde los servidores de actualizaciones de Kaspersky, los puntos de distribución u otras fuentes que su administrador del sistema especifique, y crea copias de seguridad de todos los archivos actualizados para permitir la reversión de la última actualización. Más información.

Copias de seguridad

Kaspersky Endpoint Security crea una copia de seguridad de los archivos infectados antes de intentar desinfectarlos o eliminarlos, lo que le permite restaurarlos. Más información.

Informes

Kaspersky Endpoint Security genera informes sobre eventos y acciones que involucran los componentes de la aplicación. Más información.

Notificaciones

Kaspersky Endpoint Security utiliza notificaciones para informarle sobre ciertos eventos en el funcionamiento de Kaspersky Endpoint Security. Las notificaciones pueden estar acompañadas de un sonido. Más información.

Centro de protección

Kaspersky Endpoint Security muestra mensajes del estado de la protección en el Centro de protección. El Centro de protección muestra información sobre el estado de protección del equipo y sobre cómo eliminar problemas o amenazas de seguridad. Más información.

Gestión remota de la aplicación a través de Kaspersky Security Center

Puede administrar de forma remota la protección de los equipos con Kaspersky Endpoint Security: reciba información sobre el estado actual de la protección de la computadora, solucione problemas de forma remota, responda a las amenazas de seguridad del equipo, habilite o deshabilite los componentes de protección (Protección contra archivos peligrosos, Protección contra amenazas web, Protección contra amenazas de red, Detección de comportamiento), habilite o deshabilite Control web, Managed Detection and Response y Endpoint Detection and Response Expert (on-premise), ejecute tareas de análisis, actualice bases de datos de las aplicaciones, ejecute el cifrado de disco de inicio y administre las 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 admitida por Kaspersky Endpoint Security depende de la herramienta de administración que use.

Cifrado de disco FileVault

Kaspersky Endpoint Security permite que el cifrado de FileVault se administre de forma remota. El cifrado evita que usuarios no autorizados accedan a datos confidenciales almacenados en el disco de inicio del equipo del usuario.

Control Web

Puede administrar de forma remota el acceso a los 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 su contenido. Más información.

Control de dispositivos

Control de dispositivos administra el acceso de los usuarios a los dispositivos que están instalados o conectados al equipo. Esto le permite proteger el equipo 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 proporciona interacción con el servicio de Managed Detection and Response de Kaspersky, que detecta y elimina constantemente 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 ante estas para contrarrestar ataques avanzados, que incluyen nuevos exploits, ransomware, ataques sin archivos, así como tácticas que emplean herramientas legítimas del sistema. Más información.

Endpoint Detection and Response Expert (on-premise)

El componente Endpoint Detection and Response Expert (on-premise) facilita la interacción con la solución Kaspersky Anti Targeted Attack Platform. Esta solución detecta con rapidez amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas, ataques de día cero y más. Más información.

Novedades de esta versión

Esta Ayuda se aplica a Kaspersky Endpoint Security for Mac versión 12.2.1.

Kaspersky Endpoint Security ofrece las siguientes funciones y mejoras nuevas:

- El nuevo macOS 27 Golden Gate ahora es compatible.
- Se actualizó la interfaz de administración de directiva en Web Console. Se modificó la estructura de secciones de la directiva para garantizar la coherencia con las interfaces de los complementos de Kaspersky Endpoint Security para Windows y Linux.
- Ahora es posible ver qué modificaciones se realizaron en una directiva durante un período determinado, así como guardar la información sobre dichas modificaciones en un archivo.
- Agregamos los nuevos componentes Protección contra amenazas de 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.
- Agregamos 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 de 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.
- Agregamos advertencias para acciones restringidas para la tarea Aislamiento de la red.
- Correcciones de errores generales y mejoras.

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

La funcionalidad admitida por Kaspersky Endpoint Security depende de la herramienta de administración que use (consulte la tabla a continuación).

Puede usar las siguientes herramientas para administrar Kaspersky Endpoint Security:

- Consola de administración de Kaspersky Security Center. Un complemento de Microsoft Management Console (MMC) que se instala 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 Web Console si utiliza un navegador en cualquier equipo que tenga acceso al Servidor de administración.
- Kaspersky Security Center Cloud Console. La versión de nube de Kaspersky Security Center.

Comparación de las características de Kaspersky Endpoint Security

Función	Kaspersky Security Center		
	Consola de la administración	Web Console	Cloud Console
Protección avanzada contra amenazas			
Kaspersky Security Network	✓	✓	✓
Detección de comportamiento	✓	✓	
Prevención de exploits	✓	✓	
Motor de reparación	✓	✓	
Protección básica contra amenazas			
Protección contra archivos peligrosos	✓	✓	✓
Protección contra amenazas web	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓
Protección contra amenazas de correo	✓	✓	
Firewall	✓	✓	
Controles de seguridad			
Control Web	✓	✓	✓
Control de dispositivos	✓	✓	
Cifrado de datos			
Cifrado de disco FileVault	✓	✓	✓
Clave de recuperación	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	
Endpoint Detection and Response Expert (on-premise)	✓	✓	✓
Tareas			

Función	Kaspersky Security Center		
	Consola de la administración	Web Console	Cloud Console
Agregar clave	✓	✓	✓
Actualización	✓	✓	✓
Análisis rápido	✓	✓	
Reversión	✓	✓	✓
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:

- Los archivos necesarios para instalar la aplicación utilizando cualquiera de los métodos disponibles.
- El archivo license_<loc>.txt con el Contrato de licencia de usuario final.

  El Contrato de licencia de usuario final especifica los términos de uso de la aplicación.

Descomprima el paquete de instalación para acceder a sus archivos.

Requisitos de hardware y software

Los siguientes son los requisitos de software y hardware de Kaspersky Endpoint Security:

- Tipo de procesador: Intel, Apple Silicon
- 4 GB de memoria (RAM)
- 5 GB de espacio libre en el disco duro
- macOS 14, 15, 26, 27
- Conexión de Internet

Navegadores compatibles:

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security no es compatible con las siguientes herramientas de virtualización:

- Parallels Desktop 16 para 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).

Puede administrar Kaspersky Endpoint Security de forma remota 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 12.2.1 a través de Kaspersky Security Center, debe instalar el Agente de red versión 15 en los equipos remotos.

Preparativos 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 comprimido KES_for_macOS11_and_later.zip del sitio web del Soporte técnico de Kaspersky y que 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 del 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 Soporte técnico.

Instalación de Kaspersky Endpoint Security

Importante: Los expertos de Kaspersky recomiendan instalar Kaspersky Endpoint Security solo como se indica en esta Ayuda.

Puede instalar Kaspersky Endpoint Security mediante alguno de los siguientes métodos:

- De forma local, desde el kit de distribución descargado del sitio web de Kaspersky.
- De forma remota, a través de Apple Remote Desktop
- De forma remota, a través de la Consola de administración de Kaspersky Security Center.
- De forma remota, a través de Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

  Para obtener información detallada sobre la implementación de las aplicaciones de Kaspersky con Kaspersky Security Center Web Console, consulte la Ayuda de Kaspersky Security Center. Para obtener información detallada sobre la implementación de las aplicaciones de Kaspersky con Kaspersky Security Center Cloud Console, consulte la Ayuda de Kaspersky Security Center Cloud Console.

Realizar una instalación estándar de Kaspersky Endpoint Security

1. Descomprima el archivo ZIP del kit de distribución.
2. Abra el archivo .dmg 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 termina la instalación, 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 Expert (on-premise), Endpoint Detection and Response (Optimum) y Cloud Sandbox.

Realizar una instalación personalizada de Kaspersky Endpoint Security

1. Descomprima el archivo ZIP del kit de distribución.
2. Abra el archivo .dmg 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 que se encuentran 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 termina la instalación, Kaspersky Endpoint Security se inicia automáticamente. No es necesario reiniciar el equipo.

Instalación de Kaspersky Endpoint Security de forma remota con Apple Remote Desktop

1. En la Mac, elija el **menú Apple** > **Configuración del sistema** > **General** > **Compartir**.
2. Seleccione la casilla **Administración remota**.
3. En otra Mac que desee usar como servidor, instale Apple Remote Desktop. Para obtener más información sobre Apple Remote Desktop, consulte el Soporte técnico de Apple.
4. Abra Apple Remote Desktop.
5. En la ventana de **Remote Desktop**, haga clic en **Escáner** a la izquierda y seleccione los dispositivos en los que desea instalar Kaspersky Endpoint Security.
6. Haga clic en **Instalar**.
7. Cuando se le soliciten las credenciales de administrador, ingrese un nombre de administrador y una contraseña, y haga clic en **Agregar**.

8. Haga clic en + y seleccione el archivo .dmg que tiene el paquete de instalación de Kaspersky Endpoint Security.
9. Haga clic en **Instalar**.

La instalación de Kaspersky Endpoint Security comienza en los dispositivos seleccionados.

Preparación de la aplicación para su uso

Después de instalar Kaspersky Endpoint Security, puede hacer lo siguiente:

- Active 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 malware y enviar solicitudes al Soporte técnico.

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

  Si el componente Endpoint Detection and Response no es compatible con su licencia actual, debe activar Kaspersky Endpoint Detection and Response por separado.

- Evalúe el estado de la protección del equipo.
- Actualice Kaspersky Endpoint Security.
- Analizar el equipo en busca de malware.

Desinstalación de 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 desinstalador de Kaspersky Endpoint Security.
3. En la ventana del desinstalador, haga clic en **Desinstalar**.
4. Cuando se le soliciten las credenciales de administrador, escriba el nombre y la contraseña del administrador y confirme que desea desinstalar Kaspersky Endpoint Security.

   Comienza la desinstalación de Kaspersky Endpoint Security.
5. Lea la información sobre la conclusión del proceso de desinstalación y haga clic en **Salir** para salir del desinstalador.

Kaspersky Endpoint Security ahora está desinstalado de su equipo. No es necesario reiniciar el equipo tras desinstalar la aplicación.

Iniciar la aplicación por primera vez

Kaspersky Endpoint Security se inicia en su equipo inmediatamente 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 malware, ataques de red y amenazas de Internet.

  Para obtener más información sobre los permisos que está otorgando, haga clic en ?.

- Active 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 asegurarse de que Protección contra archivos peligrosos y Protección contra 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 hacer esto, 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 le puedan hacer daño a la Mac, instale la extensión del sistema. Para hacer esto, haga clic en **Instalar** junto al elemento **Extensión del sistema** y siga las instrucciones en pantalla.

   - Si desea que la extensión del sistema funcione correctamente, permita el filtrado de contenido de la red. Para hacerlo, haga clic en **Permitir** junto al elemento **Filtrado de contenido de la red** y siga las instrucciones en pantalla.

   - Si desea que Kaspersky Endpoint Security busque malware 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 ícono de la aplicación y elija **Kaspersky Endpoint Security**.

La ventana principal de la aplicación de Kaspersky Endpoint Security contiene elementos de la interfaz que brindan 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:

Supervisar	Haga clic para abrir la página **Supervisar** que proporciona información sobre lo que Kaspersky Endpoint Security hace 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.
Actualización	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 de **Supervisar**

La página de **Supervisar** muestra el indicador de estado de la 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 sobre problemas de protección del equipo. Más información.
Informes	Le permite ver los eventos que ocurrieron durante el funcionamiento de la aplicación, los componentes individuales y las tareas. Más información.
Copia de seguridad	Le permite ver una lista de copias guardadas de archivos infectados que la aplicación eliminó. 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.

Ícono de Kaspersky Endpoint Security

Tan pronto como se instala Kaspersky Endpoint Security, el ícono de Kaspersky Endpoint Security aparece en la barra de menús. Cuando se activa la aplicación, el ícono de la aplicación muestra su estado. Si el ícono de la aplicación está activo ( ), significa que todos o algunos de los componentes de protección están habilitados. Si el ícono de la aplicación está inactivo ( ), significa que todos los componentes de protección están deshabilitados.

Abrir el menú del ícono de la aplicación

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

Por defecto, el ícono de la aplicación siempre está presente en la barra de menús. Puede eliminar el ícono de la aplicación de la barra de menús.

Eliminar la aplicación que se encuentra en la barra de menús

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección del **Ícono de la aplicación**, desmarque la casilla **Mostrar en la barra de menús**.

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

A través del menú del ícono de la aplicación, puede acceder a la ventana principal de la aplicación y realizar las siguientes acciones:

- Deshabilitar la protección del equipo.
- Reanudar la protección del equipo.
- Abrir el Centro de protección.
- Iniciar análisis rápido.
- Ejecutar una actualización.
- Abrir la ventana de configuración de la aplicación.
- Salga de Kaspersky Endpoint Security.

Ventana de configuración de la aplicación

Abrir la ventana de configuración de la aplicación

Realice una de las siguientes acciones:

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

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

- **Esencial**. En esta pestaña, puede habilitar o deshabilitar la protección del equipo y configurar las opciones de Protección contra archivos peligrosos, Protección contra amenazas web y Protección contra amenazas de red.
- **Análisis**. En esta pestaña, puede establecer la configuración de las tareas de análisis y el inicio programado de las tareas de análisis.
- **Amenazas**. En esta pestaña, puede seleccionar las categorías de objetos a detectar, crear la Zona de confianza y establecer la configuración del Depósito de copias de seguridad.
- **Avanzado**. En esta pestaña, puede unirse o dejar de participar en Kaspersky Security Network.
- **Actualización**. En esta pestaña, puede configurar las opciones 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 ícono de Kaspersky Endpoint Security, las notificaciones y los informes, y habilitar o deshabilitar el registro de información de depuración en un archivo de rastreo.

Con el botón , puede bloquear a los usuarios sin derechos de administrador para que no puedan editar la configuración de Kaspersky Endpoint Security. Este botón se encuentra en la parte inferior de la ventana de configuración de la aplicación. Para editar la configuración, debe ingresar las credenciales del administrador.

Al hacer clic en el botón ?, se abre la Ayuda de Kaspersky Endpoint Security, que describe toda la configuración de la ventana de la aplicación actual. También puede abrir el tema de ayuda para la ventana activa de la aplicación al seleccionar Abrir la Ayuda de esta ventana en el menú **Ayuda**.

Acerca de las notificaciones

Kaspersky Endpoint Security muestra notificaciones para informarle sobre eventos de aplicaciones. Según la versión del sistema operativo instalado en el equipo, las notificaciones aparecen en el Centro de notificaciones del sistema operativo. La apariencia de las notificaciones depende de las opciones establecidas en la configuración de notificaciones del sistema operativo.

En Kaspersky Endpoint Security, los eventos 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. Recomendamos que no deshabilite 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.

- *Informativo*: eventos informados para su información.

Deshabilitar notificaciones

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Notificaciones**, desmarque la casilla **Habilitar notificaciones**.

Habilitar el registro de eventos no críticos

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

   Se abre la ventana de configuración 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 habilitadas o deshabilitadas, los informes de la aplicación contienen información sobre los eventos que ocurren mientras se ejecuta Kaspersky Endpoint Security.

Las notificaciones pueden ir acompañadas de sonido (por ejemplo, notificaciones sobre un malware detectado). Puede deshabilitar la alerta sonora.

El registro de eventos no críticos aumenta considerablemente el tamaño total del archivo de informe. Tenga en cuenta que esta configuración se aplica solo a la Protección contra archivos peligrosos.

Deshabilitar las alertas de sonido que acompañan a las notificaciones

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Notificaciones**, desmarque la casilla **Activar los sonidos de alerta al detectar malware**.

Si se requiere una acción en respuesta a un evento, Kaspersky Endpoint Security muestra una ventana de notificación. Por ejemplo, cuando la aplicación detecta un objeto malicioso, le pregunta si desea eliminarlo o desinfectarlo. La ventana de notificación desaparece de la pantalla solo después de seleccionar 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 los términos de uso de la aplicación.

Importante: lea detenidamente el Contrato de licencia antes de empezar a usar la aplicación.

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

- Durante la instalación de Kaspersky Endpoint Security
- Leer el documento license.txt que se encuentra en la carpeta de instalación de la 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 utilice la aplicación.

Acerca de la licencia

Una *licencia* es un derecho de uso de Kaspersky Endpoint Security durante un tiempo limitado, concedido bajo los términos del Contrato de licencia firmado (Contrato de licencia de usuario final).

El alcance de los servicios y el período de validez dependen de la licencia que se usa para la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *De prueba*. Una licencia gratuita destinada a probar la aplicación.

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

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

- *Comercial*. Una licencia de pago.

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

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

Acerca de la suscripción

La *suscripción a Kaspersky Endpoint Security* constituye una orden de compra de la aplicación con parámetros específicos (fecha de vencimiento, cantidad de dispositivos protegidos). Puede solicitar una suscripción a Kaspersky Endpoint Security a su proveedor de servicios (como su proveedor de servicios de Internet, o ISP). Puede administrar la suscripción en el área para miembros en el sitio web del proveedor de servicios. Por ejemplo, puede renovar o cancelar su suscripción, reducir su plazo o cambiar la cantidad de dispositivos protegidos bajo su suscripción.

La suscripción puede ser limitada (tener un límite de un año, por ejemplo) o ilimitada (sin fecha de caducidad). Para mantener Kaspersky Endpoint Security activo tras el vencimiento del plazo de suscripción limitada, debe renovar la suscripción de forma manual. La suscripción ilimitada se renueva automáticamente siempre y cuando le haya pagado al proveedor de servicios de antemano.

Si usa la aplicación con una suscripción limitada, al caducar la suscripción recibirá un período de gracia para renovarla. Durante ese período, la aplicación continúa funcionando.

Una vez que caduca su suscripción de actualizaciones y después de que finaliza el período de gracia para la renovación de la suscripción, Kaspersky Endpoint Security sigue funcionando, pero deja de actualizar las bases de datos de la aplicación.

Después de que caduque su suscripción a actualizaciones y protección y después de que finalice el período de gracia para la renovación de la suscripción, Kaspersky Endpoint Security deja de proteger su equipo.

Para utilizar Kaspersky Endpoint Security con suscripción, debe agregar el código de activación que recibió por parte del proveedor de servicios. Cuando se usa la aplicación con una suscripción, no es posible renovar la licencia con un código de activación diferente. Es posible utilizar un código de activación diferente solo después de que caducó la suscripción o si la cancela. Para cancelar la suscripción, debe comunicarse con el proveedor de servicios que le vendió Kaspersky Endpoint Security.

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

Si ya usa Kaspersky Endpoint Security con una licencia válida, pero desea usarla con una suscripción, elimine la clave activa actual para poder activar la aplicación con una clave de suscripción. Se puede usar en otro equipo el código de activación que se utilizó anteriormente para activar la aplicación en este equipo.

Nota: las opciones de suscripción disponibles pueden variar según el proveedor de servicios. También es posible que algunos proveedores decidan no conceder un período de gracia para renovar la suscripción.

Sobre el 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 otorgado la licencia
- Información de la aplicación que se puede activar con la licencia
- Límite del número de unidades con licencia (p. ej., dispositivos en los cuales se puede usar la aplicación con la licencia)
- Fecha de inicio de validez de la licencia
- Fecha de caducidad de la licencia o plazo de licencia
- Tipo de licencia

Acerca de la clave

Una *clave* es una secuencia de bits que puede aplicar para activar y luego utilizar la aplicación de acuerdo con los términos del Contrato de licencia de usuario final. Las claves son generadas por especialistas de Kaspersky.

Puede agregar una clave a la aplicación a través de uno de los siguientes métodos: la aplicación de un *archivo de claves* o el ingreso de un *código de activación*. Una vez que la agrega a la aplicación, la clave se muestra en la interfaz como una secuencia alfanumérica exclusiva.

Kaspersky puede bloquear la clave si se infringen los términos del Contrato de licencia. En ese caso, debe agregar otra clave para usar la aplicación.

La clave puede estar activa o ser de reserva.

Una *clave activa* es una clave que la aplicación utiliza actualmente. Se puede agregar una clave activa para una licencia de prueba o comercial, o una suscripción. La aplicación no puede tener más de una clave activa.

La *clave de reserva* confirma el permiso para usar la aplicación aunque no esté actualmente en uso. Una clave de reserva se convierte en activa automáticamente cuando caduca la licencia asociada con la clave activa actual. Una clave de reserva puede agregarse solo si ya se ha agregado una clave activa.

Una clave de licencia de prueba se puede agregar como clave activa. Una clave para una 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 ingresar un código de activación para agregar una clave de licencia para activar Kaspersky Endpoint Security. Recibirá el código de activación en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Endpoint Security o solicitó su versión de prueba.

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

Si perdió su código de activación después de instalar la aplicación, comuníquese 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 de claves están diseñados para activar la aplicación agregando una clave de licencia.

Recibirá un archivo de claves en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Endpoint Security o solicitó su versión de prueba.

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

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

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

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

Sobre la provisión de datos

Contrato de licencia de usuario final

Al activar Kaspersky Endpoint Security mediante el código de activación, a fin 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 proporcionar automáticamente la siguiente información durante el uso de Kaspersky Endpoint Security:

- El tipo, la versión y la localización del software instalado.
- Las versiones de las actualizaciones instaladas.
- El identificador del equipo y de la instalación del software en el equipo.
- El código de activación y el identificador de activación único para la licencia actual.
- El tipo, la versión y el tamaño de palabra del sistema operativo.
- El nombre del entorno virtual cuando el software se instala en uno.
- Los identificadores de los componentes del software que están activos en el momento en que proporciona la información.
- El origen de datos admitido.
- Tiempo de espera.

- Fecha y hora en el equipo del usuario.
- Versión del protocolo.
- Tipo de contenido del protocolo.
- Longitud del contenido del protocolo.
- El tipo de compresión de datos utilizado.
- El tipo de firma en el recibo de activación.
- Identificador del centro de activación regional.
- Hash del código de activación calculado usando el algoritmo SHA1.
- Hash del cuerpo del recibo calculado usando el algoritmo SHA1.
- Fecha y hora de creación del recibo de la licencia.
- Identificador de activación de la licencia.
- Identificador del recibo de la licencia actual.
- Identificador de la secuencia del recibo de la licencia.
- Fecha y hora de activación de la licencia.
- Fecha y hora de caducidad de la licencia.
- Estado de la licencia.
- Versión de la licencia.
- El identificador único del equipo del usuario.
- Versión del encabezado del recibo de la licencia.
- Nombre de la aplicación.
- Tipo de los datos transferidos.
- Versión del esquema de los datos transferidos.
- La versión completa del sistema operativo.
- Descripción de la máquina virtual utilizada.
- Lista de los ID para aplicaciones compatibles.

Cuando utiliza los servidores de actualizaciones de Kaspersky para descargar las actualizaciones, con el fin de aumentar la eficacia del procedimiento de actualización, acepta brindar periódicamente la información siguiente para la identificación de la aplicación durante las actualizaciones de las bases de datos y los módulos:

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

Declaración de Kaspersky Security Network (KSN)

Es posible que el uso de KSN aumente la velocidad de reacción del Software ante las amenazas de seguridad de la red y la información. Este propósito se logra mediante las siguientes acciones:

- La determinación de la reputación de los objetos analizados.
- La detección de amenazas de seguridad informática que son nuevas y difíciles de detectar, y sus fuentes.
- La toma de medidas rápidas para aumentar la protección de los datos almacenados y procesados por un usuario con el equipo.
- La reducción de posibles falsos positivos.
- El aumento del rendimiento de los componentes de la aplicación.
- La investigación del tipo de infección del equipo de un usuario.
- La mejora del rendimiento de los productos de Kaspersky.
- La recepción de información de referencia sobre la cantidad de objetos con reputación conocida.
- La rápida detección y corrección de los errores relacionados con la instalación, eliminación y actualización del producto.

Durante el uso de KSN, Kaspersky recibirá y procesará automáticamente los 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 entre 1 y 4 nodos, Kaspersky recibirá y procesará automáticamente los siguientes datos durante el uso de Kaspersky Security Network:

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

- Versión completa del Software instalado; tipo del Software instalado; identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador único del dispositivo; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

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 acerca de la versión del sistema operativo (SO) y los paquetes de servicio instalados en la computadora, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo de kernel del SO, y los parámetros del modo de ejecución del SO; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada de 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 del procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactivo; cantidad de eventos de acción procesados del SO; 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 del procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento del evento recurrente; 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 de una acción en el SO.

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

- Información acerca de la aplicación del Titular de los derechos que se instaló y acerca del estado de protección antivirus: identificador de la instalación (PCID) del software; 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 del Software instalado; identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); 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; identificador de actualización del Software; tipo del Software instalado; fecha y hora de inicio de la Vigía proactiva; fecha y hora de instalación del software; probabilidad de que la Vigía proactiva envíe estadísticas; código del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo máximo permitido para el procesamiento de un evento por parte de la Vigía proactiva; tiempo de procesamiento del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por la Vigía proactiva.

- Información sobre todos los objetos y operaciones analizados: veredicto del software sobre el 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 la Vigía proactiva; fecha y hora de detección de software por la Vigía proactiva; características de detección; identificador del registro desencadenado en las bases de datos antivirus del software; motivo por el que la Vigía proactiva detectó el software; 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 desencadenado de las bases de datos antivirus del software; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; las direcciones URL y del referido desde las que se descargó; el tamaño de los archivos analizados y la ruta 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 empacador (si se empacó el archivo); 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 valor de la suma de control complementaria del objeto; datos acerca de la firma digital del objeto (certificado): 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 de firma del archivo; el nombre, el tipo, el tipo de identificador, la suma de comprobación (MD5) y el tamaño de la aplicación que cargó el objeto que se está validando; la ruta de la aplicación y las rutas de las plantillas; un atributo que indique la presencia en la Lista de ejecución automática; la fecha de entrada; la lista de atributos; el nombre del empaquetador; la información acerca de la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME, la fecha y la 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 empaquetador (si el archivo estaba empaquetado), 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 inició 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 del solicitud 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 empaquetadores (si se empaquetó el archivo); la información sobre la disponibilidad y validez de estas estadísticas; el identificador del modo para generar las estadísticas que se envían.

- Si se detectan amenazas o vulnerabilidades, además de la información sobre el objeto detectado, se proporciona información sobre el identificador, la versión y el tipo de registro en la base de datos antivirus, el nombre de la amenaza según la clasificación de Kaspersky, la fecha y hora de la última actualización de la base de datos antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de la aplicación que solicitó la URL donde se detectó la amenaza, la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador de vulnerabilidad y su nivel de amenaza, la URL y el referente de la página web donde se detectó la vulnerabilidad.

- Si se detecta un posible objeto malicioso, la información acerca de los datos se proveerá en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo atacante y número del puerto en la computadora del usuario al que ataca la red, identificador del protocolo de ataque, nombre y tipo de ataque.

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

- Las direcciones URL e IP de la página web en la que se detectó contenido dañino o sospechoso; el nombre, el tamaño y la suma de comprobación del archivo que solicitó la dirección URL; el identificador, el peso y el grado de la regla utilizada para llegar a un veredicto, el objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: estado de terminación de la tarea de actualización, tipo de error que puede ocurrir durante el proceso de actualización, cantidad de actualizaciones con errores, identificador del componente de la aplicación que realiza actualizaciones.

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

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se detectó el evento, tipo y categoría del evento, nombre del origen del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la que se solicita la reputación y la referencia, el 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 analizado (MD5), el tipo de amenaza detectada, la información sobre el registro usado para detectar una amenaza (el identificador de registro para la base de datos del antivirus y el tipo y la marca de tiempo del registro); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

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

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

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

- Información sobre el dispositivo: ID de dispositivo.

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

Además, a fin de conseguir el objetivo declarado de aumentar la eficacia de la protección proporcionada por la aplicación, Kaspersky puede recibir objetos que los intrusos podrían aprovechar para dañar el equipo y crear amenazas de seguridad informática. Estos objetos son los siguientes:

- Archivos ejecutables o no ejecutables o partes de ellos.

- Las áreas de la RAM del equipo.

- Sectores involucrados en el proceso de arranque del SO.

- Paquetes de datos del tráfico de red.

- Páginas web y correos electrónicos que contienen objetos maliciosos o sospechosos.

- Descripción de clases e instancias de la clase para el almacenamiento de WMI.

- Informes de actividad de la aplicación.

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

- Nombre, tamaño y versión del archivo que se envía, descripción y sumas de control (MD5, SHA2-256, SHA1), ID del formato, nombre del fabricante, nombre de la aplicación a la que pertenece el archivo, la ruta totalmente calificada al archivo en el equipo y el código de la plantilla de la ruta, fecha y hora de creación del archivo y actualización.

- Fecha y hora de inicio y finalización de la validez del certificado si el archivo que se envía 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 algoritmos usados para calcularlos, número de serie del certificado.
- Nombre de la cuenta que había ejecutado el proceso.
- Sumas de comprobación (MD5, SHA2-256, SHA1) para el nombre del equipo que está ejecutando el proceso.
- Encabezados de las ventanas del proceso.
- ID para las bases de datos de antivirus, nombre de la amenaza identificada según la clasificación de Kaspersky.
- Información sobre la licencia utilizada para la aplicación, ID de la licencia, tipo y la fecha de vencimiento.
- Hora local del equipo al momento en que se proporcionó la información.
- Los nombres y las rutas de los archivos a los que accedió el proceso.
- Las direcciones URL e IP a las que accedió el proceso.
- Las direcciones URL e IP desde las que se descargó el archivo en ejecución.

Además, a fin de alcanzar el propósito declarado de evitar falsos positivos, es posible que el Titular del Derecho reciba archivos de confianza, ejecutables y no ejecutables, o bien fragmentos de estos.

Leer la Declaración de Kaspersky Security Network

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Avanzado**, haga clic en **Mostrar la Declaración de KSN**.

Kaspersky Endpoint Security guarda la siguiente información en los archivos de rastreo:

- Información sobre el dispositivo y el sistema operativo (ID único del dispositivo, tipo de dispositivo, direcciones MAC de dispositivos de red, tipo de sistema operativo, versión del sistema operativo).
- Información sobre el funcionamiento de la aplicación y sus módulos.
- Información sobre la suscripción (tipo de suscripción, región).
- Información sobre la configuración regional del idioma, ID de aplicación, personalización de la aplicación, versión de la aplicación, ID único de instalación de la aplicación, ID único del equipo.
- Información sobre el estado de protección contra malware de la computadora y la totalidad de objetos detectados y procesados (nombre del objeto detectado, fecha y la hora de la detección, dirección web desde la que se lo descargó, nombres, tamaños y rutas de los archivos infectados, dirección IP del equipo atacante y número de puerto del equipo al que estuvo dirigido el ataque de red, lista de actividades realizadas por el malware y direcciones web no deseadas). También se informará sobre las decisiones y las medidas pertinentes que hayan tomado la aplicación y el usuario.
- Información sobre las aplicaciones descargadas por el usuario (direcciones web, atributos, tamaño de los archivos, información sobre los procesos que descargaron los archivos).

- Información sobre las aplicaciones ejecutadas y sus módulos (tamaño, atributos, fecha de creación, detalles de encabezado PE, región, nombre, ubicación, empaquetadores).
- Información sobre los errores y el uso de la interfaz de la aplicación de Kaspersky instalada.
- Información sobre las conexiones de red: dirección IP de la computadora remota y de la computadora del usuario, los números de los puertos a través de los cuales se estableció la conexión y el protocolo de red de la conexión.
- Información sobre los paquetes de red recibidos y enviados por el equipo a través de redes de TI y telecomunicaciones.
- Información sobre correos electrónicos y mensajes de mensajería instantánea enviados o recibidos.
- Información sobre las direcciones web visitadas: la hora en que se estableció la conexión mediante un protocolo abierto, datos sobre el nombre de usuario y contraseña del sitio web y el contenido de las cookies.
- Certificado público del servidor.

Los archivos de rastreo contienen solo la información necesaria para solucionar 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, se desactiva la creación de archivos de rastreo. Puede habilitar la generación de archivos de rastreo en la configuración de la aplicación.

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

Puede elegir el modo en que los archivos de rastreo se envían a Kaspersky.

Antes de enviar archivos de rastreo a Kaspersky, revise 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 contenidos en los archivos de rastreo que envía, y brinda su consentimiento para el método usado para enviarlos.

También es posible que, para someterlos a un análisis más profundo, se envíen a Kaspersky ciertos archivos (o partes de archivos) que los intrusos puedan aprovechar para dañar el equipo o los datos.

Kaspersky protege toda información recibida de acuerdo con la ley y las reglas de Kaspersky aplicables. 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, posteriormente puede cambiar su decisión en cualquier momento.

Activar Kaspersky Endpoint Security

Importante: antes de activar Kaspersky Endpoint Security, asegúrese de que la fecha y hora del equipo coincidan con la fecha y hora reales.

La activación de la aplicación implica agregar una clave a la aplicación.

Nota: se requiere conexión a Internet para activar la aplicación.

Activar la versión de prueba

1. Abrir 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 **Activar**.

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

   Importante: la versión de prueba de Kaspersky Endpoint Security se puede activar solo si la aplicación no se activó previamente en el equipo.

Activar la aplicación con un código de activación

1. Abrir 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**, escriba el código de activación que recibió al comprar Kaspersky Endpoint Security.
4. Haga clic en **Activar**.

   Nota: el código de activación es una combinación única de 20 números y letras latinas con el formato 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 comprueba el código de activación correctamente, la aplicación recibe y agrega automáticamente la clave de licencia.

   Nota: Según el código de activación que recibió, es posible que deba completar un formulario de registro.

   Si la verificación del código de activación falla, se muestra la notificación correspondiente. En este caso, comuníquese con el proveedor de software que le proporcionó ese código de activación.

Una vez que activa 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 tiene)
- El tipo de licencia y la cantidad de equipos en los que se puede usar la aplicación de acuerdo con la licencia actual o a la suscripción
- Funciones de la aplicación que están disponibles bajo la licencia o suscripción actual
- Fecha y hora de caducidad de la licencia
- Cantidad de días restantes hasta que la licencia caduque

Ver información de licencia

Ver información de licencia

1. Abrir 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 tiene)
- El tipo de licencia y la cantidad de equipos en los que se puede usar la aplicación de acuerdo con la licencia actual o a la suscripción
- Funciones de la aplicación que están disponibles bajo la licencia o suscripción actual
- Fecha y hora de caducidad de la licencia
- Cantidad de días restantes hasta que la licencia caduque

Administrar licencias y suscripciones

Debe renovar la licencia si la licencia asociada con la clave activa venció y no se agregó ninguna clave de reserva. Cuando la licencia vence, la aplicación continúa funcionando con una funcionalidad reducida (las actualizaciones, Kaspersky Security Network, Control Web y Cifrado de disco FileVault a través de Kaspersky Security Center dejan de estar disponibles). Puede continuar utilizando todos los componentes de la aplicación y ejecutar análisis de malware, pero solo con las bases de datos antimalware que se instalaron antes del vencimiento de la licencia.

Importante: Cuando las bases de datos antimalware están desactualizadas, el riesgo de infección del equipo es más alto.

Renovar una licencia

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

   Se abre la ventana **Centro de protección**.

2. En la ventana **Centro de protección**, haga clic en **Renovar**.

   Se abre una página que contiene información sobre la renovación de una licencia a través de la tienda en línea de Kaspersky o los partners de Kaspersky. Cuando renueva una licencia en la tienda en línea, se envía un código de activación para Kaspersky Endpoint Security a la dirección de correo electrónico especificada en el formulario de pedido luego de completado el pago.

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

Si usa la aplicación bajo una suscripción ilimitada, Kaspersky Endpoint Security renueva su suscripción automáticamente, sin que usted tenga que llevar a cabo ninguna acción.

Si utiliza la aplicación con una suscripción limitada y el período de gracia para renovar la suscripción ha finalizado, Kaspersky Endpoint Security se lo notificará y dejará de intentar renovar automáticamente la suscripción y actualizar las bases de datos de la aplicación.

Puede renovar su suscripción manualmente si se comunica con el proveedor que le vendió Kaspersky Endpoint Security.

Renovar la suscripción

1. Abrir 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**.

   El sitio web de su proveedor de servicios se abre.

El estado de la suscripción puede quedar desactualizado. En este caso, debe actualizar manualmente el estado de la suscripción. Si no tiene una suscripción actual, Kaspersky Endpoint Security deja de actualizar las bases de datos de la aplicación (si tiene una suscripción a las actualizaciones) o deja de proteger el equipo (si tiene una suscripción a las actualizaciones y la protección).

Actualizar el estado de la suscripción

1. Abrir 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 el botón ↻.

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

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

Comparación de las características 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 avanzada contra amenazas						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Detección de comportamiento	✓	✓	✓	✓	✓	✓
Prevención de exploits	✓	✓	✓	✓	✓	✓
Motor de reparación	✓	✓	✓	✓	✓	✓
Protección básica contra amenazas						
Protección contra archivos peligrosos	✓	✓	✓	✓	✓	✓
Protección contra amenazas web	✓	✓	✓	✓	✓	✓
Protección contra amenazas de correo	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓	✓	✓	✓
Controles de seguridad						
Control de dispositivos	✓	✓	✓	✓	✓	✓
Control Web	✓	✓	✓	✓	✓	✓
Cifrado de datos						
Cifrado de disco 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)*	✓	✓	✓	✓	✓	✓

Realizar las tareas más usuales

Iniciar y cerrar la aplicación

En cuanto se completa la instalación, la aplicación se inicia automáticamente y aparece el ícono de la aplicación en la barra de menús.

Abrir la aplicación

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

Salir de la aplicación

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

Cuando sale de la aplicación, el proceso de 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 la protección del equipo

El indicador de estado de la protección le informa sobre problemas de protección del equipo. Este indicador tiene forma de escudo y está ubicado en la ventana principal de la aplicación. El color del indicador cambia según el estado de protección del equipo. Si Kaspersky Endpoint Security detecta alguna amenaza, aparece un mensaje al respecto en la ventana principal de la aplicación y la ventana principal de la aplicación cambia de color.

El color del indicador puede cambiar de los siguientes modos:

- **Verde**. Su equipo está protegido de manera adecuada.

  Una ventana principal de la aplicación de color verde significa que las bases de datos antimalware están actualizadas y que todos los componentes de la aplicación están configurados según las recomendaciones de Kaspersky. No hay objetos maliciosos en el equipo o se los ha neutralizado.

- **Amarillo**. El nivel de protección del equipo no es el óptimo.

  Una ventana principal de la aplicación de color amarillo significa que Kaspersky Endpoint Security sabe que hay un problema. Estos problemas incluyen pequeñas desviaciones de la configuración de protección recomendada o bases de datos de aplicaciones ligeramente obsoletas.

- **Rojo**. El equipo corre el riesgo de infectarse.

  Un indicador de color rojo significa que hay problemas peligrosos que pueden provocar infección en el equipo y pérdida de datos. Esto ocurre, por ejemplo, cuando las bases de datos de malware están obsoletas, la aplicación no está activada o hay objetos maliciosos detectados.

  Recomendamos que solucione cualquier problema y aborde las amenazas de seguridad lo antes posible.

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 de **Seguridad**. El indicador junto al nombre de cada componente refleja su estado.

Ver el estado del componente

1. Abrir 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 ejecuta y está administrado por una directiva de seguridad.
	El componente no funciona correctamente.
	El componente no funciona correctamente y está administrado por una directiva de seguridad.
	El componente está apagado.
	El componente está desactivado y 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 el componente.

Deshabilitar y reanudar la protección del equipo

De forma predeterminada, Kaspersky Endpoint Security se inicia luego de que comienza a funcionar el sistema operativo y protege el equipo hasta que se apaga. Todos los componentes de protección (Protección contra archivos peligrosos, Protección contra amenazas web y Protección contra amenazas de red) están habilitados y en ejecución.

Puede deshabilitar la protección completamente o deshabilitar componentes específicos de la protección.

Importante: Kaspersky le recomienda enfáticamente no deshabilitar la protección ni los componentes de protección, ya que esto puede causar una infección del equipo y la pérdida de datos.

Cuando la protección del equipo se deshabilita:

- El ícono de la aplicación en la barra de menús está inactivo.
- El indicador de estado de la protección de la ventana principal de la aplicación aparece en rojo.

Cuando uno o varios componentes de protección se deshabilitan, el indicador de estado de la protección aparece en rojo o amarillo.

Nota: deshabilitar o suspender estos componentes de protección no tiene ningún efecto sobre las tareas de análisis ni sobre la tarea de actualización.

Puede deshabilitar o reanudar la protección del equipo mediante uno de los siguientes métodos:

- Desde el ícono de la aplicación
- Desde la ventana de configuración de la aplicación
- Desde el menú **Protección**

Deshabilitar/reanudar la protección del equipo desde el ícono de la aplicación

1. En la barra de menús, haga clic en el ícono de la aplicación y elija **Desactivar protección/Activar protección**.

   Al desactivar la protección, se le solicitará que ingrese las credenciales de administrador.

2. Cuando se le soliciten las credenciales de administrador, escriba el nombre y la contraseña del administrador y confirme que desea desactivar la protección.

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

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **General**, marque o desmarque la casilla **Habilitar protección**.

Deshabilitar/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 deshabilitó la protección del equipo, no se volverá a habilitar automáticamente cuando se reinicie Kaspersky Endpoint Security. Debe volver a habilitar el componente de protección manualmente.

Deshabilitar un componente de protección

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial** de la sección **<nombre del componente>**, desactive la casilla **Habilitar <nombre del componente>**.

Importante: si deshabilita un componente de protección, no se volverá a habilitar automáticamente cuando se reinicie Kaspersky Endpoint Security. Debe volver a habilitar el componente de protección manualmente.

Habilitar un componente de protección

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial** de la sección **<nombre del componente>**, seleccione la casilla **Habilita <nombre del componente>**.

Para activar la protección del equipo o los componentes de protección, también puede utilizar el Centro de protección. Si deshabilita la protección del equipo o algún componente de protección, el riesgo de infección del equipo es muchísimo más alto. Es por ello que el Centro de protección le informa cuando está deshabilitada la protección.

Usar el Centro de protección

El *Centro de protección* es una función de Kaspersky Endpoint Security que permite analizar y solucionar problemas y amenazas de seguridad del equipo.

Abrir el Centro de protección

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

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

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

Para cada problema o amenaza, Kaspersky Endpoint Security sugiere acciones que puede realizar para resolverlos. Por ejemplo, si Kaspersky Endpoint Security detecta archivos infectados en el equipo, puede hacer clic en **Desinfectar**. Si las bases de datos antimalware no están actualizadas, puede hacer clic en **Actualizar**. Puede reparar un problema o neutralizar una amenaza de inmediato o posteriormente.

Reparar un problema o neutralizar una amenaza de inmediato

Haga clic en el botón con el nombre de la acción recomendada para reparar el problema o neutralizar la amenaza.

La aplicación lleva a cabo la acción seleccionada.

Si cierra el Centro de protección sin neutralizar las amenazas peligrosas, el indicador del estado de la protección que aparece en la ventana principal de la aplicación permanecerá en color rojo para recordarle sobre estas amenazas.

Realizar tareas de análisis

Kaspersky Endpoint Security incluye la tarea predeterminada Análisis completo. Al ejecutar esta tarea, la aplicación analiza la memoria, los objetos de inicio y todas las unidades internas del equipo en busca de virus y otros tipos de malware.

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**.

Comienza un análisis completo del equipo.

Kaspersky Endpoint Security incluye la tarea predeterminada Análisis rápido. Al ejecutar esta tarea, la aplicación analiza las áreas críticas del equipo (memoria, objetos de inicio y carpetas del sistema) en busca de virus y otros tipos de malware.

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**.

Un análisis rápido del equipo comienza automáticamente.

Si desea analizar un objeto individual (como un disco interno, una carpeta, un archivo o un disco extraíble) en busca de virus y otros tipos de malware, puede ejecutar la tarea Análisis personalizado.

Analizar un elemento seleccionado

Realice una de las siguientes acciones:

- Haga clic derecho en un elemento seleccionado y elija **Analizar en busca de malware**.
- Arrastre el elemento seleccionado al ícono de la aplicación en el Dock.
- Arrastre un elemento seleccionado a 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 del alcance 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 programado

Puede crear una programación para iniciar las tareas Análisis rápido y Análisis completo. Kaspersky Endpoint Security analiza automáticamente todo el equipo o las áreas específicas del equipo 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 **Programar análisis**.

   Un cuadro de diálogo se abrirá y desde allí podrá configurar la programación.

3. Seleccione la casilla **Análisis completo** o **Análisis rápido**.

4. Especifique la frecuencia de análisis y la hora del inicio del análisis.

5. Haga clic en **Aceptar**.

Programar una tarea de análisis desde la ventana de Configuración

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, haga clic en **Programación**.

3. En la ventana que se abre, seleccione la casilla de verificación junto al nombre de la tarea de análisis que desea iniciar en un horario.

4. Configure la frecuencia y el tiempo de la tarea de análisis.

5. Haga clic en **Aceptar** para guardar los cambios realizados en la programación de la tarea 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 actualizaciones de Kaspersky dedicados son el origen principal de actualizaciones para Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede usar puntos de distribución, carpetas locales u otros servidores web como un *origen de actualizaciones*.

Nota: se requiere una conexión a Internet para descargar actualizaciones de los servidores de actualización.

De forma predeterminada, Kaspersky Endpoint Security revisa periódicamente los Servidores de actualizaciones de Kaspersky en busca de actualizaciones. Si en un servidor hay nuevas actualizaciones disponibles, Kaspersky Endpoint Security las descarga en segundo plano y las instala en el equipo.

Iniciar una actualización de Kaspersky Endpoint Security

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

   Se abre la ventana **Actualizar**.

2. Haga clic en **Actualizar**.

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

Además, puede iniciar una tarea de actualización de una de las siguientes maneras:

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

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

Habilitar o deshabilitar las descargas automáticas de las actualizaciones de bases de datos de Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Actualización**, en la sección **Bases de datos**, active o desactive la casilla **Descargar actualizaciones automáticamente**.

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

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

Pasos a seguir si se bloquea el acceso a archivos

La aplicación Kaspersky Endpoint Security bloquea el acceso a archivos y aplicaciones infectados. Si un archivo está infectado, debe desinfectarse antes de que pueda 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 ••• junto al archivo correspondiente y seleccione **Desinfectar**.

   La aplicación comienza a desinfectar el objeto seleccionado. Cuando la desinfección está en curso, la aplicación muestra un cuadro de diálogo en el que puede seleccionar la acción que se llevará a cabo en 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 comienza a desinfectar los objetos detectados. Cuando la desinfección está en curso, la aplicación muestra un cuadro de diálogo en el que puede seleccionar la acción que se llevará a cabo en el objeto. Si selecciona la casilla **Aplicar a todo** en la ventana de notificaciones al seleccionar la acción que se llevará a cabo en el objeto, la aplicación aplicará esta acción a todos los archivos de este tipo.

Si sabe con certeza que los archivos bloqueados por la Protección contra archivos peligrosos son seguros, puede incluirlos en la Zona de confianza.

Restaurar un objeto que ha sido eliminado o desinfectado por la aplicación

En ocasiones, no es posible guardar archivos en su totalidad durante el proceso de desinfección. Si un archivo desinfectado contiene información importante a la que no puede accederse luego de la desinfección, sea de forma completa o parcial, puede intentar restaurar el archivo original a partir de su copia de respaldo.

Restaurar un archivo que ha sido eliminado o modificado por la aplicación durante el proceso de desinfección

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

   Se abre la ventana **Objetos detectados**.

2. En la sección **Depósito de copias de seguridad**, haga clic en ••• que aparece junto al archivo que desea restaurar.

   Se abre el menú despegable.

3. Elija **Restaurar archivo**.

   Se abre una ventana para especificar el nombre del archivo, la etiqueta y la carpeta en la que se restaurará el archivo. Por defecto, el nombre y la ubicación del archivo original ya están especificados.

4. Especifique el nombre del archivo y la carpeta en la que se restaurará el archivo.

5. Haga clic en **Guardar**.

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

Debe analizar el archivo inmediatamente después de restaurarlo para detectar malware. Es posible que el objeto pueda desinfectarse utilizando bases de datos actualizadas sin corromperse.

Importante: recomendamos que no restaure las copias de seguridad de archivos a menos que sea absolutamente necesario, ya que, si lo hace, se podría provocar una infección en el equipo.

Ver el informe de funcionamiento de la aplicación

Puede ver un informe de Kaspersky Endpoint Security en el que se enumeran 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 independiente para cada uno de los siguientes componentes de la aplicación: Protección contra archivos peligrosos, Protección contra amenazas web, Protección contra amenazas de red, Detección de comportamiento y las tareas de análisis y actualización.

Abrir la ventana Informes

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

Qué se debe hacer si aparecen ventanas de notificaciones

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

Si aparece una notificación en la pantalla, seleccione una de las opciones sugeridas. La opción óptima es la que los expertos de Kaspersky establecen como predeterminada.

Configuración avanzada de la aplicación

Alcance de la protección del equipo

Los objetos detectados por Kaspersky Endpoint Security se dividen en categorías de acuerdo con distintos atributos. La aplicación siempre busca virus, gusanos, troyanos y herramientas maliciosas. Estos programas pueden producir daños significativos a su equipo. Para asegurar la protección más fiable para su equipo, puede ampliar la lista de objetos detectables al habilitar la aplicación para examinar software lícito que los intrusos puedan usar para dañar su equipo o sus datos personales.

Los objetos contra los cuales Kaspersky Endpoint Security brinda protección se agrupan de la forma siguiente:

- **Virus, gusanos, programas troyanos, utilidades maliciosas, adware y marcadores automáticos**.

  Esta categoría incluye lo siguiente:

  - Todos los tipos de malware.
  - Software que puede resultarle molesto porque muestra publicidades (por ejemplo, anuncios) en el equipo o remplaza los resultados de búsqueda del navegador con sitios web de publicidad.
  - Aplicaciones que subrepticiamente establecen conexiones telefónicas a través del módem de un equipo.

  La protección contra todos los tipos de malware es el nivel mínimo de seguridad necesario. De acuerdo con las recomendaciones de los expertos de Kaspersky, Kaspersky Endpoint Security siempre supervisa los objetos de estas categorías.

- **Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales**. Esta categoría incluye el software lícito que los intrusos pueden usar para dañar su equipo o sus datos personales; por ejemplo, aplicaciones de administración remota.

Seleccionar las categorías de objetos para detectar

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

   Se abre la ventana de configuración de la aplicación.

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

   Nota: Kaspersky Endpoint Security siempre protege su equipo contra virus, gusanos, programas troyanos, herramientas maliciosas, adware y marcadores automáticos. Por lo tanto, no se puede desactivar la casilla de esta categoría.

Según las categorías seleccionadas de objetos para detectar, Kaspersky Endpoint Security utiliza todas o algunas de sus bases de datos antimalware al ejecutar la Protección contra archivos peligrosos, la Protección contra amenazas web y las tareas de análisis.

Nota: si Kaspersky Endpoint Security clasifica una aplicación como malware pero usted considera que es peligrosa, puede agregarla a una Zona de confianza.

Una *Zona de confianza* es una lista de objetos que Kaspersky Endpoint Security no analiza ni supervisa. Puede agregar objetos a una Zona de confianza si, por ejemplo, Kaspersky Endpoint Security bloquea el acceso a un archivo, una aplicación o un sitio web, incluso si está absolutamente seguro de que el objeto, la aplicación o la dirección web no suponen ningún riesgo para la seguridad.

Cuando se agrega una aplicación a la Zona de confianza, ya no se supervisan sus actividades de red y de archivo (incluyendo las que resultan 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 la configuración de la Zona de confianza.

Agregar/eliminar un archivo o carpeta a la lista de archivos y carpetas de confianza

1. En la barra de menús, haga clic en el ícono de la aplicación y elija **Configuración**.
   Se abre la ventana de configuración 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 la Zona de confianza.
3. En la pestaña **Archivos y carpetas**, edite la lista de archivos y carpetas de confianza:
   - Para agregar un archivo o una carpeta a la lista:
     a. Haga clic en +.
        Se abre un diálogo en el que puede seleccionar un archivo o una carpeta.
     b. Seleccione el archivo o la carpeta que desea agregar.
     c. Haga clic en **Abrir**.
   - Para eliminar un archivo o una carpeta de la lista:
     a. Seleccione el archivo o la carpeta que desea eliminar de la lista de archivos y carpetas de confianza.
     b. Haga clic en –.
4. Haga clic en **Aceptar**.

Agregar/eliminar una dirección web de confianza a la lista de direcciones web de confianza

1. En la barra de menús, haga clic en el ícono de la aplicación y elija **Configuración**.
   Se abre la ventana de configuración 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 la Zona de confianza.
   También puede abrir esta ventana haciendo clic en el botón **Zona de confianza** en la sección **General** de la pestaña **Esencial**.

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. Escriba la dirección web que desea agregar a la lista.

     c. Haga clic en **Aceptar**.

   - Para eliminar una dirección web de la lista:

     a. Seleccione la dirección web que desea eliminar.

     b. Haga clic en –.

4. Haga clic en **Aceptar**.

De forma predeterminada, la lista de direcciones web de confianza está vacía.

Agregar/eliminar una aplicación de confianza en la lista de aplicaciones de confianza

1. En la barra de menús, haga clic en el ícono de la aplicación y elija **Configuración**.
   Se abre la ventana de configuración 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 la Zona de confianza.
   También puede abrir esta ventana haciendo clic en el botón **Zona de confianza** en la sección **General** de la pestaña **Esencial**.

3. En la pestaña **Aplicaciones de confianza**, edite la lista de aplicaciones de confianza:

   - Para agregar una aplicación a la lista:

     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 desee agregar:

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

     > **Nota:** Puede ingresar los valores de estos dos parámetros manualmente o hacer clic en el botón **Seleccionar** y elegir la aplicación que desee agregar en la ventana que se abre. En este caso, los valores de estos parámetros se insertarán de forma automática.

c. En la sección **Opciones**, seleccione al menos un tipo de actividad que no desee 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:

a. Seleccione la aplicación que desee eliminar.

b. Haga clic en –.

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

Editar una aplicación de confianza

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

   Se abre la ventana de configuración 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 la Zona de confianza.

   También puede abrir esta ventana haciendo clic en el botón **Zona de confianza** en la sección **General** de la pestaña **Esencial**.

3. En la pestaña **Aplicaciones de confianza**, seleccione la aplicación que desee editar.

4. Haga clic en **Editar**.

5. En la ventana que se abre, edite los parámetros de la aplicación.

6. Haga clic en **Aceptar**.

Habilitar la supervisión de una dirección web de confianza

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

   Se abre la ventana de configuración 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 la Zona de confianza.

3. En la pestaña **Direcciones web**, desmarque la casilla situada junto a una dirección web que desee que la aplicación Kaspersky Endpoint Security supervise.

4. Haga clic en **Aceptar**.

Protección contra archivos peligrosos

La Protección contra archivos peligrosos protege el equipo contra la infección del sistema de archivos. El componente se ejecuta durante el inicio del sistema operativo, permanece en la memoria del equipo y analiza todos los archivos abiertos guardados o ejecutados en el equipo y en todos los discos conectados en busca de malware. Si se deshabilita la Protección contra archivos peligrosos, no se ejecutará en el arranque del sistema operativo. Deberá volver a habilitar la Protección contra archivos peligrosos manualmente.

Habilitar/deshabilitar la Protección contra archivos peligrosos

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de archivo**, marque/desmarque la casilla **Habilitar la Protección contra amenazas de archivo**.

   También puede habilitar la Protección contra archivos peligrosos en el Centro de protección. Si deshabilita la protección del equipo o algún componente de protección, el riesgo de infección del equipo es muchísimo más alto. Es por ello que el Centro de protección le informa cuando está deshabilitada la protección.

Puede crear un alcance de la protección para la Protección contra archivos peligrosos.

Agregar/eliminar un archivo o carpeta al alcance de la protección

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de archivo**, haga clic en **Alcance de la protección**.

   Se abre una ventana con una lista de objetos que la Protección contra archivos peligrosos analiza. De forma predeterminada, la Protección contra archivos peligrosos analiza todos los objetos que se encuentran en los discos internos, extraíbles y de red conectados al equipo.

   > **Nota:** Puede omitir el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis. De manera predeterminada, la Protección contra archivos peligrosos no analiza el volumen del sistema de solo lectura.

3. En la sección **Alcance de la protección**, agregue o elimine objetos en el alcance de la protección:

   - Para agregar un archivo o una carpeta al alcance de la protección:

     a. Haga clic en +.

        Se abre un menú desplegable en el que puede seleccionar los objetos que desea agregar al alcance de la protección.

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

        Se abre un diálogo en el que puede seleccionar un archivo o una carpeta.

     c. Seleccione el archivo o la carpeta que desea agregar al alcance de protección.

     d. Haga clic en **Abrir**.

- Para eliminar un archivo o carpeta del alcance de la protección:

  a. Seleccione un objeto en la lista de objetos del alcance de la protección.

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

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

   Importante: la optimización puede estar deshabilitada por razones de seguridad.

5. Haga clic en **Guardar**.

Agregar/eliminar un objeto de la lista de objetos predeterminados al/del alcance de la protección:

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de archivo**, haga clic en **Alcance de la protección**.

   Se abre una ventana con una lista de objetos que la Protección contra archivos peligrosos analiza. De forma predeterminada, la Protección contra archivos peligrosos analiza todos los objetos que se encuentran en los discos internos, extraíbles y de red conectados al equipo.

   Nota: Puede omitir el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis. De manera predeterminada, la Protección contra archivos peligrosos no analiza el volumen del sistema de solo lectura.

3. En la sección **Alcance de la protección**, agregue o elimine los objetos de la lista de objetos predeterminados en el alcance de la protección:

   - Para agregar un objeto de la lista de objetos predeterminados al alcance de la protección:

     a. Haga clic en +.

     Se abre un menú desplegable en el que puede seleccionar los objetos que desea agregar al alcance de la protección.

     b. En el menú desplegable, seleccione un objeto que desee agregar al alcance de la protección (por ejemplo, **Todos los discos internos**).

   - Para eliminar un objeto de la lista de objetos predeterminados desde el alcance de la protección:

     a. Seleccione un objeto en la lista de objetos del alcance de la protección.

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

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

   Importante: la optimización puede estar deshabilitada por razones de seguridad.

5. Haga clic en **Guardar**.

Deshabilitar la protección de un objeto que se encuentra en el alcance de la protección

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de archivo**, haga clic en **Alcance de la protección**.

   Se abre una ventana con una lista de objetos que la Protección contra archivos peligrosos analiza. De forma predeterminada, la Protección contra archivos peligrosos analiza todos los objetos que se encuentran en los discos internos, extraíbles y de red conectados al equipo.

   Nota: Puede omitir el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis. De manera predeterminada, la Protección contra archivos peligrosos no analiza el volumen del sistema de solo lectura.

3. Desactive la casilla junto al objeto en la lista de objetos del alcance de la protección.

4. Haga clic en **Guardar**.

Habilitar el análisis del volumen del sistema de solo lectura

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de archivo**, haga clic en **Alcance de la protección**.

   Se abre una ventana con una lista de objetos que la Protección contra archivos peligrosos analiza. De forma predeterminada, la Protección contra archivos peligrosos analiza todos los objetos que se encuentran en los discos internos, extraíbles y de red conectados al equipo.

   Nota: Puede omitir el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis. De manera predeterminada, la Protección contra archivos peligrosos no analiza el volumen del sistema de solo lectura.

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

   Importante: la optimización puede estar deshabilitada por razones de seguridad.

4. Haga clic en **Guardar**.

Cuando usted o una aplicación intentan obtener acceso a un archivo incluido en el alcance de la protección, la Protección contra archivos peligrosos comprueba si las bases de datos de iSwift contienen información sobre el archivo y utiliza esta información para decidir si debe analizarlo.

Es posible identificar los objetos maliciosos gracias al uso del *análisis de firmas*, un modo de búsqueda de amenazas que utiliza las descripciones de amenazas incluidas en las bases de datos antimalware. Además del análisis de firmas, la Protección contra archivos peligrosos usa el análisis heurístico y otras tecnologías de análisis.

Si se detecta una amenaza en un archivo, Kaspersky Endpoint Security identifica el tipo de malware detectado (por ejemplo, *virus* o *troyano*). Después, la aplicación muestra una notificación sobre el objeto detectado y realiza una acción sobre el objeto en función de la configuración de la Protección contra archivos peligrosos.

Seleccionar qué acción realizará la Protección contra archivos peligrosos después de detectar un objeto infectado

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de archivo**, seleccione la acción que la Protección contra archivos peligrosos realizará cuando detecte un archivo infectado.

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

La información sobre la Protección contra archivos peligrosos y todos los objetos detectados se registra en un informe.

Nota: si la Protección contra archivos peligrosos se detiene y muestra un mensaje de error, vea el informe e intente reiniciar el componente. Si el problema no se resuelve, puede comunicarse con el Soporte técnico de Kaspersky.

Ver el informe de Protección contra archivos peligrosos

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

   Se abrirá la ventana **Informes**.

2. Abra la pestaña **Protección contra amenazas de archivo**.

Protección contra amenazas web

Cuando usa Internet, su equipo corre el riesgo de sufrir una infección por malware y otras amenazas de seguridad. Las amenazas de la seguridad pueden penetrar el equipo cuando descarga programas gratuitos o visita sitios web que fueron atacados por piratas informáticos. Además, los gusanos de red pueden atacar su equipo ni bien este se conecte a Internet, incluso antes de que abra una dirección web o descargue un archivo.

Kaspersky Endpoint Security protege la información que envía y recibe 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 se utilizan con mayor frecuencia para la transferencia de datos a través de HTTP y HTTPS. Kaspersky Endpoint Security analiza las conexiones cifradas (HTTPS) solo si está seleccionada la casilla de verificación **Verificar conexiones seguras (HTTPS)** en la sección **General**.

Habilitación/deshabilitación de la Protección frente a amenazas en la web

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas web**, marque o desmarque la casilla **Habilitar Protección contra amenazas web**.

También puede habilitar la Protección frente a amenazas en la web en el Centro de protección. Si deshabilita la protección del equipo o algún componente de protección, el riesgo de infección del equipo es muchísimo más alto. Es por ello que el Centro de protección le informa cuando está deshabilitada la protección.

Importante: si deshabilitó la Protección frente a amenazas en la web, no se volverá a habilitar en forma automática cuando inicie nuevamente Kaspersky Endpoint Security ni cuando reinicie el sistema operativo. Debe volver a habilitar la Protección frente a amenazas en la web manualmente.

La Protección frente a amenazas en la web analiza el tráfico web según la configuración recomendada por Kaspersky. Los objetos maliciosos son reconocidos a través de análisis de firmas, análisis heurístico e información proveniente de Kaspersky Security Network.

Si se verifican los vínculos de los sitios web en busca de amenazas de phishing y direcciones web maliciosas, es posible evitar los *ataques de phishing*. Los *ataques de phishing* suelen ser mensajes de correo electrónico enviados por delincuentes que se hacen pasar por instituciones financieras (por ejemplo, bancos) y envían vínculos a sitios web fraudulentos. En estos correos electrónicos, los criminales intentan engañar al usuario para que visite un sitio web fraudulento e introduzca datos confidenciales (por ejemplo, el número de su tarjeta bancaria o el nombre de usuario y la contraseña de su cuenta bancaria en línea). Un ataque phishing se puede disfrazar, por ejemplo, como un mensaje desde su banco con un vínculo a su sitio web oficial, pero en realidad el vínculo abre una copia exacta del sitio web oficial del banco creado por impostores.

La Protección frente a amenazas en la web supervisa el tráfico web en busca de intentos de visitar un sitio web fraudulento y bloquea el acceso a dichos sitios. Para comprobar los vínculos de los sitios web en busca de amenazas de phishing y direcciones web maliciosas, Kaspersky Endpoint Security utiliza las bases de datos de la aplicación, el análisis heurístico y los datos de Kaspersky Security Network.

Algoritmo de análisis de tráfico web

La Protección frente a amenazas en la web intercepta y analiza en busca de código malicioso cada sitio web o archivo a los que el usuario o una aplicación acceden a través de los protocolos HTTP y HTTPS:

- Si un sitio web o archivo contiene código malicioso, Kaspersky Endpoint Security lo bloquea y muestra una notificación para indicar que el sitio web o archivo solicitado está infectado.
- Si el archivo o sitio web no contiene código malicioso, el usuario puede acceder a él inmediatamente.

Seleccionar la acción que Protección contra amenazas web debe realizar al detectar objetos peligrosos de tráfico web

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas web**, seleccione la acción que la Protección contra amenazas web realizará cuando detecte un objeto peligroso de tráfico web.

La información sobre el funcionamiento de la Protección frente a amenazas en la web y todos los objetos peligrosos del tráfico web se registra en un informe.

Nota: si la Protección frente a amenazas en la web se detiene y muestra un mensaje de error, vea su informe e intente reiniciar el componente. Si el problema no se resuelve, puede comunicarse con el Soporte técnico de Kaspersky.

Ver el informe de Protección frente a amenazas en la web

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

   Se abrirá la ventana **Informes**.

2. Abra la pestaña **Protección contra amenazas web**.

Protección contra amenazas de correo

El componente Protección contra amenazas de 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 equipo 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.

De manera predeterminada, la Protección contra amenazas de correo está habilitada. Puede deshabilitar la Protección contra amenazas de correo si es necesario.

Según el modo de funcionamiento seleccionado, la Protección contra amenazas de correo realiza las siguientes acciones:

- **Eliminar objetos maliciosos de forma automática**. Si esta opción está seleccionada, 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**. Si esta opción está seleccionada, 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.

Habilitar/deshabilitar la Protección contra amenazas de correo mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Comunicación y Protección web → Protección contra amenazas de correo**.
5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de correo**.
6. Si la Protección contra amenazas de correo está habilitada, seleccione 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 archivos o el tamaño máximo del archivo a analizar.
8. Guarde los cambios.

Habilitar/deshabilitar la Protección contra amenazas de correo mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Protección básica contra amenazas** > **Protección contra amenazas de correo**.
7. Seleccione o anule la selección de la casilla **Habilitar Protección contra amenazas de correo**.
8. En la sección **Acción al detectar una amenaza**, seleccione la acción que se realizará cuando Kaspersky Endpoint Security detecte una amenaza.
9. Si es necesario, en la sección **Configuración de Protección contra amenazas de correo**, configure el límite de tiempo para analizar archivos o el tamaño máximo del archivo a analizar.
10. Haga clic en **Aceptar** para guardar los cambios.

11. Siga uno de estos procedimientos 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.

Habilitar/deshabilitar la Protección contra amenazas de correo mediante la aplicación Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de correo**, marque/desmarque la casilla **Habilitar Protección contra amenazas de correo**.

3. Si la casilla **Habilitar Protección contra amenazas de correo** está seleccionada, seleccione 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 a analizar.

Ver el informe de Protección contra amenazas de correo

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

   Se abrirá la ventana **Informes**.

2. Abra la pestaña **Protección contra amenazas de correo**.

Protección contra amenazas de red

Kaspersky Endpoint Security protege su equipo contra ataques de red.

Un *ataque de red* es un intento de ingresar en el sistema operativo de un equipo remoto. Los criminales llevan a cabo estás intrusiones para apoderarse del control del sistema operativo, provocar la denegación de servicio en el sistema operativo o acceder a información confidencial. Para conseguir estos objetivos, los delincuentes realizan ataques directos, como análisis de puerto y ataques de fuerza bruta, o usan el malware instalado en un equipo bajo ataque.

Los ataques de red pueden dividirse en los siguientes tipos:

- *Análisis de puertos*. Este tipo de ataque de red, por lo general, se lleva a cabo como preparación para otro ataque de red mucho más peligroso. El intruso analiza los puertos UDP/TCP que utilizan servicios de red en el equipo atacado y determina la vulnerabilidad del equipo ante otros ataques de red más peligrosos. El análisis de puertos también permite que el intruso determine el sistema operativo del equipo bajo amenaza y seleccione el ataque red adecuado para ese sistema.

- *Ataques DoS* o ataques de red que provocan que el servicio no responda. Estos ataques dejan el sistema operativo bajo amenaza inestable o completamente inoperable.

Estos son los tipos principales de ataques de denegación de servicio:

- Transmisión de paquetes de red especialmente diseñados que el equipo de destino no espera y, por lo tanto, el sistema operativo de destino comienza a sufrir fallas o deja de funcionar por completo.
- Envío de un gran número de paquetes de red al equipo remoto en muy poco tiempo. Todos los recursos del equipo de destino se utilizan para procesar los paquetes de red que envía el intruso. Por lo tanto, el equipo deja de realizar sus funciones.

- *Ataques de ingreso a la red*. Tales ataques de red están diseñados para "secuestrar" el sistema operativo del equipo de destino. Este es el tipo de ataque más peligroso porque, en caso de tener éxito, el intruso toma por completo el control del sistema operativo.

  Este tipo de ataque a la red se utiliza cuando el intruso desea obtener datos confidenciales (como números de tarjetas bancarias o contraseñas) de un equipo remoto o utilizar en secreto el equipo remoto para sus propios fines (como atacar otros equipos desde este equipo).

Habilitar/deshabilitar la Protección contra amenazas de red

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de red**, marque/desmarque la casilla **Habilitar Protección contra amenazas de red**.

También puede habilitar la Protección contra amenazas de red en el Centro de protección. Si deshabilita la protección del equipo o algún componente de protección, el riesgo de infección del equipo es muchísimo más alto. Es por ello que el Centro de protección le informa cuando está deshabilitada la protección.

Importante: si deshabilitó la Protección contra amenazas de red, no se volverá a habilitar en forma automática cuando inicie nuevamente Kaspersky Endpoint Security ni después de que se reinicie el sistema operativo. Debe volver a habilitar la Protección contra amenazas de red manualmente.

Cuando la aplicación detecta una actividad de red peligrosa, Kaspersky Endpoint Security automáticamente agrega 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 ícono de la aplicación y elija **Configuración**.

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de red**, seleccione la casilla **Habilitar Protección contra amenazas de red**.

3. Haga clic en **Configuración**.

   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 representa una amenaza, seleccione la dirección IP del equipo en la lista y haga clic en **Desbloquear**.

   Se abre un cuadro de diálogo de confirmación.

6. En la ventana 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 prefiere que Kaspersky Endpoint Security no vuelva a bloquear la dirección IP seleccionada, 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 ícono de la aplicación y elija **Configuración**.

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Protección contra amenazas de red**, seleccione la casilla **Habilitar Protección contra amenazas de red**.

3. Haga clic en **Configuración**.

   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, escriba la dirección IP del equipo de confianza.

   - Para eliminar una dirección IP de la lista de equipos de confianza:

     a. Seleccione la dirección IP en la lista.

     b. Haga clic en –.

   - Para editar una dirección IP en la lista de equipos de confianza:

     a. Seleccione la dirección IP en la lista.

     b. Haga clic en **Editar**.

     c. Modifique la dirección IP.

6. Haga clic en **Guardar**.

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

Nota: si el componente Protección contra amenazas de red se detiene y muestra un mensaje de error, vea el informe e intente reiniciar el componente. Si el problema no se resuelve, puede comunicarse con el Soporte técnico de Kaspersky.

Ver el informe de Protección contra amenazas de red

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

   Se abrirá la ventana **Informes**.

2. Abra la pestaña **Protección contra amenazas de red**.

Firewall

Firewall bloquea conexiones no autorizadas al equipo mientras se trabaja en Internet o en una red local. Esto le permite proteger su LAN corporativa contra el robo de identidad y otros ataques. El componente proporciona protección al equipo 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 agrega 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 equipo que está conectado a dicha red, Firewall bloquea el acceso a los archivos y las impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. Firewall asigna el tipo de red pública a Internet de forma predeterminada. No puede cambiar el tipo de Internet.

- **Red local**. Red para usuarios con acceso restringido a archivos e impresoras en este equipo (por ejemplo, para una LAN corporativa o una red doméstica).

- **Red de confianza**. Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de las redes con este estado.

Administrar el componente Firewall en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Protección básica contra amenazas** > **Firewall**.
7. Seleccione o anule la selección de la casilla **Habilitar Firewall**.
8. En la sección **Configuración de Firewall**, haga clic en el botón **Configuración** y agregue, edite o elimine reglas, o cambie su prioridad.
9. En la sección **Redes disponibles**, haga clic en el botón **Configuración** y agregue, edite, elimine o cambie el tipo de redes.
10. Haga clic en **Aceptar** para guardar los cambios.
11. Siga uno de estos procedimientos 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, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Comunicación y Protección web** → **Firewall**.
5. Habilite o deshabilite el componente usando el conmutador **Firewall**.
6. En la sección **Configuración de Firewall**, haga clic en el **Reglas de paquete de red** y agregue, edite o elimine reglas, o cambie su prioridad.
7. En la sección **Redes disponibles**, haga clic en el botón **Configuración de red** y agregue, 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 ícono de la aplicación y elija **Configuración**.

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Esencial**, en la sección **Firewall**, seleccione o anule la selección de la casilla **Habilitar Firewall**.

3. En caso de ser necesario, haga clic en el botón **Configuración** y configure la configuración de Firewall:

   - En la pestaña **Reglas de paquete de red**, puede agregar, editar o eliminar reglas, o cambiar su prioridad.
   - En la pestaña **Redes disponibles**, puede agregar, editar o cambiar el tipo de redes.

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

Ver el informe de Firewall

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

   Se abrirá 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 equipo 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. Las funcionalidades de Kaspersky Endpoint Security basadas en firmas de patrones de comportamiento proporcionan una defensa proactiva para el equipo.

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

Habilitar/deshabilitar la Detección de comportamiento mediante Web Console

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

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

   Se abre la ventana de propiedades de la directiva.

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

4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Detección de comportamiento**.

5. Habilite o deshabilite el componente usando el conmutador **Detección de comportamiento**.

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

   - **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.

   - **Solicitar acción**

     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 según el estado del objeto.

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

   - **Informar**

     Si selecciona esta opción, al detectar un intento de modificar archivos en carpetas compartidas, la aplicación Kaspersky Endpoint Security agrega información sobre este intento a la lista de amenazas activas, agrega 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.

Habilitar/deshabilitar la Detección de comportamiento mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Protección avanzada contra amenazas** > **Detección de comportamiento**
7. Seleccione o anule la selección de la casilla **Habilitar Detección de comportamiento**.
8. Si es necesario, en la sección **Acción al detectar actividad de malware**, seleccione la acción que se realizará cuando se detecte actividad de malware.

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

10. Siga uno de estos procedimientos 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.

Habilitar/deshabilitar la Detección de comportamiento mediante la aplicación Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

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

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

   - **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.

   - **Solicitar acción**

     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 según el estado del objeto.

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

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

Análisis

La Protección contra amenazas de archivo y la Protección contra amenazas web brindan protección informática en tiempo real. También recomendamos que analice regularmente su equipo en busca de malware y otras amenazas a la seguridad del equipo. Esto es necesario para evitar la transmisión de malware no detectado por los componentes de protección.

Kaspersky Endpoint Security contiene las siguientes tareas de análisis integradas:

- **Análisis completo**.

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

- Análisis rápido.

  Análisis de malware limitado a las áreas críticas del equipo: memoria, objetos de inicio y carpetas del sistema.

- **Análisis personalizado**.

  Un análisis de malware de un objeto específico (archivo, carpeta, disco interno o disco extraíble).

- **Análisis de discos externos**

  Un análisis de malware de los discos externos que se realiza cuando se conecta un disco externo al equipo.

Cuando la aplicación realiza una tarea de análisis, los objetos maliciosos se reconocen a través del análisis de firmas. Además del análisis de firmas, Kaspersky Endpoint Security usa 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 Análisis rápido y Análisis completo

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**.

Se inicia la tarea del análisis.

Iniciar la tarea 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 **Análisis personalizado**, realice una de las siguientes acciones:

   - Arrastre un archivo o carpeta a la ventana.
   - Haga clic en **Elegir** y abra un archivo o carpeta.

Se inicia la tarea del análisis.

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 Detener ( ) junto a la tarea de análisis que desea detener.

   Se abre un cuadro de diálogo de confirmación.

3. En el diálogo de confirmación, haga clic en **Detener**.

Se detiene la tarea de análisis.

Puede programar la tarea del Análisis rápido o un Análisis completo.

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 **Programar análisis**.

   Un cuadro de diálogo se abrirá y desde allí podrá configurar la programación.

3. Seleccione la casilla **Análisis completo** o **Análisis rápido**.

4. Especifique la frecuencia de análisis y la hora del inicio del análisis.

5. Haga clic en **Aceptar**.

Programar una tarea de análisis desde la ventana de Configuración

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, haga clic en **Programación**.

3. En la ventana que se abre, seleccione la casilla de verificación junto al nombre de la tarea de análisis que desea iniciar en un horario.

4. Configure la frecuencia y el tiempo de la tarea de análisis.

5. Haga clic en **Aceptar** para guardar los cambios realizados en la programación de la tarea de análisis.

Cuando se conecta un disco externo al equipo, la aplicación Kaspersky Endpoint Security puede comenzar automáticamente a analizar el disco, pedirle que lo analice o no hacer nada. Puede seleccionar una de las opciones en la configuración de la tarea Análisis de discos externos.

Seleccione la acción que la aplicación Kaspersky Endpoint Security realiza cuando se conecta un disco externo al equipo

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

   Se abre la ventana de configuración de la aplicación.

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

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

Las tareas de Análisis completo y Análisis rápido ya contienen alcances de análisis predeterminados. 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 el alcance del análisis de la tarea Análisis rápido.

Nota: Puede omitir el análisis del volumen del sistema de solo lectura para reducir significativamente el tiempo de análisis. De forma predeterminada, Kaspersky Endpoint Security no analiza el volumen del sistema de solo lectura cuando realiza una tarea de Análisis rápido, aunque sí lo hace 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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Habilitar/deshabilitar el análisis del volumen del sistema de solo lectura

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, en la lista a la izquierda, seleccione la tarea **Análisis completo** o **Análisis rápido**.

3. En la sección **Optimización**, anule la selección/seleccione la casilla **Omitir análisis de volumen del sistema de solo lectura**.

   Importante: la optimización puede estar deshabilitada por razones de seguridad.

Agregar/eliminar un archivo o una carpeta del alcance del análisis de la tarea Análisis rápido

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, en la lista a la izquierda, seleccione la tarea **Análisis rápido**.

3. En la sección **Alcance del análisis**, haga clic en **Editar**.

   Se abre una ventana con la lista de objetos en la cobertura del análisis de tareas de Análisis rápido.

4. Editar la lista de objetos del alcance del análisis:

   - Para agregar un archivo o carpeta al alcance del análisis de la tarea del Análisis rápido:

     a. Haga clic en +.

        Se abre un menú desplegable en el que puede seleccionar los objetos que desea agregar a la cobertura del análisis.

     b. Elija el elemento **Archivos y carpetas**.

        Se abre un diálogo en el que puede seleccionar un archivo o una carpeta.

     c. Seleccione el archivo o la carpeta que desea agregar al alcance del análisis de la tarea Análisis rápido.

     d. Haga clic en **Abrir**.

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

  a. Seleccione el objeto que desea eliminar.

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

5. Haga clic en **Guardar**.

Agregar un objeto de la lista de objetos predeterminados de la tarea Análisis rápido al alcance del análisis de la tarea Análisis rápido

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, en la lista a la izquierda, seleccione la tarea **Análisis rápido**.

3. En la sección **Alcance del análisis**, haga clic en **Editar**.

   Se abrirá una ventana con la lista de objetos del alcance del análisis.

4. Haga clic en +.

   Se abre un menú desplegable en el que puede seleccionar los objetos que desea agregar a la cobertura del análisis.

5. En el menú desplegable, seleccione un objeto que desea agregar al alcance del análisis (por ejemplo, **Memoria**).

6. Haga clic en **Aceptar**.

Deshabilitar la protección de un objeto en el alcance del análisis de la tarea Análisis rápido

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, en la lista a la izquierda, seleccione la tarea **Análisis rápido**.

3. En la sección **Alcance del análisis**, haga clic en **Editar**.

   Se abrirá una ventana con la lista de objetos del alcance del análisis.

4. Desmarque la casilla junto al objeto en la lista de objetos del alcance del análisis.

5. Haga clic en **Aceptar**.

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

Seleccionar la acción que realiza Kaspersky Endpoint Security si detecta archivos infectados.

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Análisis**, seleccione una tarea en la lista de tareas.

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 en el depósito de copias de seguridad, para que pueda restaurar el archivo original, si es necesario.

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

Nota: Si se produce algún error durante la ejecución de una tarea de análisis de malware, reiníciela. Si el nuevo intento de ejecutar el análisis también ocasiona un error, comuníquese con el Soporte técnico de Kaspersky.

Ver el informe de tarea de análisis

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

   Se abrirá la ventana **Informes**.

2. Abra la pestaña **Análisis**.

Tareas de actualización

Tener al día las bases de datos de la aplicación es esencial para garantizar la protección del equipo. La Protección contra archivos peligrosos, la Protección contra amenazas web y las tareas de análisis utilizan las bases de datos de la aplicación para buscar y neutralizar malware en el equipo. Las bases de datos de la aplicación se actualizan regularmente con diferentes tipos de amenazas y formas de neutralizarlas, por eso es importante actualizarlas periódicamente.

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

Nota: debe tener acceso a Internet para conectarse a los servidores de actualización y descargar las actualizaciones. Si se conecta a Internet a través de un servidor proxy, es posible que deba establecer la configuración de red.

Para descargar las bases de datos de la aplicación actualizadas, utilice uno de los siguientes métodos:

- **Automático**. Kaspersky Endpoint Security comprueba periódicamente si existen actualizaciones en los servidores de actualizaciones de Kaspersky. Si en un servidor se encuentra disponible una actualización, Kaspersky Endpoint Security la descarga en segundo plano y la instala en el equipo. Esta opción está habilitada de forma predeterminada.

- **Manual**. Puede verificar manualmente si hay actualizaciones disponibles para Kaspersky Endpoint Security en cualquier momento.

Habilitar o deshabilitar las descargas automáticas de las actualizaciones de bases de datos de Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Actualización**, en la sección **Bases de datos**, active o desactive la casilla **Descargar actualizaciones automáticamente**.

Buscar 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 **Actualización**.

   Se abre la ventana **Actualizar**.

2. Haga clic en **Actualizar**.

La aplicación empieza a actualizar las bases de datos.

Además, puede iniciar una tarea de actualización de una de las siguientes maneras:

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

Durante la actualización, los módulos y las bases de datos de la aplicación se comparan con los archivos disponibles en los servidores de actualizaciones. Si las bases de datos instaladas en el equipo son las más recientes, la ventana **Actualización** muestra un mensaje en el que se indica que las bases de datos de la aplicación están actualizadas. Si la versión de la aplicación y las bases de datos de la aplicación difieren de las disponibles en los servidores de actualizaciones, solo se descargan y se instalan en el equipo los componentes faltantes de la actualización. Las actualizaciones incrementales de las bases de datos de la aplicación tardan menos 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 ícono de la aplicación y elija **Configuración**.

   Se abre la ventana de configuración de la aplicación.

2. Seleccione la pestaña **Actualización**.
3. En la sección **Proxy**, seleccione la casilla **Usar servidor proxy** y haga clic en **Configuración**.

   Se abre una ventana en la que puede establecer la configuración de conexión del servidor proxy.

4. Configure 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 estas, por lo que se puede realizar una reversión, si es necesario. La reversión resulta útil si la nueva versión de las bases de datos de la aplicación contiene una firma incorrecta a causa de la cual Kaspersky Endpoint Security bloquea una aplicación segura.

Nota: si las bases de datos de Kaspersky Endpoint Security se corrompen, le recomendamos que inicie una actualización para descargar e instalar la última versión de las bases de datos de la aplicación.

Revertir la última actualización

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

   Se abre la ventana de configuración de la aplicación.

2. Seleccione la pestaña **Actualización**.

3. En la sección **Reversión**, haga clic en **Revertir actualización**.

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

Ver el informe de tareas de actualización

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

2. Se abrirá la ventana **Informes**.

3. Seleccione la pestaña **Actualización**.

Nota: La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y 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 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 malware, puede configurar análisis automáticos de los discos externos al conectarlos 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 malware para el disco externo conectado.

  Esta opción está seleccionada por defecto.

  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 falla la desinfección

  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 se desinfecta, Kaspersky Endpoint Security lo guarda en su ubicación original con su nombre original. Si la desinfección no funciona, Kaspersky Endpoint Security elimina los objetos infectados que no se pudieron desinfectar.

Esta opción está seleccionada por defecto.

Solicitar acción

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

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

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

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **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 de la tarea Análisis de discos externos en Web Console y Cloud Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección contra amenazas de host → Análisis de unidades extraíbles**.
5. Habilite o deshabilite el componente usando el conmutador **Análisis de unidades extraíbles**.
6. Guarde los cambios.

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

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

Copias de seguridad

A veces, la integridad de los archivos infectados no se puede preservar durante el proceso de desinfección. Si un archivo desinfectado contiene información importante a la que no puede accederse luego de la desinfección, sea de forma completa o parcial, puede restaurar el archivo original desde el Depósito de copias de seguridad.

Las *copias de seguridad* son copias de archivos peligrosos que se crean cuando el archivo se desinfecta o elimina. Se almacena en el Depósito de copias de seguridad.

El *Depósito de copias de seguridad* es un área especial de almacenamiento que contiene copias de seguridad de archivos que se eliminaron o modificaron cuando se sometieron a desinfección. La función principal del Depósito de copias de seguridad es la de darle al usuario la oportunidad de restaurar un archivo original en cualquier momento. Los archivos que están en el Depósito de copias de seguridad se guardan en un formato especial y no son peligrosos para el equipo.

Ver 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 **Depósito de copias de seguridad**, vea la lista de archivos respaldados.

Puede restaurar o eliminar copias de seguridad de archivos del Depósito de copias de seguridad.

Restaurar copias de seguridad de archivos 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 **Depósito de copias de seguridad**, haga clic en ••• que aparece junto al archivo que desea restaurar.

   Se abre el menú despegable.

3. Elija **Restaurar archivo**.

   Se abre una ventana para especificar el nombre del archivo, la etiqueta y la carpeta en la que se restaurará el archivo. Por defecto, el nombre y la ubicación del archivo original ya están especificados.

4. Especifique el nombre del archivo y la carpeta en la que se restaurará el archivo.

5. Haga clic en **Guardar**.

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

Debe analizar el archivo inmediatamente después de restaurarlo para detectar malware. Es posible que el objeto pueda desinfectarse utilizando bases de datos actualizadas sin corromperse.

Importante: recomendamos que no restaure las copias de seguridad de archivos a menos que sea absolutamente necesario, ya que, si lo hace, se podría provocar una infección en el equipo.

Eliminar copias de seguridad de archivos 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 **Depósito de copias de seguridad**, realice lo siguiente:

   - Para eliminar todas las copias de respaldo de los archivos, haga clic en **Eliminar todo**.
   - Para eliminar la copia de seguridad seleccionada, haga clic en ••• que se encuentra junto a esta y elija Eliminar copia de seguridad.

De manera predeterminada, el período de almacenamiento de los archivos que se encuentran en el Depósito de copias de seguridad es de 30 días. Cuando este plazo vence, los archivos se eliminan. Puede cambiar el plazo máximo de almacenamiento de respaldo para archivos o eliminar el límite del período de almacenamiento.

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

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

   Se abre la ventana de configuración de la aplicación.

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

Informes

Puede ver un informe de Kaspersky Endpoint Security en el que se enumeran 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 independiente para cada uno de los siguientes componentes de la aplicación: Protección contra archivos peligrosos, Protección contra amenazas web, Protección contra amenazas de red, Detección de comportamiento y las tareas de análisis y actualización.

Abrir la ventana Informes

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

Kaspersky Endpoint Security puede guardar informes en formato de texto. Esta funcionalidad puede ser útil si los componentes de la aplicación o las tareas generan un error que no puede resolver por su cuenta y necesita la ayuda del Soporte técnico de Kaspersky. En este caso, deberá enviar un informe en formato de texto al Soporte técnico de Kaspersky para que nuestros especialistas puedan analizar el problema y solucionarlo lo antes posible.

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

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

   Se abrirá la ventana **Informes**.

2. En el panel izquierdo, seleccione la pestaña del informe deseado.

3. En la esquina derecha superior, haga clic en .

4. En la ventana que se abre, especifique el nombre de archivo, las etiquetas y la carpeta de destino del informe.

5. Haga clic en **Guardar**.

De forma predeterminada, Kaspersky Endpoint Security no registra eventos informativos en los informes. Puede habilitar el registro de eventos informativos.

Permitir el registro de eventos informativos en los informes

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

   Se abre la ventana de configuración 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 conocida como Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* busca, detecta y elimina continuamente las amenazas dirigidas a su organización. Para obtener información detallada 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 mediante un archivo de configuración BLOB.
- Ejecutar comandos desde Kaspersky Managed Detection and Response.
- Enviar datos de telemetría a Kaspersky Managed Detection and Response para la detección de amenazas.

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

- macOS 14 o versiones posteriores
- Mac con procesador Intel, Apple Silicon
- Licencia activa de Kaspersky Endpoint Security

Debe habilitar los siguientes componentes para que Managed Detection and Response funcione:

- Protección contra archivos peligrosos
- Protección contra amenazas web
- Protección contra amenazas de correo

Habilitar estos componentes no es opcional. De lo contrario, Kaspersky Managed Detection and Response no puede funcionar porque no recibirá los datos de telemetría necesarios.

Además, Kaspersky Managed Detection and Response utiliza los datos recibidos de otros componentes de la aplicación. Habilitar esos componentes es opcional. Entre los componentes que proporcionan datos adicionales están los siguientes:

- Detección de comportamiento

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 los equipos y la infraestructura del servicio en la nube de Kaspersky Security Network a través del Servidor de administración, en lugar del 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 de MDR. Puede obtener el archivo comprimido ZIP en la consola de Kaspersky Managed Detection and Response. Para obtener detalles sobre la configuración del 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 operación *"Infraestructura: Kaspersky Private Security Network"* se indicará en la configuración de directivas, en la sección Kaspersky Security Network.

   El uso de KSN Privada con Kaspersky Managed Detection and Response garantiza 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 infringir las leyes de su país.

   Importante: debe habilitar el modo extendido de KSN para que Managed Detection and Response funcione.

2. **Activar Kaspersky Managed Detection and Response**

   Puede activar el componente Managed Detection and Response en el dispositivo endpoint mediante los siguientes métodos:

   - **Activar usando un código de activación en la aplicación Kaspersky Endpoint Security**.

     1. Abrir 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**, escriba el código de activación que recibió con la compra.

        Nota: el código de activación es una combinación única de 20 números y letras latinas con el formato xxxxx-xxxxx-xxxxx-xxxxx.
     4. Haga clic en **Activar**.

        La aplicación se conecta a los servidores de activación de Kaspersky y envía el código de activación para verificar su autenticidad. Si se comprueba el código de activación correctamente, la aplicación recibe y agrega automáticamente la clave de licencia.

Nota: Según el código de activación que recibió, es posible que deba completar un formulario de registro.

Si la verificación del código de activación falla, se muestra la notificación correspondiente. En este caso, comuníquese con el proveedor de software que le proporcionó ese código de activación.

- **Activar usando el archivo BLOB**.

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

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

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Detección y respuesta** > **Managed Detection and Response**.
7. Seleccione la casilla **Habilitar Managed Detection and Response**.
8. En el bloque del **Archivo de configuración de 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 Kaspersky 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. Seleccione la pestaña **Configuración de la aplicación**.
5. Seleccione **Detection and Response** > **Managed Detection and Response**.
6. Active el conmutador de alternancia de **Managed Detection and Response**.
7. Haga clic en **Importar** y seleccione el archivo BLOB que se obtuvo en la consola de Kaspersky Managed Detection and Response. El archivo tiene la extensión .P7.
8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security verificará el archivo BLOB. La verificación del archivo BLOB incluye la verificación de la firma digital y el plazo de la licencia. Si el archivo BLOB se verifica correctamente, Kaspersky Endpoint Security cargará el archivo y lo enviará al equipo durante la próxima sincronización con Kaspersky Security Center.

- **Activar usando la tarea Agregar clave**.

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

    1. En la ventana **Seleccionar el tipo de tarea**, maximice el nodo de **Kaspersky Endpoint Security for Mac 12.2.1**.
    2. Para crear una tarea para agregar una clave, seleccione **Agregar clave**.
    3. En la ventana **Activación de la aplicación**, realice una de las siguientes acciones:
       a. Seleccione un código o clave de activación del almacenamiento de Kaspersky Security Center o agregue un archivo de claves almacenado en su equipo.
       b. Para agregar la clave determinada como una clave de reserva, seleccione la casilla **Agregar como clave de reserva**.
          La clave de reserva se activa cuando vence la clave activa actual.

       La información sobre la clave especificada (clave, tipo de clave y fecha de vencimiento de la clave) se muestra en la ventana **Activación de la aplicación**.
    4. En la ventana Seleccione los dispositivos a los que se asignará la tarea, seleccione el método que desea usar para especificar los equipos cliente:
       - Para seleccionar entre los equipos que el Servidor de administración detectó en la red, seleccione la opción **Seleccionar dispositivos de la red detectados por el Servidor de administración**.
       - Para especificar las direcciones IP de los equipos manualmente o importar las direcciones IP de los equipos desde un archivo, seleccione la opción **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**.
       - Para crear una tarea para una selección de dispositivos a partir de un criterio preestablecido, 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**.
    5. En la ventana que se abre (**Seleccionar los dispositivos**, **Selección de dispositivos** o **Seleccionar grupo de administración**, según la opción que seleccionó en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipo o seleccione el grupo de administración al que se aplicará la tarea.

       > **Nota:** este paso no es relevante para tareas locales o de grupo.

    6. En la ventana **Configurar programación de tarea**, seleccione el modo de inicio en la lista desplegable **Inicio programado**.
    7. Si es necesario, configure una tarea programada para que se inicie automáticamente (especificando la fecha y hora de inicio de la tarea).

8. Si desea ejecutar tareas que la aplicación no pudo iniciar de acuerdo con la programación (por ejemplo, porque el equipo estaba apagado a la hora programada), seleccione la casilla de verificación **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security inicia la tarea tan pronto como se elimina el obstáculo que impide que se inicie la tarea.

9. Si desea que Kaspersky Security Center determine automáticamente el intervalo entre lanzamientos de tareas en diferentes equipos, seleccione la casilla de verificación **Utilizar retardo aleatorio automático para el inicio de tareas**.

   Esto ayuda a reducir la carga en el Servidor de administración de Kaspersky Security Center.

10. Para establecer el intervalo entre el inicio de tareas en diferentes equipos de forma manual, seleccione la casilla **Utilizar un retardo aleatorio para el inicio de tareas dentro de un intervalo de (min)** y especifique la cantidad de minutos.

    Esto ayuda a reducir la carga en el Servidor de administración de Kaspersky Security Center.

11. En la ventana **Definir el nombre de la tarea**, en el campo **Nombre**, ingrese el nombre de la tarea que está creando.

1. En la ventana **Finalizar la creación de la tarea**, haga lo siguiente:

   a. Si desea que la tarea se inicie en cuanto finalice el asistente, seleccione la casilla **Ejecutar la tarea al finalizar el Asistente**.

   b. Haga clic en **Finalizar** para cerrar el asistente.

- **Activar Kaspersky Managed Detection and Response en Web Console y Cloud Console**

1. En la ventana principal de Web Console, seleccione **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 (12.2.1).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Agregar clave**.

   c. En el campo **Nombre de la tarea**, escriba 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 seleccionar 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, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración 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 DNS, direcciones IP y subredes IP de los dispositivos a los que desee 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 del personal de contaduría 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 determinada selección. Puede especificar una de las selecciones ya existentes.

  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 elegido de la tarea.
5. Seleccione la clave de licencia de la lista. Si la lista no contiene una licencia adecuada, puede agregar una nueva clave de licencia al repositorio del Servidor de administración.
6. Ingrese las credenciales de la cuenta del usuario cuyos derechos desee 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 (raíz).

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

   Si habilitó 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 programar el 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. Configure la programación de la tarea.

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

11. Haga clic en **Guardar**.

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

    a. Seleccione la casilla junto a la tarea.

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

Endpoint Detection and Response Expert (on-premise)

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 más. Para obtener información detallada 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, 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 tareas iniciadas en la interfaz web de Kaspersky Anti Targeted Attack Platform.

El componente Endpoint Detection and Response Expert (on-premise) tiene los siguientes requisitos adicionales:

- Kaspersky Anti Targeted Attack Platform 6.0 o posterior.
- La versión de Kaspersky Security Center es 14.2 o posterior.
- La integración con Endpoint Detection and Response Expert (versión 7.1 o anterior) se puede configurar en la Consola de administración de Kaspersky Security Center (MMC), en Web Console o Cloud Console.
- La integración con Endpoint Detection and Response Expert (versión 8.0 o posterior) 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 Endpoint Detection and Response (KATA) consta de los siguientes pasos:

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

   Puede seleccionar 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 por separado.

   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 el establecimiento de 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 habilitar la verificación bidireccional. Para habilitar la verificación bidireccional, debe usar un contenedor de cifrado protegido con contraseña. Para obtener información detallada sobre la descarga de un contenedor de cifrado, consulte la *Ayuda de Kaspersky Anti Targeted Attack Platform*.

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

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Detección y respuesta** > **Endpoint Detection and Response Expert (on-premise)**.
7. Seleccione la casilla **Habilitar Endpoint Detection and Response Expert (versión 7.1 o anteriores)**.
8. Haga clic en **Configuración de la conexión del servidor**.
9. En la ventana **Configuración de la conexión del servidor** que se abre, configure lo siguiente:
   - Haga clic en **Cargar certificado TLS** para seleccionar un certificado TLS que se usará 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 usar la verificación bidireccional, seleccione la casilla **Usar autenticación bidireccional**. Haga clic en **Cargar contenedor de criptomonedas** para seleccionar un archivo de contenedor de cifrado e ingrese la contraseña en el campo **Contraseña del contenedor de criptomonedas**.
10. Haga clic en **Guardar**.
11. Para agregar un servidor KATA, haga clic en **Agregar**.
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, seleccione **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. Seleccione **Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**.
5. Active el conmutador de alternancia de **Endpoint Detection and Response Expert (on-premise)**.
6. Haga clic en **Configuración de conexión**.
7. En la ventana **Configuración de conexión con el servidor** que se abre, configure lo siguiente:
   - Haga clic en **Agregar certificado TLS** para seleccionar un certificado TLS que se usará 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 usar la verificación bidireccional, seleccione la casilla **Usar autenticación bidireccional**. Haga clic en **Cargar criptocontenedor** para seleccionar un archivo de contenedor de cifrado e ingrese la contraseña en el campo **Contraseña de criptocontenedor**.
8. Haga clic en **Aceptar**.
9. Para agregar un servidor KATA, haga clic en **Agregar**.
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 de ciberamenazas avanzadas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de reaccionar ante estas para contrarrestar ataques avanzados, que incluyen nuevos exploits, ransomware, ataques sin archivos, así como tácticas que emplean 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 las amenazas y proporciona al *personal de seguridad* o al *Administrador* la información sobre el posible ataque necesaria para una respuesta oportuna. Kaspersky Endpoint Detection and Response muestra los detalles de la alerta en una ventana independiente. *Detalles de alerta* es una herramienta que permite ver toda la información que se recopiló sobre una amenaza detectada. Por ejemplo, Detalles de alerta incluye el historial de archivos que aparecen en el equipo. 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.

Configuración de Endpoint Detection and Response

Parámetro	Descripción
Aislamiento de la red	Aislamiento automático del equipo de la red en respuesta a amenazas detectadas. Cuando el aislamiento de la red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones nuevas de TCP/IP del equipo. La aplicación solo deja activas las siguientes conexiones: • Conexiones que figuran en Exclusiones del aislamiento de la red. • Conexiones iniciadas por los servicios de Kaspersky Endpoint Security. • Conexiones iniciadas por el Agente de red de Kaspersky Security Center.
Desbloquear automáticamente el equipo aislado en N horas	Aislamiento de la red se puede desactivar de forma automática después de un tiempo especificado o manualmente. De manera predeterminada, Kaspersky Endpoint Security desactiva Aislamiento de la red 8 horas después del inicio del aislamiento.
Exclusiones de aislamiento de la red	Lista de reglas para las exclusiones del aislamiento de la red. Las conexiones de red que coinciden con las reglas no se bloquean en los equipos cuando el aislamiento de la red está activado. Para configurar las exclusiones del aislamiento de la red, puede usar 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 los roles 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 la red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si Aislamiento de la red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center o en los detalles de la alerta.
Prevención de ejecución	Prevención de ejecución permite administrar el funcionamiento de archivos ejecutables y scripts, así como abrir archivos en formato Office. De esta manera, puede, por ejemplo, evitar la ejecución de aplicaciones que no considere seguras. Como resultado, se puede detener la propagación de la amenaza. Prevención de ejecución admite un conjunto de intérpretes de scripts. Para usar el componente Prevención de ejecución, debe agregar reglas de prevención de ejecución. La regla de Prevención de ejecución es un conjunto de criterios que la aplicación tiene en cuenta para reaccionar frente a la ejecución de un objeto, por ejemplo, cuando bloquea el funcionamiento de un objeto. La aplicación identifica archivos por las rutas o sumas de control que se calculan mediante algoritmos hash MD5 y SHA256.
Acción ante operaciones de ejecución o apertura de un objeto prohibido	**Bloquear y escribir 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. **Registrar solo eventos**. 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.
Cloud Sandbox	Cloud Sandbox es una tecnología que le permite detectar amenazas avanzadas en una computadora. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Cloud Sandbox para su análisis. Cloud Sandbox ejecuta estos archivos en un entorno aislado para identificar actividades maliciosas y decide sobre su reputación. Los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Cloud Sandbox detectó un archivo malicioso, Kaspersky Endpoint Security realiza la acción adecuada para eliminar esta amenaza en todos los equipos donde se detecte este archivo. **Nota:** La tecnología Cloud Sandbox siempre está 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 agregar 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 con las siguientes condiciones para que Endpoint Detection and Response funcione:

- La versión de Kaspersky Security Center es 13.2 o posterior. En versiones anteriores de Kaspersky Security Center, no es posible activar la funcionalidad de 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 ver 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 incluye esta 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 seleccionar 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 por separado.

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

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

   Puede habilitar o deshabilitar el componente en la configuración de la directiva de Kaspersky Endpoint Security for Mac.

Cómo habilitar o deshabilitar el componente Endpoint Detection and Response en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
5. Active el conmutador de alternancia de **Endpoint Detection and Response Expert (on-premise)**.
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 equipo (datos en riesgo). 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 equipo y tomar medidas de respuesta a las amenazas.

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

Modo de ejecución de la tarea Análisis de IOC

Kaspersky Endpoint Detection and Response le permite crear tareas de análisis de IOC estándar para detectar datos en peligro. La tarea estándar de Análisis de IOC es una tarea grupal o local que se crea y configura manualmente en Web Console. Las tareas se ejecutan con archivos de IOC que prepara el usuario. Si desea agregar 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:

- En Detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta que permite ver toda la información que se recopiló sobre una amenaza detectada. Por ejemplo, Detalles de alerta incluye el historial de archivos que aparecen en el equipo. 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:

1. En la ventana principal de Web Console, seleccione **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 (12.2.1).

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

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

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

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

5. En la sección **Configuración de análisis de IOC**, cargue los archivos de IOC para buscar indicadores de peligro. Puede agregar 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 en los archivos de IOC.

   > **Nota:** No se recomienda agregar ni eliminar archivos de IOC después de ejecutar la tarea. Esto puede hacer que los resultados de Análisis de IOC se muestren de forma incorrecta para ejecuciones anteriores de la tarea. Para buscar indicadores de peligro por nuevos archivos de IOC, se recomienda agregar nuevas tareas.

6. Configurar acciones al detectar un IOC:

   - **Aislar el equipo de la red**. Si esta opción está seleccionada, Kaspersky Endpoint Security aísla el equipo de la red para evitar que la amenaza se propague. Puede configurar la duración del aislamiento en Configuración del componente Endpoint Detection and Response.
   - **Mover la copia a la Cuarentena y eliminar objeto**. Si esta opción está seleccionada, Kaspersky Endpoint Security elimina el objeto malicioso que se encuentra en el equipo. Antes de eliminar el objeto, Kaspersky Endpoint Security crea una copia de seguridad en caso de que sea necesario restaurar el objeto más adelante. Kaspersky Endpoint Security mueve la copia de seguridad a Cuarentena.
   - **Ejecutar análisis de áreas críticas**. Si se selecciona esta opción, Kaspersky Endpoint Security ejecuta la tarea 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 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 alcances del análisis para los siguientes tipos de datos:

- **Procesos: ProcessItem**
- **Archivos: FileItem**
- **Puertos de la red: PortItem**
- **Cuentas de los usuarios: UserItem**
- **Tablas ARP: ArpEntryItem**
- **Hosts: SystemInfoItem**
- **Direcciones web – UrlHistoryItem**
- **Rutas – RouteEntryItem**

9. Haga clic en **Aceptar**.
10. Ingrese las credenciales de la cuenta del usuario cuyos derechos desee 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 (raíz).

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

    Si habilitó 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 programar el 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. Configure la programación de la tarea.

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

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

    a. Seleccione la casilla junto a la tarea.

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

17. De esta manera, Kaspersky Endpoint Security ejecuta la búsqueda de indicadores de compromiso en el equipo. Puede ver los resultados de la tarea en las propiedades de la tarea, en la sección **Resultados**. Puede ver la información sobre los indicadores de vulneración detectados en las propiedades de la tarea: **Configuración de la aplicación** > **Resultados del análisis de IOC**.

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

Poner archivo en cuarentena

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

Puede crear tareas *Poner archivo en cuarentena* de las siguientes maneras:

- En Detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta que permite ver toda la información que se recopiló sobre una amenaza detectada. Por ejemplo, Detalles de alerta incluye el historial de archivos que aparecen en el equipo. 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 ingresar la ruta del archivo o el hash (SHA256 o MD5), o ambos.

La tarea *Poner archivo en cuarentena* tiene las siguientes limitaciones:

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

Para crear una tarea Poner archivo en cuarentena:

1. En la ventana principal de Web Console, seleccione **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 (12.2.1).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Poner archivo en cuarentena**.

c. En el campo **Nombre de la tarea**, escriba 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 seleccionar 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, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración 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 DNS, direcciones IP y subredes IP de los dispositivos a los que desee 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 del personal de contaduría 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 determinada selección. Puede especificar una de las selecciones ya existentes.

  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 elegido 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 seleccionada en el paso anterior.

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

   Se inicia el asistente para agregar archivos.

7. En la lista desplegable **Indique el archivo para mover a Cuarentena**, seleccione una de las opciones y complete los campos obligatorios. Para agregar el archivo, debe ingresar 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. Ingrese las credenciales de la cuenta del usuario cuyos derechos desee 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 (raíz).

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

    Si habilitó 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 programar el 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. Configure la programación de la tarea.

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

14. Haga clic en **Guardar**.

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

    a. Seleccione la casilla junto a la tarea.

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

De esta manera, Kaspersky Endpoint Security mueve el archivo a cuarentena.

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

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

Obtener archivo

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

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

Para crear una tarea Obtener archivo:

1. En la ventana principal de Web Console, seleccione **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 (12.2.1).

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

   c. En el campo **Nombre de la tarea**, escriba 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 seleccionar 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, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración 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 DNS, direcciones IP y subredes IP de los dispositivos a los que desee 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 del personal de contaduría 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 determinada selección. Puede especificar una de las selecciones ya existentes.

     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 elegido de la tarea. En la ventana **Obtener archivo**, haga clic en **Agregar**.

   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 obligatorios.

   Para agregar el archivo, debe ingresar 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 agregará se muestra en la lista de archivos.

7. Haga clic en **Siguiente**.

8. Ingrese las credenciales de la cuenta del usuario cuyos derechos desee 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 (raíz).

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

   Si habilitó 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 programar el 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. Configure la programación de la tarea.

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

13. Haga clic en **Guardar**.

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

    a. Seleccione la casilla junto a la tarea.

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

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

Eliminar 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, seleccione **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 (12.2.1).

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

c. En el campo **Nombre de la tarea**, escriba 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 seleccionar 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, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración 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 DNS, direcciones IP y subredes IP de los dispositivos a los que desee 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 del personal de contaduría 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 determinada selección. Puede especificar una de las selecciones ya existentes.

  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 elegido de la tarea.

5. En la lista desplegable **Especifique qué archivo desea eliminar**, seleccione una de las opciones y complete los campos obligatorios. Para agregar el archivo, debe ingresar 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. Ingrese las credenciales de la cuenta del usuario cuyos derechos desee 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 (raíz).

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

   Si habilitó 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 programar el 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. Configure la programación de la tarea.

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

12. Haga clic en **Guardar**.

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

    a. Seleccione la casilla junto a la tarea.

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

De esta manera, Kaspersky Endpoint Security elimina el archivo del equipo. Si el archivo está bloqueado por un proceso diferente, la tarea se muestra como *Completada*, pero el archivo en sí se elimina después de reiniciar el equipo. Después de reiniciar el equipo, confirme que el archivo se haya eliminado.

La tarea *Eliminar archivo* puede finalizar con el error *Acceso denegado* si intenta eliminar un archivo ejecutable que se está ejecutando actualmente. Cree una tarea Finalizar proceso para el archivo y vuelva a intentarlo.

Iniciar proceso

Puede ejecutar archivos de manera remota mediante la tarea *Iniciar proceso*.

Importante: Puede configurar la tarea de EDR Optimum en Web Console.

Para crear una tarea Iniciar proceso:

1. En la ventana principal de Web Console, seleccione **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 (12.2.1).

   b. En la lista desplegable **Tipo de tarea**, seleccione **Iniciar proceso**.

   c. En el campo **Nombre de la tarea**, escriba 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 seleccionar 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, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración 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 DNS, direcciones IP y subredes IP de los dispositivos a los que desee 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 del personal de contaduría 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 determinada selección. Puede especificar una de las selecciones ya existentes.

  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 elegido 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 seleccionada 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 la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó 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 programar el 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. Configure la programación de la tarea.

> **Nota:** Asegúrese de que el equipo esté encendido para ejecutar la tarea.

11. Haga clic en **Guardar**.
12. Para ejecutar la tarea de inmediato independientemente de la programación configurada, haga lo siguiente:
    a. Seleccione la casilla junto a la tarea.
    b. 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 en la sección **Resultados de la ejecución**.

Finalizar proceso

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 Prevención de ejecución. Puede prohibir la ejecución de archivos ejecutables, scripts, archivos de formato de Office.

La tarea de *Finalizar proceso* tiene las siguientes limitaciones:

- Puede configurar la tarea únicamente para EDR Optimum en Web Console.

Para crear una tarea Finalizar proceso:

1. En la ventana principal de Web Console, seleccione **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 (12.2.1).
   b. En la lista desplegable **Tipo de tarea**, seleccione **Finalizar proceso**.
   c. En el campo **Nombre de la tarea**, escriba 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 seleccionar 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, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración 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 DNS, direcciones IP y subredes IP de los dispositivos a los que desee 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 del personal de contaduría 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 determinada selección. Puede especificar una de las selecciones ya existentes.

  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 elegido 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 seleccionada 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 ingresar 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. Ingrese las credenciales de la cuenta del usuario cuyos derechos desee 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 (raíz).

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

   Si habilitó 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 programar el 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. Configure la programación de la tarea.

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

13. Haga clic en **Guardar**.

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

    a. Seleccione la casilla junto a la tarea.

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

    De esta manera, Kaspersky Endpoint Security finaliza el proceso en el equipo. Por ejemplo, si se está ejecutando una aplicación *Juego* y finaliza el proceso *Juego*, la aplicación se cierra sin guardar los datos. Puede ver los resultados de la tarea en las propiedades de la tarea, en la sección **Resultados**.

Prevención de ejecución

Prevención de ejecución permite administrar el funcionamiento de archivos ejecutables y scripts, así como abrir archivos en formato Office. De esta manera, puede, por ejemplo, evitar la ejecución de aplicaciones que no considere seguras. 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 para reaccionar frente a la ejecución de un objeto, por ejemplo, cuando bloquea el funcionamiento de un objeto. La aplicación identifica archivos por las rutas o sumas de control que se calculan mediante algoritmos hash MD5 y SHA256.

Puede crear reglas de Prevención de ejecución:

- En Detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta que permite ver toda la información que se recopiló sobre una amenaza detectada. Por ejemplo, Detalles de alerta incluye el historial de archivos que aparecen en el equipo. 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 ingresar la ruta del archivo o el hash (SHA256 o MD5), o ambos.

También puede administrar la 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 necesitan para ejecutarse.

Modos de la regla de Prevención de ejecución

El componente 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: Puede definir la configuración del componente solo en Web Console.

Para prevenir ejecuciones:

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.

   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 conmutador de alternancia **Prevención de ejecución**.
6. En el bloque **Acción ante operaciones de ejecución o apertura de un objeto prohibido**, seleccione el modo de funcionamiento del componente:

   - **Bloquear y escribir 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.

   - **Registrar solo eventos**. 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, ingrese el nombre de la regla de prevención de ejecución (por ejemplo, Aplicación A).

   c. En la lista desplegable **Tipo**, seleccione el objeto que desee bloquear: **Aplicación**, **Script** o **Documento**.

   Si selecciona un tipo de objeto incorrecto, Kaspersky Endpoint Security no bloquea el archivo o el script.

   d. Para agregar el archivo, debe ingresar el hash del archivo (SHA256 o MD5), la ruta completa al archivo o ambos.

> **Nota:** Si el archivo está ubicado en una unidad de red, ingrese la ruta del archivo de la siguiente manera: /Volúmenes/nombre_carpeta_compartida/nombre_archivo. Si la ruta del archivo contiene una letra de la unidad de la red, Kaspersky Endpoint Security no bloquea el archivo o el script.

   a. Haga clic en **Aceptar**.

8. Guarde los cambios.

Como resultado, Kaspersky Endpoint Security bloquea la ejecución de objetos: la ejecución de archivos ejecutables y scripts, la apertura de archivos con formato de Office. Sin embargo, puede, por ejemplo, abrir un archivo de script en un editor de texto 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 habilitadas en la configuración de la aplicación.

Aislamiento de la red informática

El aislamiento de la red informática permite aislar automáticamente un equipo de la red en respuesta a la detección de un indicador de peligro (IOC); este es el modo automático. Puede activar el aislamiento de la red manualmente mientras investiga la amenaza detectada; este es el modo manual.

Cuando el aislamiento de la red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones de red TCP/IP nuevas en el equipo, excepto las siguientes conexiones:

- Conexiones que figuran en Exclusiones del aislamiento de la red.
- Conexiones iniciadas por los servicios de Kaspersky Endpoint Security.
- Conexiones iniciadas por el Agente de red de Kaspersky Security Center.

> **Importante:** Puede definir la configuración del componente solo en Web Console.

Modo automático de aislamiento de la red

Puede configurar el aislamiento de la red para que se active automáticamente en respuesta a la detección de un IOC. Puede configurar el modo automático de aislamiento de la red con una directiva de grupo.

Cómo configurar el aislamiento de la red para que se active automáticamente en respuesta a la detección de un IOC

1. En la ventana principal de Web Console, seleccione **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. Seleccione la pestaña **Configuración de la aplicación**.
5. En el bloque **Acción al detectar un IOC**, seleccione la opción **Alertar y tomar medidas de respuesta después de que se encuentra un IOC** y luego la casilla **Aislar el equipo de la red (8 horas)**.
6. Guarde los cambios.
7. Como resultado, cuando se detecta un IOC, la aplicación aísla el equipo de la red para evitar la propagación de la amenaza.

Puede configurar el aislamiento de la red para que se desactive automáticamente después de que transcurra un período específico. De manera predeterminada, la aplicación desactiva el aislamiento de la red una vez que hayan transcurrido 8 horas desde el momento en que se activó. También puede desactivarlo manualmente (consulte las instrucciones a continuación). Después de desactivar el aislamiento de la red, el equipo puede usar la red sin restricciones.

Cómo configurar la demora en desactivar el aislamiento de red de un equipo en modo automático

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
5. En el bloque **Aislamiento de la red**, haga clic en **Establezca la configuración del desbloqueo del equipo**.
6. En la ventana que se abre, seleccione la casilla **Desbloquear automáticamente el equipo aislado en** e ingrese la demora en desactivar automáticamente el aislamiento de la red.
7. Guarde los cambios.

Modo manual de aislamiento de la red

Puede activar y desactivar manualmente el aislamiento de la red. Puede configurar el modo de Aislamiento de la red manual mediante las propiedades del equipo en la consola de Kaspersky Security Center.

Puede activar el aislamiento de la red:

- En Detalles de alerta (solo para EDR Optimum).

  Detalles de alerta es una herramienta que permite ver toda la información que se recopiló sobre una amenaza detectada. Por ejemplo, Detalles de alerta incluye el historial de archivos que aparecen en el equipo. 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 el aislamiento de la red de un equipo manualmente

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Dispositivos administrados**.
2. Seleccione el equipo para el que desee definir la configuración de la aplicación local.

   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Aplicaciones**.
4. Haga clic en **Kaspersky Endpoint Security for Mac**.

   Se abre la configuración de la aplicación local.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
7. En el bloque **Aislamiento de la red**, haga clic en **Aislar el equipo de la red**.

Puede configurar el aislamiento de la red para que se desactive automáticamente después de que transcurra un período específico. De manera predeterminada, la aplicación desactiva el aislamiento de la red una vez que hayan transcurrido 8 horas desde el momento en que se activó. Después de desactivar el aislamiento de la red, el equipo puede usar la red sin restricciones.

Cómo configurar la demora en desactivar el aislamiento de red de un equipo en modo manual

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Dispositivos administrados**.
2. Seleccione el equipo para el que desee definir la configuración de la aplicación local.

   Se abren las propiedades del equipo.
3. Seleccione la pestaña **Tareas**.

   Se muestra la lista de tareas disponibles en el equipo.
4. Seleccione la tarea **Aislamiento de la red**.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. En la ventana que se abre, seleccione la demora en desactivar el aislamiento de la red.
7. Guarde los cambios.

Cómo desactivar el aislamiento de la red de un equipo manualmente

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Dispositivos administrados**.
2. Seleccione el equipo para el que desee definir la configuración de la aplicación local.
3. Se abren las propiedades del equipo.
4. Seleccione la pestaña **Aplicaciones**.
5. Haga clic en Kaspersky Endpoint Security for Mac.
6. Se abre la configuración de la aplicación local.
7. Seleccione la pestaña **Configuración de la aplicación**.
8. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
9. En el bloque de **Aislamiento de la red**, haga clic en **Desbloquear el equipo aislado de la red**.

También puede deshabilitar el aislamiento de la red localmente con la línea de comandos.

Exclusiones de aislamiento de la red

Puede configurar exclusiones del aislamiento de la red. Las conexiones de red que coinciden con las reglas no se bloquean en el equipo cuando el aislamiento de la red está activado.

Para configurar las exclusiones del aislamiento de la red, puede usar 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 los roles 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 la red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si Aislamiento de la red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center.

Nota: Una directiva activa no impide aplicar las exclusiones del aislamiento de la red configuradas en las propiedades del equipo, ya que estos parámetros tienen diferentes escenarios de uso.

Cómo agregar una exclusión de aislamiento de la red en modo automático

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.
3. Se abre la ventana de propiedades de la directiva.
4. Seleccione la pestaña **Configuración de la aplicación**.

5. Vaya a **Detection and Response** > **Endpoint Detection and Response**.

6. En el bloque **Exclusiones de aislamiento de la red**, haga clic en **Exclusiones**.

7. En la siguiente ventana, haga clic en **Agregar del perfil** y seleccione los perfiles de red estándar para configurar las exclusiones.

8. Las exclusiones de aislamiento de la red del perfil se agregan a la lista de exclusiones de aislamiento de la red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de la conexión de red.

9. Si es necesario, agregue una exclusión de aislamiento de la red manualmente. Para hacerlo, en la ventana con la lista de exclusiones, haga clic en **Agregar** y edite manualmente la configuración de la conexión de red.

10. Guarde los cambios.

Cómo agregar una exclusión de aislamiento de red en modo manual

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Dispositivos administrados**.

2. Seleccione el equipo para el que desee definir la configuración de la aplicación local.

3. Se abren las propiedades del equipo.

4. Seleccione la pestaña **Tareas**.

5. Se muestra la lista de tareas disponibles en el equipo.

6. Seleccione la tarea **Aislamiento de la red**.

7. Seleccione 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 **Agregar del perfil** y seleccione los perfiles de red estándar para configurar las exclusiones.

10. Las exclusiones de aislamiento de la red del perfil se agregan a la lista de exclusiones de aislamiento de la red. Puede ver las propiedades de las conexiones de red. Si es necesario, puede modificar la configuración de la conexión de red.

11. Si es necesario, agregue una exclusión de aislamiento de la red manualmente. Para hacerlo, en la ventana con la lista de exclusiones, haga clic en **Agregar** y edite manualmente la configuración de la conexión de red.

12. Guarde los cambios.

También puede ver la lista de exclusiones de aislamiento de la red localmente mediante la línea de comandos. En este caso, el equipo debe estar aislado.

Cloud Sandbox

Cloud Sandbox es una tecnología que le permite detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Cloud Sandbox para su análisis. Cloud Sandbox ejecuta estos archivos en un entorno aislado para identificar actividades maliciosas y decide sobre su reputación. Los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Cloud Sandbox detecta un archivo malicioso, Kaspersky Endpoint Security realizará la acción adecuada para eliminar la amenaza en todos los equipos donde se detecte el archivo.

Importante: Para que Cloud Sandbox funcione, debe habilitar el uso de Kaspersky Security Network.

Nota: Si utiliza Kaspersky Private Security Network, la tecnología de Cloud Sandbox no está disponible.

Para habilitar Cloud Sandbox:

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Configuración de agentes integrados** → **Endpoint Detection and Response**.
5. Seleccione la pestaña **Cloud Sandbox**.
6. Active el conmutador de **Cloud Sandbox**.
7. Guarde los cambios.

Siempre que exista una amenaza, Kaspersky Endpoint Security activa el contador de amenazas detectadas mediante Cloud Sandbox en la ventana principal de la aplicación, en la sección **Detección de amenazas**. Kaspersky Endpoint Security también indicará la tecnología de detección de amenazas Cloud Sandbox en el Informe sobre amenazas de la consola de Kaspersky Security Center.

Cifrado de disco FileVault

Kaspersky Endpoint Security permite que el cifrado de FileVault se administre de forma remota. El cifrado evita que usuarios no autorizados accedan a datos confidenciales almacenados en el disco de inicio del equipo del usuario.

Cuando un administrador inicia el cifrado de FileVault en un equipo desde Kaspersky Security Center, Kaspersky Endpoint Security solicita a un usuario de este equipo que ingrese sus credenciales. El cifrado de disco se inicia solo después de que el usuario proporciona las credenciales, el equipo se reinicia y pasaron 30 minutos desde que se recibió la configuración de la directiva en el equipo. El intervalo mínimo entre las solicitudes de credenciales también es de 30 minutos.

Para evitar que el usuario descifre el disco de inicio de la Mac cuando el cifrado de FileVault está habilitado, un administrador debe usar JAMF para implementar un perfil de MDM que prohíba el descifrado de disco. Para descifrar el disco de inicio de una Mac con un perfil de MDM que prohíbe el descifrado de disco, el administrador primero debe eliminar el perfil.

Nota: Si la administración de cifrado de FileVault no está habilitada en Kaspersky Security Center, los usuarios con derechos de administrador pueden cifrar y descifrar sus discos de inicio de Mac desde Configuración 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 usuario que ingresó sus credenciales.

Permitir a otros usuarios desbloquear el disco

1. Elija el **menú Apple** > **Configuración del sistema** > **Privacidad y seguridad**.
2. Haga clic en **FileVault**.
   Se abre la ventana **FileVault**.
3. Haz clic en **Habilitar usuarios**.
4. En la ventana que se abre, seleccione un usuario para autorizar el desbloqueo del equipo.
5. Ingrese 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, Web Console o Cloud Console de Kaspersky Security Center y un usuario de este equipo 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 con la Consola de administración de Kaspersky Security Center

Cómo obtener una clave de recuperación con 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 habilitada, Kaspersky Endpoint Security exige una contraseña al intentar 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 desinstalador.

- Restaurar archivos en cuarentena desde Copia de seguridad
- Ver informes.

Deshabilitar la protección con contraseña no deshabilita la configuración de la directiva. Si la directiva prohíbe la edición de una configuración, no podrá editarla aunque la protección con contraseña esté deshabilitada.

Habilitar Protección con contraseña mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Configuración adicional > Interacción con el usuario**.
7. En la sección **Protección con contraseña**, seleccione la casilla **Habilitar protección con contraseña**.
8. En la ventana **Configuración de la protección con contraseña** que se abre, configure lo siguiente:
   - Ingrese la contraseña en el campo **Contraseña** y vuelva a ingresarla en el campo **Confirmar contraseña**.
   - En la sección **Solicitar contraseña para**, seleccione las casillas necesarias para proteger las acciones correspondientes en el dispositivo del usuario.
9. Haga clic en **Aceptar** para guardar los cambios.
10. Siga uno de estos procedimientos 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.

Editar la configuración de Protección con contraseña mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **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 desee cambiar.
9. Haga clic en **Aceptar** para guardar los cambios.

Habilitar Protección con contraseña mediante Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
3. Se abre la ventana de propiedades de la directiva.
4. Seleccione la pestaña **Configuración de la aplicación**.
5. Seleccione **Configuración adicional** > **Interacción con el usuario**.
6. Active el conmutador de **rotección con contraseña**.
7. En la ventana **Configuración de la protección con contraseña** que se abre, configure lo siguiente:
   - Ingrese la contraseña en el campo **Contraseña** y vuelva a ingresarla en el campo **Confirmar contraseña**. De forma predeterminada, los caracteres de la contraseña se ocultan por razones de seguridad. Para ver la contraseña, haga clic en **Mostrar**.
   - En la sección **Solicitar contraseña para**, seleccione las casillas necesarias 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 Protección con contraseña mediante Web Console

1. En la ventana principal de Web Console, seleccione **Dispositivos** > **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security for Mac.
3. Se abre la ventana de propiedades de la directiva.
4. Seleccione la pestaña **Configuración de la aplicación**.
5. Seleccione **Configuración adicional** > **Interacción con el usuario**.
6. En la sección **rotección 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 desee 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.

Habilitar Protección con contraseña mediante la aplicación Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Protección con contraseña**, seleccione la casilla **Habilitar protección con contraseña**.

3. En la ventana que se abre, configure lo siguiente:

   - Ingrese la contraseña en el campo **Contraseña** y vuelva a ingresarla en el campo **Confirmar contraseña**.

   - En la sección **Solicitar contraseña para**, seleccione las casillas necesarias 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, deberá ingresar la contraseña dos veces para cambiar la configuración de Protección con contraseña.

Editar Protección con contraseña mediante la aplicación Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Protección con contraseña**, haga clic en **Configuración**.

3. En la ventana que se abre, edite la configuración que desee 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 código malicioso. Como resultado de este ataque, el exploit puede iniciar una instalación no autorizada de malware. Cuando se detecta que una aplicación vulnerable ha intentado iniciar un archivo ejecutable y se determina que la orden no provino del usuario, Kaspersky Endpoint Security bloquea la ejecución del archivo o le muestra una notificación al usuario.

De manera predeterminada, la Prevención de exploits está habilitada. Puede deshabilitar la Prevención de exploits si es necesario.

Habilitar/deshabilitar la Prevención de exploits mediante Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Prevención de exploits**.
5. Habilite o deshabilite el componente usando el conmutador **Prevención de exploits**.
6. Si la Prevención de exploits está habilitada, seleccione una de las siguientes acciones que se realizarán cuando se detecte un exploit:

   - **Bloquear**

     Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.

   - **Informar**

     Si se selecciona este elemento, cuando Kaspersky Endpoint Security detecta un exploit, registra una entrada que contiene información sobre el exploit y agrega información sobre él a la lista de amenazas activas.
7. Guarde los cambios.

Habilitar/deshabilitar la Prevención de exploits mediante la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Protección avanzada contra amenazas** > **Prevención de exploits**.
7. Seleccione o anule la selección de la casilla **Habilitar Aprovechar prevención**.
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. Siga uno de estos procedimientos 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.

Habilitar/deshabilitar la Prevención de exploits mediante la aplicación Kaspersky Endpoint Security

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Avanzado**, en la sección Prevención de exploits, seleccione o anule la selección de la casilla Habilitar Aprovechar prevención.

3. Si la casilla **Habilitar 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 malware que presente un peligro**

     Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.

   - **Informar**

     Si se selecciona este elemento, cuando Kaspersky Endpoint Security detecta un exploit, registra una entrada que contiene información sobre el exploit y agrega 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 abrirá la ventana **Informes**.

2. Abra la pestaña **Prevención de exploits**.

Motor de reparación

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

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

- **Actividad de archivos**

  Kaspersky Endpoint Security realiza las siguientes acciones:

  - Elimina 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 la 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 equipo.

Habilitar/deshabilitar el Motor de reparación en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Protección avanzada contra amenazas** > **Motor de reparación**.
7. Seleccione o anule la selección de la casilla **Habilitar Motor de reparación**.
8. Haga clic en **Aceptar** para guardar los cambios.
9. Siga uno de estos procedimientos 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.

Habilitar/deshabilitar el Motor de reparación en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Motor de reparación**.

5. Habilite o deshabilite el componente usando el conmutador **Motor de reparación**.

6. Guarde los cambios.

Habilitar/deshabilitar el Motor de reparación en la interfaz de la aplicación

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Avanzado**, en la sección **Motor de reparación**, seleccione o anule la selección de la casilla Habilitar Motor de reparación.

De esta manera, si la opción Motor de reparación está habilitada, Kaspersky Endpoint Security revertirá las acciones realizadas por aplicaciones maliciosas en el sistema operativo.

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 **Verificar conexiones seguras (HTTPS)** en la sección **Esencial** de la pestaña **General**.

Agregar una nueva regla en la Consola de administración

1. Inicie la Consola de administración.

2. Maximice el nodo del **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 ficha **Directivas**.

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

6. En la ventana **Propiedades**, seleccione **Controles de seguridad** > **Control web**.

7. Seleccione la casilla **Habilitar Control web**.

8. Haga clic en **Agregar**.

9. En la ventana que se abre, ingrese el nombre de una regla.

10. Si desea que la regla esté activa, seleccione la casilla **Regla activa**.

11. Realice una de las siguientes acciones:

    - Si desea que la regla se aplique a direcciones web específicas, seleccione la opción **Dirección web o un grupo de direcciones web por máscara**.
    - Si desea que la regla se aplique a categorías específicas de sitios web, seleccione 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, seleccione la opción **Bloquear**.
    - Si desea que Kaspersky Endpoint Security permita el acceso, seleccione la opción **Permitir**.
    - Si desea que Kaspersky Endpoint Security muestre una advertencia, seleccione la opción **Mostrar advertencia**.

15. Haga clic en **Aceptar** para guardar los cambios.
16. Siga uno de estos procedimientos 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.

Agregar una nueva regla en Web Console

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la 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, ingrese el nombre de una regla.
8. Realice una de las siguientes acciones:

    - Si desea que la regla esté activa, seleccione la opción **Activa**.
    - Si desea que la regla esté inactiva, seleccione la opción **Inactiva**.

9. Realice una de las siguientes acciones:

    - Si desea que Kaspersky Endpoint Security permita el acceso, seleccione la opción **Permitir**.
    - Si desea que Kaspersky Endpoint Security bloquee el acceso, seleccione la opción **Bloquear**.
    - Si desea que Kaspersky Endpoint Security muestre una advertencia, seleccione la opción **Mostrar advertencia**.

10. Realice una de las siguientes acciones:

    - Si desea que la regla se aplique a categorías específicas de sitios web, seleccione la opción **Categorías** y haga clic en **Seleccione las categorías** para seleccionar las categorías.
    - Si desea que la regla se aplique a direcciones web específicas, seleccione la opción **Direcciones individuales** y agréguelas 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 equipo. Esto le permite proteger el equipo 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**. Puede controlar el acceso a discos duros, discos extraíbles, disquetes, unidades de CD/DVD y el acceso a redes Wi-Fi.

  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 agregar dispositivos de confianza en función 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 mediante las herramientas del sistema operativo. Ejemplo de Id. de dispositivo: SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000. Agregar dispositivos por Id. es conveniente si desea agregar 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 ingresar el VID y PID: VID_1234&PID_5678. Agregar dispositivos por modelo es conveniente si usa dispositivos de un determinado modelo en su organización. De esta manera, puede agregar todos los dispositivos de este modelo.

- **Dispositivos por máscara de Id**. Si está usando varios dispositivos con Id. similares, puede agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` reemplaza cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al ingresar 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 agregar dispositivos a la lista de confianza mediante las máscaras. El carácter `*` reemplaza cualquier conjunto de caracteres. Kaspersky Endpoint Security no admite el carácter `?` al ingresar una máscara. Por ejemplo, `VID_05AC&PID_*`.

Administrar el componente Control de dispositivos en la Consola de administración

1. Inicie la Consola de administración.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades**, seleccione **Controles de seguridad** > **Control de dispositivos**.
7. Seleccione la casilla **Habilitar 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. Siga uno de estos procedimientos 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, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la 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 habilitado, la aplicación transmite información sobre los dispositivos conectados a Kaspersky Security Center. Puede ver la lista de dispositivos conectados en Kaspersky Security Center en la carpeta **Avanzado → Repositorios → Hardware**.

Ver el informe de Control de dispositivos

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

   Se abrirá la ventana **Informes**.
2. Abra la pestaña **Control de dispositivos**.

Participar 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 expreso.

La participación en Kaspersky Security Network es voluntaria. La decisión de participar se toma al instalar la aplicación. No obstante, posteriormente puede cambiar su decisión en cualquier momento.

Habilitar Kaspersky Security Network

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **KSN**, en la sección **Avanzado**, haga clic en **Mostrar la Declaración de KSN** para ver la Declaración de Kaspersky Security Network.

3. Si desea que Kaspersky Endpoint Security utilice la información sobre la reputación de los archivos, los recursos web y las aplicaciones que recibe de Kaspersky Security Network y acepta todos los términos de la Declaración, seleccione la casilla **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 **Habilitar el modo KSN extendido**.

Nota: de forma predeterminada, Kaspersky Endpoint Security utiliza el modo ampliado de KSN. El *Modo ampliado de KSN* es un modo en el que Kaspersky Endpoint Security envía datos adicionales a Kaspersky. Si no desea proporcionar estos datos a Kaspersky, desactive la casilla **Habilitar el modo KSN extendido**.

Datos proporcionados a Kaspersky mediante Kaspersky Security Network

Si la casilla **Participar en Kaspersky Security Network** está seleccionada y la casilla **Habilitar el modo KSN extendido** no está seleccionada, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

- Versión completa del Software instalado;
  tipo del Software instalado;
  identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del

servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador único del dispositivo; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

Si las casillas **Participar en Kaspersky Security Network** y **Habilitar el modo KSN extendido** están seleccionadas, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información acerca de la versión del sistema operativo (SO) y los paquetes de servicio instalados en la computadora, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo de kernel del SO, y los parámetros del modo de ejecución del SO; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada de 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 del procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactivo; cantidad de eventos de acción procesados del SO; 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 del procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento del evento recurrente; 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 de una acción en el SO.

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

- Información acerca de la aplicación del Titular de los derechos que se instaló y acerca del estado de protección antivirus: identificador de la instalación (PCID) del software; 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 del Software instalado; identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); 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; identificador de actualización del Software; tipo del Software instalado; fecha y hora de inicio de la Vigía proactiva; fecha y hora de instalación del software; probabilidad de que la Vigía proactiva envíe estadísticas; código del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo máximo permitido para el procesamiento de un evento por parte de la Vigía proactiva; tiempo de procesamiento del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por la Vigía proactiva.

- Información sobre todos los objetos y operaciones analizados: veredicto del software sobre el 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 la Vigía proactiva; fecha y hora de detección de software por la Vigía proactiva; características de detección; identificador del registro desencadenado en las bases de datos antivirus del software; motivo por el que la Vigía proactiva detectó el software; 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 desencadenado de las bases de datos antivirus del software; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; las direcciones URL y del referido desde las que se descargó; el tamaño de los archivos analizados y la ruta 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 empacador (si se empacó el archivo); 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 valor de la suma de control complementaria del objeto; datos acerca de la firma digital del objeto (certificado): 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 de firma del archivo; el nombre, el tipo, el tipo de identificador, la suma de comprobación (MD5) y el tamaño de la aplicación que cargó el objeto que se está validando; la ruta de la aplicación y las rutas de las plantillas; un atributo que indique la presencia en la Lista de ejecución automática; la fecha de entrada; la lista de atributos; el nombre del empaquetador; la información acerca de la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME, la fecha y la 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 empaquetador (si el archivo estaba empaquetado), 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 inició 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 del solicitud 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 empaquetadores (si se empaquetó el archivo); la información sobre la disponibilidad y validez de estas estadísticas; el identificador del modo para generar las estadísticas que se envían.

- Si se detectan amenazas o vulnerabilidades, además de la información sobre el objeto detectado, se proporciona información sobre el identificador, la versión y el tipo de registro en la base de datos antivirus, el nombre de la amenaza según la clasificación de Kaspersky, la fecha y hora de la última actualización de la base de datos antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de la aplicación que solicitó la URL donde se detectó la amenaza, la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador de vulnerabilidad y su nivel de amenaza, la URL y el referente de la página web donde se detectó la vulnerabilidad.

- Si se detecta un posible objeto malicioso, la información acerca de los datos se proveerá en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo atacante y número del puerto en la computadora del usuario al que ataca la red, identificador del protocolo de ataque, nombre y tipo de ataque.

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

- Las direcciones URL e IP de la página web en la que se detectó contenido dañino o sospechoso; el nombre, el tamaño y la suma de comprobación del archivo que solicitó la dirección URL; el identificador, el peso y el grado de la regla utilizada para llegar a un veredicto, el objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: estado de terminación de la tarea de actualización, tipo de error que puede ocurrir durante el proceso de actualización, cantidad de actualizaciones con errores, identificador del componente de la aplicación que realiza actualizaciones.

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

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se detectó el evento, tipo y categoría del evento, nombre del origen del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la que se solicita la reputación y la referencia, el 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 analizado (MD5), el tipo de amenaza detectada, la información sobre el registro usado para detectar una amenaza (el identificador de registro para la base de datos del antivirus y el tipo y la marca de tiempo del registro); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

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

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

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

- Información sobre el dispositivo: ID de dispositivo.

- Información sobre el funcionamiento del componente Control web:
versión del componente, motivo de categorización, información adicional sobre el motivo de la categorización, URL categorizada, dirección IP del host del objeto bloqueado o 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 lo notifica cuando cambia de Kaspersky Private Security Network a Kaspersky Security Network y le solicita que acepte los términos 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 admite 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 a Kaspersky información sobre los objetos detectados en el equipo del usuario para que los analistas de Kaspersky les realicen un análisis más profundo y se incluyan 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 u otras aplicaciones de Kaspersky obtener acceso a las bases de datos de reputación de Kaspersky Security Network y a 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 cualquiera de los siguientes motivos:
  - Las estaciones de trabajo locales no están conectadas a Internet.
  - La transmisión de cualquier dato fuera del país o fuera de la LAN corporativa está prohibida por ley o restringida por políticas de seguridad corporativas.

De forma predeterminada, Kaspersky Security Center usa 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 consultar KSN y enviar información a KSN incluso sin acceso directo a Internet.
- El servicio de proxy de KSN almacena en caché los datos procesados, lo que reduce la carga en el canal de comunicación de la red externa y acelera la recepción de la 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 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 con otros archivos que contienen código malicioso. Para evitarlo, Kaspersky Endpoint Security puede comprobar la integridad de los componentes de la aplicación. La aplicación comprueba los módulos y los 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 aplicación comprueba los módulos y los 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 ubicada 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 verificar 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`: no se confirma la integridad de los archivos (el código de retorno no es `0`)

Administración de la aplicación a través de la Consola de administración de Kaspersky Security Center

Kaspersky Security Center se diseñó para la administración centralizada de la seguridad de la red corporativa. 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.

Implemente Kaspersky Endpoint Security en una red corporativa

1. Implemente el *Servidor de administración* en la red.

   El Servidor de administración es un componente de Kaspersky Security Center que almacena de manera centralizada información sobre todas las aplicaciones de Kaspersky que están instaladas dentro de la red corporativa para administrar estas aplicaciones.

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 proporciona 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 instalado en los 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 dedicado que proporciona una interfaz para administrar las 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. Instale el Agente de red en equipos Mac remotos de una de las siguientes maneras:

   - De forma local
   - De forma remota, a través de Apple Remote Desktop
   - De forma remota a través de Kaspersky Security Center
   - De forma remota, con el protocolo SSH

   Nota: Para administrar Kaspersky Endpoint Security for Mac 12.2.1 a través de Kaspersky Security Center, debe instalar el Agente de red versión 15 en los equipos remotos.

5. Instale Kaspersky Endpoint Security en equipos Mac remotos de una de las siguientes maneras:

   - De forma local
   - De forma remota, a través de Apple Remote Desktop
   - De forma remota, con el protocolo SSH
   - De forma remota a través de Kaspersky Security Center

   Importante: Si Kaspersky Internet Security for Mac o un software antimalware de terceros está instalado en equipos remotos, desinstálelos antes de instalar Kaspersky Endpoint Security.

Para obtener información detallada sobre cómo implementar el Servidor de administración e instalar la Consola de administración, consulte la Ayuda de Kaspersky Security Center.

Actualice Kaspersky Endpoint Security versión 11.1 o posterior a la versión 12.2.1

Nota: Para administrar Kaspersky Endpoint Security for Mac 12.2.1 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 12.2.1 de una de las siguientes maneras:

- Actualice simultáneamente Kaspersky Endpoint Security a la versión 12.2.1 y el Agente de red a la versión 15 en los equipos remotos.
- Actualice primero el Agente de red a la versión 15 y, luego, actualice Kaspersky Endpoint Security a la versión 12.2.1.

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

- Para actualizar Kaspersky Endpoint Security a la versión 12.2.1, se necesita macOS 14 o posterior.
- Debe descargar el archivo KES_11.3_profile.zip del sitio web de Soporte técnico para aplicar el nuevo perfil de configuración.
- Después de actualizar Kaspersky Endpoint Security a la versión 12.2.1, 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 12.2.1, debe desinstalar la aplicación y actualizar macOS a la versión 14 o posterior. Luego, puede instalar Kaspersky Endpoint Security versión 12.2.1.

Nota: La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antimalware y 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 requisito indispensable para la instalación de Kaspersky Endpoint Security a través de Kaspersky Security Center.

Instale el complemento de administración de Kaspersky Endpoint Security

El complemento de administración de Kaspersky Endpoint Security proporciona una interfaz para administrar Kaspersky Endpoint Security a través de la Consola de administración.

Instale el 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 con los archivos del paquete de instalación de Kaspersky Endpoint Security.
3. Haga doble clic en klcfginst.exe.

Se inicia 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 en la estación de trabajo del administrador de Kaspersky Security Center.

Instale el Agente de red localmente

El Agente de red coordina la interacción entre el Servidor de administración y Kaspersky Endpoint Security instalado en los equipos dentro de la red corporativa.

Instale el Agente de red localmente

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 abre una ventana con el contenido del kit de distribución.
3. En la ventana con el contenido del kit de distribución, haga doble clic en **Agente de red de Kaspersky**.

4. Confirme que desea instalar el Agente de red haciendo clic en **Continuar**.
5. En la ventana **Introducción**, 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. Haga lo siguiente:
   - Para aceptar todos los términos del contrato y continuar con la instalación, haga clic en **Continuar**.
   - Para imprimir el texto del contrato, haga clic en **Imprimir**.
   - Para guardar el contrato como un 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 al 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 **Configuración**, haga lo siguiente:
   a. En el campo **Servidor**, especifique la dirección IP o el nombre DNS del servidor en el que está instalado Kaspersky Security Center.
   b. En el campo **Puerto**, especifique el número de puerto para una conexión no cifrada al servidor.
   c. En el campo **Puerto SSL**, especifique el número de puerto para una conexión SSL al servidor.
   d. Si desea iniciar 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 al servidor, desmarque la casilla de verificación **Usar SSL**. Para continuar 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 con la configuración recomendada, haga clic en **Instalar** e ingrese la contraseña de administrador para confirmar su elección.

   Espere hasta que el instalador del Agente de red termine de instalar los componentes de la aplicación.
10. Haga clic en **Cerrar** para salir del instalador.

Instale el Agente de red con Apple Remote Desktop

1. En un equipo remoto, seleccione el **menú Apple** > **Configuración del sistema** > **General** > **Compartir**.
2. Seleccione la casilla **Administración remota**.
3. En otra Mac que desee usar como servidor, instale Apple Remote Desktop. Para obtener más información sobre Apple Remote Desktop, consulte el Soporte técnico de Apple.
4. Abra Apple Remote Desktop.

5. En la ventana **Remote Desktop**, haga clic en **Escáner** 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 ítems en**, elija **Top folder of the disk** (Carpeta superior del disco).

9. Haga clic en **Copiar**.

10. Una vez que los archivos se hayan copiado correctamente, haga clic en **Unix**.

11. Ingrese 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 ingresar 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 comenzará en los dispositivos seleccionados.

Instale el Agente de red con Kaspersky Security Center

Kaspersky Security Center instala el Agente de red en un equipo cliente usando 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.
- La Consola de administración se instala en la estación de trabajo del administrador de Kaspersky Security Center.
- El inicio de sesión remoto está habilitado en equipos remotos.
- Se crea una cuenta de administrador dedicada que se utilizará para ejecutar la tarea de instalación remota en un equipo remoto. Puede usar una cuenta de dominio para la instalación.
- La contraseña de sudo está deshabilitada para la cuenta dedicada.

Crear el paquete de instalación del Agente de red

1. Inicie la Consola de administración de Kaspersky Security Center.

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

3. En el árbol de la consola, seleccione la carpeta **Avanzado**, luego la subcarpeta **Instalación remota** y luego 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 **Definir el nombre del paquete de instalación**, escriba el nombre del nuevo paquete de instalación en el campo **Nombre** y haga clic en **Siguiente**.

7. En la ventana **Seleccionar el paquete de distribución para la instalación**, haga clic en **Examinar**.

   Se abre la ventana para seleccionar un archivo para crear el paquete de instalación.

8. Abra la carpeta con el contenido del paquete de instalación del Agente de red y seleccione el archivo klnagent.kud.

   La ventana **Seleccionar el paquete de distribución para la instalación** muestra el nombre y la versión de la aplicación que se instalará de forma remota utilizando el archivo que se ha agregado.

9. Haga clic en **Siguiente**.

   El paquete de instalación de Kaspersky Endpoint Security se crea con la configuración determinada.

10. En la última ventana del asistente, haga clic en **Finalizar** para salir del Asistente de paquete nuevo.

Cree una tarea para la instalación remota del Agente de red en un equipo cliente

1. Inicie la Consola de administración de Kaspersky Security Center.

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

3. Seleccione la carpeta **Tareas**.

4. En el espacio de trabajo, haga clic en **Nueva tarea** para iniciar el Asistente de nueva tarea.

5. Siga los pasos del Asistente de nueva tarea a continuación para crear una tarea para la instalación remota de Kaspersky Endpoint Security en el equipo cliente.

Para continuar con el 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:** la apariencia de los botones puede variar según su versión de Windows.

Paso 1. Selección del tipo de tarea

1. En la ventana **Seleccione el tipo de tarea**, maximice el nodo del **Servidor de administración de Kaspersky Security Center**.

2. Seleccione la tarea **Instalar aplicación de forma remota**.

Paso 2. Selección del paquete de instalación

En la ventana **Seleccionar paquete de instalación**, realice una de las siguientes acciones:

- Si el paquete de instalación del Agente de red con la configuración requerida se creó anteriormente, selecciónelo en la lista de paquetes de instalación en la parte superior de la ventana **Seleccionar paquete de instalación**.
- Si el paquete de instalación requerido aún no se ha creado, haga clic en **Nuevo** para iniciar el Asistente de paquete nuevo.

Paso 3. Configuración de los parámetros de instalación

En la ventana **Configuración**, haga lo siguiente:

1. Seleccione la casilla de verificación **Con los recursos del sistema operativo a través del Servidor de administración**.
2. Desmarque todas las demás casillas de verificación.

Paso 4. Selección de un grupo de administración para agregar equipos después de la instalación

En la ventana **Ubicación en una lista de dispositivos administrados**, seleccione un grupo al que se moverán los equipos después de la instalación, si es necesario.

Paso 5. Determinación de cómo seleccionar los equipos cliente para los cuales se creará la tarea

En la ventana **Seleccione los dispositivos a los que se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos que el Servidor de administración detectó en la red, seleccione la opción **Seleccionar dispositivos de la red detectados por el Servidor de administración**.
- Para especificar las direcciones IP de los equipos manualmente o importar las direcciones IP de los equipos desde un archivo, seleccione la opción **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**.
- Para crear una tarea para una selección de dispositivos a partir de un criterio preestablecido, 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. Selección de los equipos cliente

En la ventana que se abre (**Seleccionar los dispositivos**, **Selección de dispositivos** o **Seleccionar grupo de administración**, según la opción que seleccionó en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipo o seleccione el grupo de administración al que se aplicará la tarea.

Paso 7. Selección de la cuenta para ejecutar la tarea

1. En la ventana **Seleccione una cuenta con la que ejecutar la tarea**, seleccione la casilla de verificación **Se necesita una cuenta (no se utiliza el Agente de red)**.
2. Haga clic en **Agregar** > **Cuenta**.

   Se abre la ventana **Cuenta**.

3. Ingrese el nombre de usuario y la contraseña de la cuenta de administrador dedicada de un equipo remoto.

4. Haga clic en **Aceptar**.

Paso 8. Configuración de la programación de tareas

1. En la ventana **Configurar programación de tarea**, 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 pudo iniciar de acuerdo con la programación (por ejemplo, porque el equipo estaba apagado a la hora programada), seleccione la casilla de verificación **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security inicia la tarea tan pronto como se elimina el obstáculo que impide que se inicie la tarea.

Paso 9. Especificación del nombre de la tarea

En la ventana **Definir el nombre de la tarea**, en el campo **Nombre**, ingrese el nombre de la tarea que está creando.

Paso 10. Finalización de la creación de la tarea

En la ventana **Finalizar la creación de la tarea**, haga lo siguiente:

1. Si desea que la tarea se inicie en cuanto finalice el asistente, seleccione la casilla **Ejecutar la tarea al finalizar el Asistente**.

2. Haga clic en **Finalizar** para cerrar el asistente.

Instale el Agente de red con el protocolo SSH

Una forma de instalar el Agente de red en un equipo remoto es mediante el protocolo SSH.

Cerciórese de que se cumplan los siguientes requisitos:

- El servidor de administración de Kaspersky Security Center se implementa en la red corporativa.
- La Consola de administración se instala en la estación de trabajo del administrador de Kaspersky Security Center.
- El paquete de instalación del Agente de red se crea y almacena en una carpeta compartida del Servidor de administración.
- El inicio de sesión remoto está habilitado en el equipo remoto.
- La cuenta de equipo utilizada para instalar el Agente de red se incluye en sudoers.

Para obtener información detallada sobre los paquetes de instalación, consulte la Ayuda de Kaspersky Security Center.

Instale el Agente de red con 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 una unidad de red en el equipo remoto. Para hacer esto, ingrese 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
   ```

   Descripción de parámetros:

   - `<cuenta del administrador>`: nombre de la cuenta de administrador en el Servidor de administración.
   - `<contraseña>`: contraseña del administrador en el Servidor de administración.
   - `<dirección IP del Servidor de administración>`: dirección IP del servidor que aloja Kaspersky Security Center.

4. Ejecute el script de instalación. Para hacer esto, ingrese el siguiente comando en el cliente SSH:

   ```
   cd /Volumes/KLSHARE/<klnagent_package_folder>
   ```

   dónde `<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 <server>] [-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>]
   ```

   Descripción 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 utilizará para establecer una conexión no cifrada con el Servidor de administración. El puerto predeterminado es el 14000.
   - `use_ssl 0|1`: parámetro que determina si se utilizará 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 utilizará para establecer una conexión cifrada con el Servidor de administración a través del protocolo SSL. El puerto predeterminado es el 13000.
   - `use_proxy 0|1`: parámetro que define si se utilizará un servidor proxy al realizarse la conexión a Internet. Si el valor es "0", no se utiliza un servidor proxy. Si el valor es "1", la conexión se establece a través del servidor proxy (valor predeterminado).
   - `<proxy>`: dirección IP o nombre de DNS del servidor proxy.
   - `<proxy_login>`: nombre 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 en el equipo remoto. Para hacer esto, ingrese el siguiente comando en el cliente SSH:
   ```
   umount /Volumes/KLSHARE
   ```

6. Compruebe si el Agente de red funciona correctamente en el equipo remoto. Para hacer esto, ingrese los siguientes comandos en el cliente SSH:
   ```
   cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
   sudo ./klnagchk
   ```
   Si la verificación es exitosa, el Agente de red funciona correctamente.

Desinstale el Agente de red localmente

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 abre una ventana con el contenido del kit de distribución.

3. En la ventana con el contenido del kit de distribución, haga doble clic en **Desinstalador del Agente de red**.

4. En la ventana **Introducción**, haga clic en **Continuar**.

5. En la ventana **Información**, haga clic en **Desinstalar**.

6. Cuando se le soliciten las credenciales de administrador, escriba el nombre y la contraseña de administrador y confirme que desea desinstalar el Agente de red.

   Se inicia la desinstalación del Agente de red.

7. Lea la información sobre la desinstalación y haga clic en **Finalizar** para salir del desinstalador.

El Agente de red ahora se eliminará del equipo remoto.

Administre el Agente de red desde la línea de comandos

Esta sección contiene información sobre cómo administrar el Agente de red utilizando la línea de comandos en un equipo cliente.

Puede detener el Agente de red e iniciarlo nuevamente utilizando la línea de comandos en un equipo cliente.

También puede conectar un equipo remoto al Servidor de administración manualmente con la utilidad klmover y verificar 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 equipo remoto

Puede detener el Agente de red e iniciarlo nuevamente 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 desde 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 desde 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.

Compruebe la conexión entre un equipo cliente y el Servidor de administración manualmente. Utilidad Klnagchk

Verifique la conexión entre un equipo remoto y el Servidor de administración

En el equipo remoto, ejecute la utilidad klnagchk desde la línea de comandos.

La utilidad klnagchk está incluida en el kit de distribución del Agente de red.

Después de instalar el Agente de red, la utilidad klnagchk se encuentra en la carpeta /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Según los parámetros que especifique, la utilidad klnagchk realiza las siguientes operaciones cuando se ejecuta desde la línea de comandos:

- Muestra la configuración especificada 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 el último inicio del Agente de red) 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, envía un paquete ICMP para verificar el estado del equipo en el que está instalado el Servidor de administración.

Antes de ejecutar la utilidad, vaya a /Library/Application Support/Kaspersky Lab/klnagent/Binaries en la línea de comandos.

Sintaxis del comando:

```
sudo ./klnagchk [-logfile <nombre del archivo>] [-sp] [-savecert <ruta del archivo del certificado>] [-restart]
```

Importante: se requieren derechos de administrador para ejecutar la utilidad.

Descripción de parámetros

`-logfile <nombre del archivo>`: guarde la configuración de la conexión entre el Agente de red y el Servidor de administración, y los resultados de ejecución de la utilidad en un archivo. Si no se especifica este parámetro, la configuración de conexión del servidor, los resultados de ejecución y los mensajes de error se muestran en la pantalla.

`-sp`: visualice la contraseña para la autenticación del servidor proxy en la pantalla o guárdela en un archivo. Este parámetro se usa si el Agente de red se conecta al Servidor de administración a través de un servidor proxy. Por defecto, este parámetro no se utiliza.

`-savecert <nombre del archivo>`: guarde el certificado para la autenticación en el Servidor de administración en un archivo especificado.

`-restart:` reinicie el Agente de red después de que la utilidad termine de ejecutarse.

Ejemplo:
sudo ./klnagchk -logfile klnagchk.log -sp

Conecte un equipo remoto al Servidor de administración manualmente. Utilidad Klmover

Conecte 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.

Después de instalar el Agente de red, la utilidad klmover se encuentra en la carpeta /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

Según los parámetros que especifique, la utilidad klmover realiza las siguientes operaciones cuando se ejecuta 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, vaya a /Library/Application Support/Kaspersky Lab/klnagent/Binaries en la línea de comandos.

Sintaxis de la línea de comandos:

```
sudo ./klmover [-logfile <nombre del archivo>] [-address <dirección del servidor>] [-pn
<número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta del archivo del
certificado >] [-silent] [-dupfix]
```

Importante: se requieren derechos de administrador para ejecutar la utilidad.

Descripción de parámetros

`-logfile <nombre del archivo>`: guarde los resultados de ejecución en un archivo. Si no se especifica este parámetro, los resultados de ejecución y los mensajes de error se muestran en la pantalla.

`-address <dirección del servidor>`: dirección que el Agente de red usa para conectarse al Servidor de administración. Puede especificar la dirección IP o el nombre DNS del servidor.

Nota: también puede usar el comando con este parámetro para cambiar la dirección del Servidor de administración al que están conectadas los equipos remotos.

`-pn <número de puerto>`: número del puerto que se utilizará para establecer una conexión no cifrada con el Servidor de administración. El puerto predeterminado es el 14000.

`-ps <número de puerto SSL>`: número del puerto que se utilizará para establecer una conexión cifrada con el Servidor de administración a través del protocolo SSL. El puerto predeterminado es el 13000.

`-nossl`: utilice una conexión no cifrada al 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 del archivo del certificado>`: use el archivo de certificado especificado para la autenticación en un nuevo Servidor de administración. Si no se especifica este parámetro, el Agente de red recibirá un certificado en la primera conexión al Servidor de administración.

`-silent`: ejecute la utilidad en modo silencioso.

`-dupfix`: este parámetro se usa si el Agente de red se instaló de una manera diferente a los métodos descritos en esta ayuda; por ejemplo, si se recuperó de una imagen de disco con Agente de red instalado. Si la autoidentificación automática del Agente de red da como resultado íconos duplicados del equipo original y de otros equipos de la Consola de administración, intente volver a conectar los equipos duplicados.

Nota: al ejecutar la utilidad klmover, se recomienda especificar valores para todos los parámetros.

Ejemplo:
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

El equipo remoto que está conectado al Servidor de administración a través del Agente de red se llama *equipo cliente*.

Desinstalación del Agente de red

Sintaxis del comando:

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Instalar y desinstalar Kaspersky Endpoint Security

Esta sección describe la instalación remota y la desinstalación de Kaspersky Endpoint Security en un equipo cliente.

También puede instalar o desinstalar Kaspersky Endpoint Security de forma local o a través de Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

Instale la aplicación con 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.
- La Consola de administración se instala en la estación de trabajo del administrador de Kaspersky Security Center.
- Se ha creado un paquete de instalación para Kaspersky Endpoint Security que se encuentra en una carpeta compartida en el Servidor de administración.
- Un archivo de claves para Kaspersky Endpoint Security se almacena en la carpeta compartida en el Servidor de administración (opcional).
- El inicio de sesión remoto está habilitado en el equipo remoto.
- La cuenta de equipo utilizada para instalar la aplicación se incluye en sudoers.

Instale Kaspersky Endpoint Security en un equipo cliente utilizando 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 una unidad de red en el equipo remoto. Para hacer esto, ingrese 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
   ```

Descripción de parámetros:

- `<cuenta del administrador>`: nombre de la cuenta de administrador en el Servidor de administración.
- `<contraseña>`: contraseña del administrador en el Servidor de administración.
- `<dirección IP del Servidor de administración>`: dirección IP del servidor que aloja Kaspersky Security Center.

4. Ejecute el script de instalación. Para hacer esto, ingrese los siguientes comandos en el cliente SSH:
   ```
   cd /Volumes/KLSHARE/<carpeta del paquete de KES>
   ./install.sh --accept_eula
   ```
   dónde `<carpeta del 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 en el equipo remoto. Para hacer esto, ingrese el siguiente comando en el cliente SSH:
   ```
   umount /Volumes/KLSHARE
   ```

Instale la aplicación con 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.
- La Consola de administración se instala en la estación de trabajo del administrador de Kaspersky Security Center.
- El Agente de red está instalado en el equipo cliente.
- Se ha creado un paquete de instalación para Kaspersky Endpoint Security que se almacena en la carpeta compartida en el Servidor de administración.
- Un archivo de claves para Kaspersky Endpoint Security se almacena en la carpeta compartida en el Servidor de administración (opcional).
- El equipo cliente se agrega al grupo de administración de **Dispositivos administrados** en el Servidor de administración (opcional).

Para obtener información detallada sobre los grupos de administración en el Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

Para instalar Kaspersky Endpoint Security en un equipo cliente con Kaspersky Security Center, debe crear e iniciar la tarea **Instalar la aplicación de forma remota**.

Cree una tarea para la instalación remota de Kaspersky Endpoint Security en un equipo cliente

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **Servidor de administración <Nombre del servidor>**.
3. Seleccione la carpeta **Tareas**.
4. En el espacio de trabajo, haga clic en **Nueva tarea** para iniciar el Asistente de nueva tarea.
5. Siga los pasos del Asistente de nueva tarea a continuación para crear una tarea para la instalación remota de Kaspersky Endpoint Security en el equipo cliente.

Para continuar con el 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: la apariencia de los botones puede variar según su versión de Windows.

Paso 1. Selección del tipo de tarea

1. En la ventana **Seleccione el tipo de tarea**, maximice el nodo del **Servidor de administración de Kaspersky Security Center**.
2. Seleccione la tarea **Instalar aplicación de forma remota**.

Paso 2. Selección del paquete de instalación

En la ventana **Seleccionar paquete de instalación**, realice una de las siguientes acciones:

- Si el paquete de instalación de Kaspersky Endpoint Security con la configuración requerida se creó anteriormente, selecciónelo en la lista de paquetes de instalación en la parte superior de la ventana **Seleccionar paquete de instalación**.
- Si el paquete de instalación requerido aún no se ha creado, haga clic en **Nuevo** para iniciar el Asistente de paquete nuevo.

Paso 3. Instalación de aplicaciones adicionales

En la ventana **Avanzado**, seleccione las casillas de verificación **Instalar el Agente de red junto con esta aplicación** y **<nombre del paquete de instalación del Agente de red>** si también desea instalar el Agente de red 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. Configuración de los parámetros de instalación

En la ventana **Configuración**, configure la instalación remota de la aplicación.

Paso 5. Selección de un grupo de administración para agregar equipos después de la instalación

En la ventana **Ubicación en una lista de dispositivos administrados**, seleccione un grupo al que se moverán los equipos después de la instalación, si es necesario.

Nota: la ventana **Ubicación en una lista de dispositivos administrados** aparece si selecciona la instalación del Agente de red en el paso 3.

Paso 6. Determinación de cómo seleccionar los equipos cliente para los cuales se creará la tarea

En la ventana **Seleccione los dispositivos a los que se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos que el Servidor de administración detectó en la red, seleccione la opción **Seleccionar dispositivos de la red detectados por el Servidor de administración**.
- Para especificar las direcciones IP de los equipos manualmente o importar las direcciones IP de los equipos desde un archivo, seleccione la opción **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**.
- Para crear una tarea para una selección de dispositivos a partir de un criterio preestablecido, 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. Selección de los equipos cliente

En la ventana que se abre (**Seleccionar los dispositivos**, **Selección de dispositivos** o **Seleccionar grupo de administración**, según la opción que seleccionó en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipo o seleccione el grupo de administración al que se aplicará la tarea.

Paso 8. Selección de la cuenta para ejecutar la tarea

En la ventana **Seleccione una cuenta con la que ejecutar la tarea**, seleccione la casilla de verificación **No se necesita una cuenta (el Agente de red está instalado)**.

Se da por sentado que ha instalado el Agente de red antes de iniciar este asistente.

Paso 9. Configuración de la programación de tareas

1. En la ventana **Configurar programación de tarea**, 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 pudo iniciar de acuerdo con la programación (por ejemplo, porque el equipo estaba apagado a la hora programada), seleccione la casilla de verificación **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security inicia la tarea tan pronto como se elimina el obstáculo que impide que se inicie la tarea.

Paso 10. Especificación del nombre de la tarea

En la ventana **Definir el nombre de la tarea**, en el campo **Nombre**, ingrese el nombre de la tarea que está creando.

Paso 11. Finalización de la creación de la tarea

En la ventana **Finalizar la creación de la tarea**, haga lo siguiente:

1. Si desea que la tarea se inicie en cuanto finalice el asistente, seleccione la casilla **Ejecutar la tarea al finalizar el Asistente**.
2. Haga clic en **Finalizar** para cerrar el asistente.

La tarea que ha creado aparece en el espacio de trabajo de la carpeta **Tareas**.

Cree un paquete de instalación

Cuando crea la tarea **Instalar aplicación de forma remota**, puede usar un paquete de instalación existente o crear uno nuevo. 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 del **Servidor de administración <Nombre del servidor>**.
3. En el árbol de la consola, seleccione la carpeta **Avanzado**, luego la subcarpeta **Instalación remota** y luego 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 **Definir el nombre del paquete de instalación**, escriba el nombre del nuevo paquete de instalación en el campo **Nombre** y haga clic en **Siguiente**.
7. En la ventana **Seleccionar el paquete de distribución para la instalación**, haga clic en **Examinar**.

   Se abre la ventana para seleccionar un archivo para crear el paquete de instalación.
8. Abra la carpeta con el contenido del paquete de instalación de Kaspersky Endpoint Security y seleccione el archivo kesmac.kud.

   La ventana **Seleccionar el paquete de distribución para la instalación** muestra el nombre y la versión de la aplicación que se instalará de forma remota utilizando 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 comienza a cargarse en el Servidor de administración. Cuando finaliza la carga, se abre la ventana **Tipo de instalación**.

10. En la ventana **Tipo de instalación**, en la sección **Paquetes a instalar**, deseleccione las casillas de verificación junto a los nombres de los componentes que desea omitir durante la instalación en el equipo cliente y haga clic en **Siguiente**.

    El paquete de instalación de Kaspersky Endpoint Security se crea con la configuración determinada.

11. En la última ventana del asistente, haga clic en **Finalizar** para completar el Asistente de paquete nuevo.

Desinstale la aplicación con Kaspersky Security Center

Antes de eliminar 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.
- La Consola de administración se instala en la estación de trabajo del administrador de Kaspersky Security Center.
- El Agente de red está instalado 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 la aplicación de forma remota**.

Importante: eliminar Kaspersky Endpoint Security de un equipo cliente puede generar un riesgo de infección.

Cree una tarea para la desinstalación remota de Kaspersky Endpoint Security de un equipo cliente

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **Servidor de administración <Nombre del servidor>**.
3. Seleccione la carpeta **Tareas**.
4. En el espacio de trabajo, haga clic en **Nueva tarea** para iniciar el Asistente de nueva tarea.
5. Siga los pasos del Asistente de nueva tarea a continuación para crear una tarea para la desinstalación remota de Kaspersky Endpoint Security del equipo cliente.

Para continuar con el 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: la apariencia de los botones puede variar según su versión de Windows.

Paso 1. Selección del tipo de tarea

1. En la ventana **Seleccione el tipo de tarea**, maximice el nodo del **Servidor de administración de Kaspersky Security Center**.
2. Expanda el nodo secundario **Avanzado**.
3. Seleccione la tarea **Desinstalar aplicación de forma remota**.

Paso 2. Selección de la aplicación para desinstalar

En la ventana **Seleccionar aplicación para desinstalar**, seleccione **Desinstalar aplicación admitida por Kaspersky Security Center**.

Paso 3. Configuración de los parámetros de desinstalación

En la ventana **Configuración**, haga lo siguiente:

1. En la lista desplegable **Aplicación para desinstalar**, seleccione **Kaspersky Endpoint Security for Mac 12.2.1**.
2. Haga clic en **Siguiente**.
3. Configure la desinstalación remota de la aplicación.

Paso 4. Selección de la opción de reinicio del sistema operativo

En la ventana **Seleccione la opción de reinicio del sistema operativo**, seleccione la opción **No reiniciar el dispositivo**.

Paso 5. Determinación de cómo seleccionar los equipos cliente para los cuales se creará la tarea

En la ventana **Seleccione los dispositivos a los que se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos que el Servidor de administración detectó en la red, seleccione la opción **Seleccionar dispositivos de la red detectados por el Servidor de administración**.
- Para especificar las direcciones IP de los equipos manualmente o importar las direcciones IP de los equipos desde un archivo, seleccione la opción **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**.
- Para crear una tarea para una selección de dispositivos a partir de un criterio preestablecido, 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. Selección de los equipos cliente

En la ventana que se abre (**Seleccionar los dispositivos**, **Selección de dispositivos** o **Seleccionar grupo de administración**, según la opción que seleccionó en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipo o seleccione el grupo de administración al que se aplicará la tarea.

Paso 7. Selección de la cuenta para ejecutar la tarea

En la ventana **Seleccione una cuenta con la que ejecutar la tarea**, seleccione la casilla de verificación **No se necesita una cuenta (el Agente de red está instalado)**.

Se da por sentado que ha instalado el Agente de red antes de iniciar este asistente.

Paso 8. Configuración de la programación de tareas

1. En la ventana **Configurar programación de tarea**, 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 pudo iniciar de acuerdo con la programación (por ejemplo, porque el equipo estaba apagado a la hora programada), seleccione la casilla de verificación **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security inicia la tarea tan pronto como se elimina el obstáculo que impide que se inicie la tarea.

Paso 9. Especificación del nombre de la tarea

En la ventana **Definir el nombre de la tarea**, en el campo **Nombre**, ingrese el nombre de la tarea que está creando.

Paso 10. Finalización de la creación de la tarea

En la ventana **Finalizar la creación de la tarea**, haga lo siguiente:

1. Si desea que la tarea se inicie en cuanto finalice el asistente, seleccione la casilla **Ejecutar la tarea al finalizar el Asistente**.
2. Haga clic en **Finalizar** para cerrar el asistente.

La tarea que ha creado aparece en el espacio de trabajo de la carpeta **Tareas**.

Inicie y detenga la aplicación a través de Kaspersky Security Center

Puede iniciar o detener Kaspersky Endpoint Security en un equipo seleccionado en la lista de dispositivos administrados a través de Kaspersky Security Center.

Inicie o detenga Kaspersky Endpoint Security a través de Kaspersky Security Center

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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. Abra la ventana **Propiedades: <nombre del equipo>** con uno de los siguientes métodos:
    - Haga doble clic en el nombre del equipo cliente.
    - Haga clic con el botón derecho 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 con el botón derecho para abrir el menú contextual del elemento **Kaspersky Endpoint Security for Mac 12.2.1** y realice una de las siguientes acciones:
    - Para iniciar la aplicación, seleccione el elemento **Iniciar**.
    - Para detener la aplicación, seleccione el elemento **Detener**.

Importante: después de detener Kaspersky Endpoint Security, el equipo cliente continúa ejecutándose en modo desprotegido, lo que puede generar un riesgo de infección.

Cree y administre tareas

Esta sección indica 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
- Reversión
- Análisis
- Actualización

Puede realizar las siguientes acciones en las tareas:

- Inicie y detenga las tareas.
- Configure los parámetros de la tarea.
- Realice un seguimiento del progreso de una tarea.
- Copie y mueva tareas de un grupo a otro.
- Elimine tareas.
- Importe y exporte tareas.

Para obtener más información sobre las tareas, consulte la Ayuda de Kaspersky Security Center.

Crear tareas

Al administrar 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 independiente.
- Tareas de grupo. *Una tarea de grupo* es una tarea que se ejecuta en equipos en un grupo de administración.
- Tareas para un conjunto arbitrario de equipos. Puede crear una tarea para que se ejecute en cualquier equipo, independientemente de si pertenecen a un grupo de administración o una selección de equipos.

Crear una tarea local para un equipo cliente independiente

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Dispositivos**.
6. Seleccione el equipo de la lista de equipos cliente.
7. Abra la ventana **Propiedades: <nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo cliente.
   - Haga clic con el botón derecho en el equipo cliente y elija **Propiedades** en el menú contextual.
8. En la ventana **Propiedades: <Nombre del equipo>**, seleccione la sección **Tareas**.

   La lista de tareas del sistema y tareas personalizadas para el equipo cliente seleccionado se muestra en el espacio de trabajo a la derecha.
9. Haga clic en **Agregar** en la parte inferior del espacio de trabajo.

   Se abre el Asistente de nueva tarea.
10. Siga los pasos del Asistente de nueva tarea para crear una tarea local para un equipo cliente concreto.

Crear una tarea para equipos cliente en un grupo de administración

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Tareas**.

6. En el espacio de trabajo, haga clic en **Nueva tarea** para iniciar el Asistente de nueva tarea.

7. Siga los pasos del Asistente de nueva tarea para 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 conjunto arbitrario de equipos

1. Inicie la Consola de administración de Kaspersky Security Center.

2. Maximice el nodo del **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 de nueva tarea.

5. Siga los pasos del Asistente de nueva tarea para crear una tarea para un conjunto arbitrario de equipos.

Para continuar con el 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: la apariencia de los botones puede variar según su versión de Windows.

Paso 1. Selección de una aplicación y establecimiento del tipo de tarea

1. En la ventana **Seleccionar el tipo de tarea**, maximice el nodo de **Kaspersky Endpoint Security for Mac 12.2.1**.

2. Seleccione el tipo de tarea que desea crear:

   - Para crear una tarea para agregar una clave, seleccione **Agregar clave**.
   - Para crear una tarea de análisis de áreas críticas, seleccione **Análisis rápido**.
   - Para crear una tarea para revertir la última actualización, seleccione **Reversión**.
   - Para crear una tarea de análisis de malware, seleccione **Análisis**.
   - Para crear una tarea de actualización, seleccione **Actualización**.

Paso 2. Configuración de los parámetros para el tipo de tarea seleccionado

Según el tipo de tarea seleccionado durante el paso anterior, el contenido de la ventana de configuración puede variar. Esta ventana no se muestra para la tarea Reversión.

Activación de la aplicación

En la ventana **Activación de la aplicación**, realice una de las siguientes acciones:

1. Seleccione un código o clave de activación del almacenamiento de Kaspersky Security Center o agregue un archivo de claves almacenado en su equipo.

2. Para agregar la clave determinada como una clave de reserva, seleccione la casilla **Agregar como clave de reserva**.

   La clave de reserva se activa cuando vence la clave activa actual.

La información sobre la clave especificada (clave, tipo de clave y fecha de vencimiento de la clave) se muestra en la ventana **Activación de la aplicación**.

Actualización

Los servidores de actualizaciones de Kaspersky dedicados son el origen principal de actualizaciones para Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede usar puntos de distribución, carpetas locales u otros servidores web como un *origen de actualizaciones*.

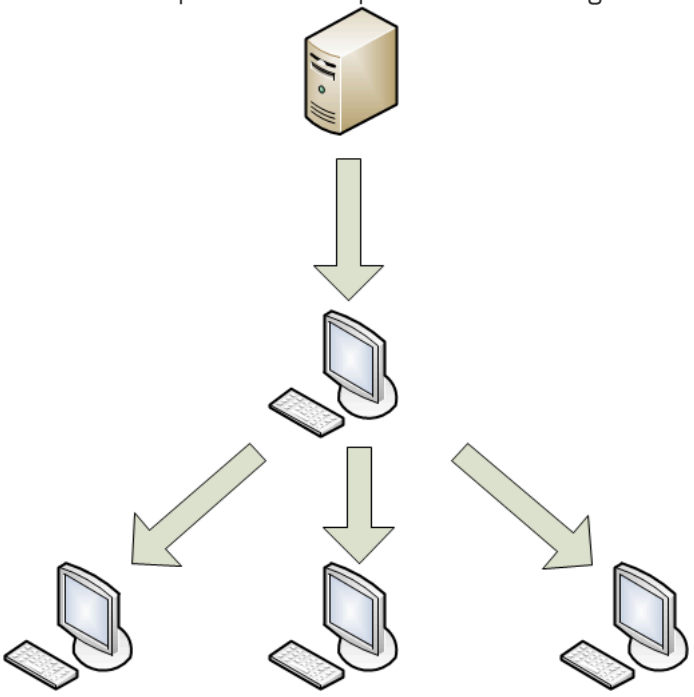
Puede colocar las actualizaciones descargadas en una carpeta local para actualizar las bases de datos de la aplicación y los módulos de Kaspersky Endpoint Security en otros equipos de la red corporativa para reducir la cantidad de tráfico de Internet.

Puede configurar la distribución de actualizaciones de la siguiente manera:

1. Uno de los equipos en la red recibe el paquete de actualización de Kaspersky Endpoint Security de los servidores de actualizaciones de Kaspersky o un origen de actualizaciones diferente. Las actualizaciones recuperadas se colocan en una carpeta local compartida.

   Nota: la carpeta local compartida se debe crear de antemano.

2. Otros equipos en la red se refieren 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 **Actualización**:

1. Para deshabilitar las actualizaciones de los módulos de la aplicación, desmarque la casilla **Actualizar módulos de la aplicación**.

2. Para cambiar los orígenes de actualización:

   a. Haga clic en **Configuración**.

   Se abre la ventana **Configuración: actualización**.

   b. Seleccione las casillas de verificación junto a los orígenes de actualización que desea usar.

3. Para especificar un origen de actualizaciones diferente, haga clic en **Agregar**.

   Se abre la ventana **Origen de actualizaciones**.

   a. Especifique la dirección web del origen de actualizaciones o la ruta a una carpeta local o de red que sea 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 **Recomendada**, solicita al usuario una acción cuando detecta un objeto infectado después del 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 del alcance 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 en la ventana **Análisis**:

1. Seleccione uno de los niveles de seguridad preestablecidos o personalice la configuración de seguridad.
2. Especifique la acción que realiza Kaspersky Endpoint Security cuando detecta un objeto infectado.
3. Determine un alcance del análisis.

Paso 3. Determinación de cómo seleccionar los equipos cliente para los cuales se creará la tarea

Nota: este paso no es relevante para tareas locales o de grupo.

En la ventana **Seleccione los dispositivos a los que se asignará la tarea**, seleccione el método que desea usar para especificar los equipos cliente:

- Para seleccionar entre los equipos que el Servidor de administración detectó en la red, seleccione la opción **Seleccionar dispositivos de la red detectados por el Servidor de administración**.
- Para especificar las direcciones IP de los equipos manualmente o importar las direcciones IP de los equipos desde un archivo, seleccione la opción **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**.
- Para crear una tarea para una selección de dispositivos a partir de un criterio preestablecido, 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. Selección de los equipos cliente

Nota: este paso no es relevante para tareas locales o de grupo.

En la ventana que se abre (**Seleccionar los dispositivos**, **Selección de dispositivos** o **Seleccionar grupo de administración**, según la opción que seleccionó en el paso anterior), seleccione los equipos cliente, especifique las direcciones IP de los equipos, especifique una selección de equipo o seleccione el grupo de administración al que se aplicará la tarea.

Paso 5. Configuración de la programación de tareas

1. En la ventana **Configurar programación de tarea**, 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 pudo iniciar de acuerdo con la programación (por ejemplo, porque el equipo estaba apagado a la hora programada), seleccione la casilla de verificación **Ejecutar tareas no realizadas**.

   Kaspersky Endpoint Security inicia la tarea tan pronto como se elimina el obstáculo que impide que se inicie la tarea.

4. Si desea que Kaspersky Security Center determine automáticamente el intervalo entre lanzamientos de tareas en diferentes equipos, seleccione la casilla de verificación **Utilizar retardo aleatorio automático para el inicio de tareas**.

   Esto ayuda a reducir la carga en el Servidor de administración de Kaspersky Security Center.

5. Para establecer el intervalo entre el inicio de tareas en diferentes equipos de forma manual, seleccione la casilla **Utilizar un retardo aleatorio para el inicio de tareas dentro de un intervalo de (min)** y especifique la cantidad de minutos.

   Esto ayuda a reducir la carga en el Servidor de administración de Kaspersky Security Center.

Paso 6. Especificación del nombre de la tarea

En la ventana **Definir el nombre de la tarea**, en el campo **Nombre**, ingrese el nombre de la tarea que está creando.

Paso 7. Finalización de la creación de la tarea

En la ventana **Finalizar la creación de la tarea**, haga lo siguiente:

1. Si desea que la tarea se inicie en cuanto finalice el asistente, seleccione la casilla **Ejecutar la tarea al finalizar el Asistente**.

2. Haga clic en **Finalizar** para cerrar el asistente.

Iniciar y detener tareas manualmente

Las tareas programadas se inician y se detienen automáticamente de acuerdo con un programa. Sin embargo, puede iniciar una tarea manualmente en cualquier momento.

Nota: las tareas se inician en un equipo cliente solo si el Agente de red se está ejecutando. Si el Agente de red deja de ejecutarse, todas las tareas activas se interrumpen.

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. Inicie o detenga la tarea de una 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 seleccione **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 desde la que desea exportar la tarea:
   - Seleccione el grupo de administración y luego abra la pestaña **Tareas**.
   - En el árbol de la consola, haga clic en **Tareas**.
2. Haga clic con el botón derecho en la tarea que desea exportar y, en el menú contextual de la tarea, elija **Todas las tareas** > **Exportar**.
3. En la ventana **Guardar como**, especifique el nombre del archivo y la ubicación donde se guardará la tarea exportada.
4. Haga clic en **Guardar**.

Importar una tarea

1. Seleccione la lista de tareas a la que desea importar la tarea:
   - Seleccione el grupo de administración y luego 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 contextual de la lista de tareas, seleccione **Todas las tareas** > **Importar**.
   - Haga clic en **Importar tarea desde archivo**.
3. En la ventana **Abrir**, especifique la ruta al archivo de tareas 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 determinado, para equipos en un grupo de administración determinado o la lista de todas las tareas no locales.

Ver tareas para un grupo de administración determinado

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Tareas**.

Se muestra 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 del **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 ficha **Dispositivos**.
6. Seleccione el equipo de la lista de equipos cliente.
7. Abra la ventana **Propiedades: <nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo cliente.
   - Haga clic con el botón derecho en el equipo cliente y elija **Propiedades** en el menú contextual.
8. En la ventana **Propiedades: <Nombre del equipo>**, seleccione la sección **Tareas**.

La lista de tareas del sistema y tareas personalizadas para el equipo cliente seleccionado se muestra en el espacio de trabajo a la derecha.

Ver tareas no locales

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **Servidor de administración <Nombre del servidor>**.
3. En el árbol de la consola, haga clic en **Tareas**.

Se muestra la lista de tareas no locales creadas para equipos que pueden o no ser parte de grupos de administración.

Administrar configuraciones específicas de tareas

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 maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.

Ver la configuración de una tarea de grupo

1. Abra la lista de tareas de grupo para un grupo de administración.
2. Seleccione una tarea de la lista y abra la configuración de la tarea de una de las siguientes maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.
   - Haga clic en el vínculo **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 maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.
   - Haga clic en el vínculo **Configurar tarea** en el espacio de trabajo.

Para obtener más información sobre las tareas, consulte la Ayuda de Kaspersky Security Center.

Para tareas locales, tareas de grupo o tareas para un conjunto arbitrario de equipos

Configuración de la tarea Agregar clave

1. Abra la ventana con la configuración de tarea **Agregar clave**.
2. Seleccione la sección **Activación de la aplicación**.

3. Si es necesario, agregue otra clave de una de las siguientes maneras:

   - Para seleccionar una clave o un código de activación entre los códigos de activación agregados al almacenamiento de Kaspersky Security Center:

     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 almacenamiento 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 **Agregar**.

     Se abre la ventana de selección de archivos.

     c. Aplique un archivo de claves.

     d. Haga clic en **Abrir**.

   Nota: la clave actual se elimina cuando se agrega una clave diferente.

4. Para agregar la clave determinada como una clave de reserva, seleccione la casilla **Agregar como clave de reserva**.

   La clave de reserva se activa cuando vence la clave actual.

   Nota: la fecha de vencimiento de la clave de reserva debe ser posterior a la fecha de vencimiento de la clave actual.

5. Guarde los cambios de una de las siguientes maneras:

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

Administrar la configuración de la tarea Análisis rápido

1. Abra la ventana con la configuración de tarea **Análisis rápido**.
2. Seleccione la sección **Análisis rápido**.

3. Para cambiar el nivel de seguridad en el que Kaspersky Endpoint Security ejecuta la tarea de análisis rápido, realice una de las siguientes acciones en la sección Nivel de seguridad:

   - Seleccione un nivel de seguridad preestablecido moviendo el control deslizante hacia arriba o hacia abajo en la escala.

     Puede elegir uno de los siguientes niveles de seguridad:

     - **Protección máxima**. Kaspersky Endpoint Security realiza la supervisión máxima de los archivos que se abren, guardan o ejecutan.
     - **Recomendada**. Kaspersky Endpoint Security supervisa los archivos con la configuración que recomienda Kaspersky.

       Este es el nivel de seguridad predeterminado.
     - **Velocidad máxima**. Kaspersky Endpoint Security monitorea un conjunto mínimo de archivos. Puede elegir este nivel de seguridad si desea utilizar otras aplicaciones que necesitan recursos de memoria significativos.

   - Configure los parámetros de seguridad manualmente:

     a. Haga clic en **Configuración**.

        Se abre la ventana **Configuración: Análisis**.

     b. En la pestaña **General**, en la sección **Tipos de archivo**, seleccione los tipos de archivos que Kaspersky Endpoint Security debe analizar al ejecutar la tarea de análisis rápido.

     c. En la pestaña **General**, en la sección **Optimización**, configure los parámetros de rendimiento de análisis.

     d. En la pestaña **General** en la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice en busca de objetos detectables.

     e. En la pestaña **Avanzado**, en la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el almacenamiento de información sobre los 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 malware.

     g. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.

        El nivel de seguridad cambia a **Personalizada**.

   - Para restaurar la configuración predeterminada, haga clic en **Predeterminada**.

     El nivel de seguridad cambia a **Recomendada**.

4. Si es necesario, en la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security debe realizar cuando se detecta un objeto infectado.

5. Para especificar un alcance del análisis, en la sección **Alcance del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Alcance 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 **Elementos de inicio**.

c. Si desea que Kaspersky Endpoint Security analice otros archivos adicionales o carpetas, haga clic en Agregar y especifique un archivo, carpeta o máscara para los nombres de archivo o carpeta.

d. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Alcance del análisis**.

6. Guarde los cambios de una de las siguientes maneras:

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

Configuración de la tarea Analizar

1. Abra la ventana con la configuración de tarea **Análisis**.
2. Seleccione la sección Análisis.
3. Para cambiar el nivel de seguridad en el que Kaspersky Endpoint Security ejecuta la tarea de análisis, realice una de las siguientes acciones en la sección Nivel de seguridad:

- Seleccione un nivel de seguridad preestablecido moviendo el control deslizante hacia arriba o hacia abajo en la escala.

  Puede elegir uno de los siguientes niveles de seguridad:

  - **Protección máxima**. Kaspersky Endpoint Security realiza la supervisión máxima de los archivos que se abren, guardan o ejecutan.
  - **Recomendada**. Kaspersky Endpoint Security supervisa los archivos con la configuración que recomienda Kaspersky.

    Este es el nivel de seguridad predeterminado.
  - **Velocidad máxima**. Kaspersky Endpoint Security monitorea un conjunto mínimo de archivos. Puede elegir este nivel de seguridad si desea utilizar otras aplicaciones que necesitan recursos de memoria significativos.

- Configure los parámetros de seguridad manualmente:

  a. Haga clic en **Configuración**.

  Se abre la ventana **Configuración: Análisis**.

  b. En la pestaña **General**, en la sección **Tipos de archivo**, seleccione los tipos de archivos que Kaspersky Endpoint Security debe analizar al ejecutar la tarea de análisis.

  c. En la pestaña **General**, en la sección **Optimización**, configure los parámetros de rendimiento de análisis.

  d. En la pestaña **General** en la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que Kaspersky Endpoint Security analice en busca de objetos detectables.

  e. En la pestaña **Avanzado**, en la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el almacenamiento de información sobre los 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 malware.

g. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Análisis**.

El nivel de seguridad cambia a **Personalizada**.

- Para restaurar la configuración predeterminada, haga clic en **Predeterminada**.

  El nivel de seguridad cambia a **Recomendada**.

4. Si es necesario, en la sección **Acción**, seleccione la acción que Kaspersky Endpoint Security debe realizar cuando se detecta un objeto infectado.

5. Para especificar un alcance del análisis, en la sección **Alcance del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Alcance del análisis** que se abre:

   a. Si desea que Kaspersky Endpoint Security analice todos los discos extraíbles, desmarque la casilla **Todos los discos extraíbles**.

   b. Si desea que Kaspersky Endpoint Security analice todas las unidades internas, seleccione la casilla de verificación **Todos los discos internos**.

   c. Si desea que Kaspersky Endpoint Security analice todas las unidades de red, seleccione la casilla de verificación **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 **Elementos de inicio**.

   f. Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas, haga clic en Agregar y especifique un archivo, carpeta o máscara para los nombres de archivo o carpeta.

   g. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Alcance del análisis**.

6. Guarde los cambios de una de las siguientes maneras:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: <Nombre de la tarea>** después de guardar los cambios.

   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: <Nombre de la tarea>** después de guardar los cambios.

Administrar la configuración de la tarea de actualización

1. Abra la ventana con la configuración de la tarea **Actualización**.

2. Seleccione la sección **Actualización**.

3. Si desea que Kaspersky Endpoint Security actualice los módulos de la aplicación junto con las bases de datos de la aplicación, seleccione la casilla **Actualizar módulos de la 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 maneras:

- 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 actualizaciones de Kaspersky, seleccione la casilla de verificación **Servidores de actualizaciones de Kaspersky**.
- Para agregar un origen de actualizaciones diferente, haga clic en **Agregar** y, en la ventana que se abre, ingrese la ruta al origen de actualizaciones.

  De manera predeterminada, Kaspersky Endpoint Security descarga actualizaciones de los servidores de actualizaciones 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 maneras:

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

Solo para tareas locales

Administrar la configuración de la tarea de Protección contra archivos peligrosos

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea Protección contra archivos peligrosos y abra sus propiedades de una de las siguientes maneras:

- Haga doble clic en el nombre de la tarea.
- Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.
- Haga clic en **Propiedades**.

3. Seleccione la sección **Protección contra amenazas de archivo**.
4. Si es necesario, configure los siguientes parámetros:

- Habilite o deshabilite la Protección contra archivos peligrosos en el equipo cliente.
- Para seleccionar uno de los niveles de seguridad preestablecidos, use el control deslizante en la sección **Nivel de seguridad**.

- Para configurar los parámetros de seguridad manualmente, haga clic en **Configuración** y en la ventana **Configuración: Protección contra amenazas de archivo** que se abre, haga lo siguiente:

  a. En la pestaña **General**, en la sección **Tipos de archivo**, seleccione los tipos de archivos que Kaspersky Endpoint Security debe analizar cuando se abren, ejecutan o guardan.

  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**, en la sección **Archivos compuestos**, seleccione qué archivos compuestos se deben analizar en busca de objetos detectables y establezca una restricción para analizar objetos grandes.

  d. En la pestaña **Alcance de la protección**, especifique los archivos o carpetas que la Protección contra archivos peligrosos debe analizar.

  De forma predeterminada, se analizan todos los objetos que se encuentran en las unidades internas, extraíbles y de red conectadas al equipo cliente. Puede agregar un objeto al alcance de la protección, modificar un objeto en la lista, deshabilitar temporalmente el análisis de un objeto en la lista o eliminar un objeto de la lista.

  e. En la pestaña **Avanzado**, en la sección **Modo de análisis**, seleccione el modo Protección contra archivos peligrosos.

  f. En la pestaña **Avanzado**, en la sección **Pausar tarea**, habilite o deshabilite la pausa programada de la Protección contra archivos peligrosos y configure la pausa automática de tareas de acuerdo con un cronograma.

  g. En la pestaña **Avanzado**, en la sección **Analizador heurístico**, configure el uso del Analizador heurístico mediante la Protección contra archivos peligrosos.

  h. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Configuración: Protección contra amenazas de archivo**.

- En la sección **Si se detecta un objeto malicioso**, seleccione la acción que realiza la Protección contra archivos peligrosos al detectar un objeto infectado.

5. Guarde los cambios de una de las siguientes maneras:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Protección contra amenazas de archivo** después de guardar los cambios.

   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Protección contra amenazas de archivo** después de guardar los cambios.

Administrar la configuración de la tarea Protección frente a amenazas en la 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 en la web y abra sus propiedades de una de las siguientes maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección **Protección contra amenazas web**.
4. Si es necesario, configure los siguientes parámetros:
   - Habilite o deshabilite la Protección frente a amenazas en la web en el equipo cliente.
   - Para seleccionar uno de los niveles de seguridad preestablecidos, use el control deslizante en la sección **Nivel de seguridad**.
   - Para configurar los parámetros de seguridad manualmente, haga clic en **Configuración** y, en la ventana **Configuración: Protección contra amenazas web** que se abre, haga lo siguiente:
     a. En la pestaña **General**, en la sección **Modo de análisis**, habilite o deshabilite la comprobación de direcciones web con la base de datos de direcciones web maliciosas.
     b. En la pestaña **General**, en la sección **Configuración antiphishing**, habilite o deshabilite la comprobación de direcciones web con la base de datos de direcciones web fraudulentas.
     c. En la pestaña **General**, en la sección **Configuración antiphishing**, habilite o deshabilite el uso del Analizador heurístico para detectar vínculos phishing.
     d. En la pestaña **Direcciones web de confianza**, habilite o deshabilite el análisis del tráfico web desde 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 **Configuración: Protección contra amenazas web**.
5. En la sección **Si se detecta un objeto malicioso**, seleccione la acción que realiza la Protección contra amenazas web cuando detecta un objeto peligroso en el tráfico web.
6. Guarde los cambios de una de las siguientes maneras:
   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Protección contra amenazas web** después de guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Protección contra amenazas web** después de guardar los cambios.

Administrar la configuración de la tarea Análisis rápido

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea Análisis rápido y abra sus propiedades de una de las siguientes maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección Análisis.
4. Si es necesario, configure los siguientes parámetros:
   - Para seleccionar uno de los niveles de seguridad preestablecidos, use el control deslizante en la sección **Nivel de seguridad**.
   - Para configurar los parámetros de seguridad manualmente, haga clic en **Configuración** y, en la ventana Configuración: Análisis que se abre, haga lo siguiente:
     a. En la pestaña **General**, en la sección **Tipos de archivo**, seleccione los tipos de archivos que Kaspersky Endpoint Security debe analizar.
     b. En la pestaña **General**, en la sección **Optimización**, configure los parámetros de rendimiento de análisis.
     c. En la pestaña **General**, en la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que analice Kaspersky Endpoint Security.
     d. En la pestaña **Avanzado**, en la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el almacenamiento de información sobre los objetos detectados en las estadísticas de la aplicación.
     e. En la pestaña **Avanzado**, en la sección Analizador heurístico, configure el uso del Analizador heurístico y seleccione el nivel de protección que este 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 debe realizar al detectar un objeto infectado.
   - Para especificar un alcance del análisis, en la sección **Alcance del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Alcance del análisis** que se abre:
     - Si desea que Kaspersky Endpoint Security analice objetos en la lista predeterminada, seleccione la casilla de verificación que se encuentra junto al objeto relevante.
     - Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas, haga clic en Agregar y especifique un archivo, carpeta o máscara para los nombres de archivo o carpeta.
     - Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Alcance del análisis**.

5. Guarde los cambios de una de las siguientes maneras:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Análisis rápido** después de guardar los cambios.

   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Análisis rápido** después de guardar los cambios.

Administrar la configuración de la tarea Análisis completo

1. Abra la lista de tareas locales para un equipo cliente.

2. En la lista de tareas locales, seleccione la tarea Análisis completo y abra sus propiedades de una de las siguientes maneras:

   - Haga doble clic en el nombre de la tarea.

   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.

   - Haga clic en **Propiedades**.

3. Seleccione la sección Análisis.

4. Si es necesario, configure los siguientes parámetros:

   - Para seleccionar uno de los niveles de seguridad preestablecidos, use el control deslizante en la sección **Nivel de seguridad**.

   - Para configurar los parámetros de seguridad manualmente, haga clic en **Configuración** y, en la ventana Configuración: Análisis que se abre, haga lo siguiente:

     a. En la pestaña **General**, en la sección **Tipos de archivo**, seleccione los tipos de archivos que Kaspersky Endpoint Security debe analizar.

     b. En la pestaña **General**, en la sección **Optimización**, configure los parámetros de rendimiento de análisis.

     c. En la pestaña **General**, en la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que analice Kaspersky Endpoint Security.

     d. En la pestaña **Avanzado**, en la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el almacenamiento de información sobre los objetos detectados en las estadísticas de la aplicación.

     e. En la pestaña **Avanzado**, en la sección Analizador heurístico, configure el uso del Analizador heurístico y seleccione el nivel de protección que este 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 debe realizar al detectar un objeto infectado.

- Para especificar un alcance del análisis, en la sección **Alcance del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Alcance del análisis** que se abre:

  - Si desea que Kaspersky Endpoint Security analice objetos en la lista predeterminada, seleccione la casilla de verificación que se encuentra junto al objeto relevante.

  - Si desea que Kaspersky Endpoint Security analice otros archivos o carpetas, haga clic en Agregar y especifique un archivo, carpeta o máscara para los nombres de archivo o carpeta.

  - Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Alcance del análisis**.

5. Guarde los cambios de una de las siguientes maneras:

   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Análisis completo** después de guardar los cambios.

   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Análisis completo** después de guardar los cambios.

Administrar la configuración de la tarea Análisis personalizado

1. Abra la lista de tareas locales para un equipo cliente.

2. En la lista de tareas locales, seleccione la tarea Análisis personalizado y abra sus propiedades de una de las siguientes maneras:

   - Haga doble clic en el nombre de la tarea.

   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.

   - Haga clic en **Propiedades**.

3. Seleccione la sección Análisis.

4. Si es necesario, configure los siguientes parámetros:

   - Para seleccionar uno de los niveles de seguridad preestablecidos, use el control deslizante en la sección **Nivel de seguridad**.

   - Para configurar los parámetros de seguridad manualmente, haga clic en **Configuración** y, en la ventana Configuración: Análisis que se abre, haga lo siguiente:

     a. En la pestaña **General**, en la sección **Tipos de archivo**, seleccione los tipos de archivos que Kaspersky Endpoint Security debe analizar.

     b. En la pestaña **General**, en la sección **Optimización**, configure los parámetros de rendimiento de análisis.

     c. En la pestaña **General**, en la sección **Archivos compuestos**, seleccione qué archivos compuestos desea que analice Kaspersky Endpoint Security.

     d. En la pestaña **Avanzado**, en la sección **Configuración avanzada**, configure el uso de la tecnología iSwift y el almacenamiento de información sobre los objetos detectados en las estadísticas de la aplicación.

e. En la pestaña **Avanzado**, en la sección Analizador heurístico, configure el uso del Analizador heurístico y seleccione el nivel de protección que este 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 debe realizar al detectar un objeto infectado.
- Para especificar un alcance del análisis, en la sección **Alcance del análisis**, haga clic en **Configuración** y haga lo siguiente en la ventana **Alcance del análisis** que se abre:
  - Haga clic en **Agregar** y especifique un archivo, una carpeta o una máscara de nombre de un archivo o una carpeta.
  - Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana **Alcance del análisis**.

5. Guarde los cambios de una de las siguientes maneras:
   - Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Análisis personalizado** después de guardar los cambios.
   - Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Análisis personalizado** después de guardar los cambios.

Administrar la configuración de la tarea Protección contra amenazas de red

1. Abra la lista de tareas locales para un equipo cliente.
2. En la lista de tareas locales, seleccione la tarea Protección contra amenazas de red y abra sus propiedades de una de las siguientes maneras:
   - Haga doble clic en el nombre de la tarea.
   - Haga clic con el botón derecho para mostrar el menú de accesos directos de la tarea y seleccione **Propiedades**.
   - Haga clic en **Propiedades**.
3. Seleccione la sección **Protección contra amenazas de red**.
4. Si es necesario, configure los siguientes parámetros:
   - Habilite o deshabilite la Protección contra amenazas de red en el equipo cliente.
   - En la sección **Configuración de protección contra amenazas de 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 hacer esto, realice los siguientes pasos:

     a. Haga clic en **Exclusiones**.

     Se abre la ventana **Exclusiones**.

     b. Haga clic en **Agregar**.

     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 maneras:

- Haga clic en **Aplicar** para permanecer en la ventana **Propiedades: Protección contra amenazas de red** después de guardar los cambios.
- Haga clic en **Aceptar** para cerrar la ventana **Propiedades: Protección contra amenazas de red** después de guardar los cambios.

Cree y administre políticas

Esta sección contiene información sobre cómo crear y configurar directivas para Kaspersky Endpoint Security.

Una directiva determina los ajustes de una aplicación y administra la capacidad de configurar esa aplicación en dispositivos dentro de un grupo de administración. Se debe crear una directiva independiente para cada aplicación. Puede crear un número ilimitado de diversas directivas para aplicaciones instaladas en dispositivos en cada grupo de administración, pero solo se puede aplicar una directiva a cada aplicación a la vez dentro de un grupo de administración.

Nota: al crear y configurar una directiva, puede permitir o prohibir cambios en cualquier grupo de configuraciones en las directivas que utilizan los botones y .

Puede realizar las siguientes acciones en las directivas personalizadas:

- Cree directivas.
- Configure directivas.
- Copie o mueva directivas de un grupo a otro.
- Elimine directivas.
- Cambie el estado de las directivas.
- Exporte directivas a un archivo.
- Importe directivas desde un archivo.

Para obtener información detallada sobre las directivas de Kaspersky Security Center, consulte la Ayuda de Kaspersky Security Center.

Cree una directiva

Esta sección contiene instrucciones sobre cómo iniciar el Asistente de nueva directiva para 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 del **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 de nueva directiva.
6. Siga los pasos del Asistente de 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 del **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 de nueva directiva.
5. Siga los pasos del Asistente de nueva directiva para crear una directiva.

Para continuar con el 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: la apariencia de los botones puede variar según su versión de Windows.

Paso 1. Selección de una aplicación

En la ventana **Seleccione la aplicación para la que desee crear una directiva de grupo**, en la lista de aplicaciones, seleccione **Kaspersky Endpoint Security for Mac (12.2.1)**.

Paso 2. Especificación del nombre de la directiva

1. En la ventana **Escriba el nombre de la directiva de grupo**, en el campo **Nombre**, especifique el nombre de la directiva que está creando. El nombre no puede contener los siguientes símbolos: " * < : > ? \ |.
2. Seleccione la casilla de verificación **Usar la configuración de la directiva para la versión anterior de la aplicación** si desea importar la configuración de una directiva existente de Kaspersky Endpoint Security a una nueva directiva.

Paso 3. Especificación de la configuración de protección

En la ventana **Protección**, configure los siguientes parámetros si es necesario:

- Configure los parámetros de protección para el sistema operativo en el equipo cliente.
- Configure la Zona de confianza.

  Puede crear una lista de objetos que Kaspersky Endpoint Security no analiza ni supervisa.
- Configure las Aplicaciones de confianza.

  Puede crear una lista de aplicaciones cuya actividad de red y archivos no se supervisará a través de Kaspersky Endpoint Security.
- Seleccione los tipos de objetos que desea detectar.
- Deshabilite o habilite el inicio de tareas programadas cuando el equipo funciona con batería.
- Limitar el uso de las tareas de análisis de la CPU.

Paso 4. Configuración de los parámetros de Protección contra archivos peligrosos

En la ventana **Protección contra amenazas de archivo**, haga lo siguiente si es necesario:

- Active o desactive la Protección contra archivos peligrosos.

  De manera predeterminada, la Protección contra archivos peligrosos está activada.
- Seleccione un nivel de seguridad.

  De forma predeterminada, se selecciona el nivel de seguridad que recomienda Kaspersky.
- Configure los parámetros de Protección contra archivos peligrosos
- Seleccione la acción que se realizará al detectar un objeto malicioso.

Paso 5. Configuración de los ajustes de Protección frente a amenazas en la web

En la ventana de **Protección contra amenazas web**, haga lo siguiente si es necesario:

- Habilite o deshabilite la Protección contra amenazas web.

  De forma predeterminada, la Protección contra amenazas web está habilitada.
- Seleccione un nivel de seguridad.

  De forma predeterminada, se selecciona el nivel de seguridad que recomienda Kaspersky.
- Ajuste la Configuración de Protección contra amenazas web.
- Seleccione la acción que se realizará al detectar un objeto malicioso en el tráfico web.

Paso 6. Configuración los parámetros de Protección contra amenazas de red

En la ventana **Protección contra amenazas de red**, haga lo siguiente si es necesario:

- Habilite o deshabilite la Protección contra amenazas de red.

  De manera predeterminada, la Protección contra amenazas de red está habilitada.

- Configure los parámetros de Protección contra amenazas de red.
- Cree o edite una lista de direcciones IP de equipos remotos cuya actividad de red nunca será bloqueada por Kaspersky Endpoint Security.

Paso 7. Ajustes de actualización

En la ventana **Actualización**, haga lo siguiente si es necesario:

- Active o desactive la actualización de los módulos de la aplicación.
- Especifique los orígenes de actualizaciones.

Paso 8. Configuración de los parámetros de KSN

En la ventana **Kaspersky Security Network**, haga lo siguiente si es necesario:

- Lea el texto completo de la Declaración de Kaspersky Security Network haciendo clic en **Declaración de KSN**.
- Consulte la información sobre la infraestructura de KSN proporcionada por Kaspersky Security Center.
- Active o desactive el uso de Kaspersky Security Network.
- Habilite o deshabilite el modo KSN extendido.
- Habilite o deshabilite el uso de un proxy de KSN.
- Habilite o deshabilite el uso de los servidores de Kaspersky cuando el proxy de KSN no esté disponible.

> **Nota:** el uso de Kaspersky Security Network y de un proxy de KSN en equipos remotos solo está disponible si el Servidor de administración de Kaspersky Security Center se usa como 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 la infraestructura de KSN Global y elige participar en Kaspersky Security Network en la configuración de directivas, las estadísticas de Kaspersky Endpoint Security desde 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 expreso.

Datos proporcionados a Kaspersky mediante Kaspersky Security Network en la infraestructura de KSN Global

Si la casilla **Acepto usar Kaspersky Security Network** está seleccionada y la casilla **Habilitar el modo extendido de KSN** no está seleccionada, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

- Versión completa del Software instalado;
  tipo del Software instalado;
  identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador único del dispositivo; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

Si las casillas **Acepto usar Kaspersky Security Network** y **Habilitar el modo extendido de KSN** están seleccionadas, Kaspersky Endpoint Security proporciona a Kaspersky los siguientes datos:

- Información acerca de la versión del sistema operativo (SO) y los paquetes de servicio instalados en la computadora, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo de kernel del SO, y los parámetros del modo de ejecución del SO; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada de 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 del procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactivo; cantidad de eventos de acción procesados del SO; 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 del procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento del evento recurrente; 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 de una acción en el SO.

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

- Información acerca de la aplicación del Titular de los derechos que se instaló y acerca del estado de protección antivirus: identificador de la instalación (PCID) del software; 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 del Software instalado; identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); 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; identificador de actualización del Software; tipo del Software instalado; fecha y hora de inicio de la Vigía proactiva; fecha y hora de instalación del software; probabilidad de que la Vigía proactiva envíe estadísticas; código del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo máximo permitido para el procesamiento de un evento por parte de la Vigía proactiva; tiempo de procesamiento del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por la Vigía proactiva.

- Información sobre todos los objetos y operaciones analizados: veredicto del software sobre el 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 la Vigía proactiva; fecha y hora de detección de software por la Vigía proactiva; características de detección; identificador del registro desencadenado en las bases de datos antivirus del software; motivo por el que la Vigía proactiva detectó el software; 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 desencadenado de las bases de datos antivirus del software; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; las direcciones URL y del referido desde las que se descargó; el tamaño de los archivos analizados y la ruta 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 empacador (si se empacó el archivo); 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 valor de la suma de control complementaria del objeto; datos acerca de la firma digital del objeto (certificado): 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 de firma del archivo; el nombre, el tipo, el tipo de identificador, la suma de comprobación (MD5) y el tamaño de la aplicación que cargó el objeto que se está validando; la ruta de la aplicación y las rutas de las plantillas; un atributo que indique la presencia en la Lista de ejecución automática; la fecha de entrada; la lista de atributos; el nombre del empaquetador; la información acerca de la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME, la fecha y la 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 empaquetador (si el archivo estaba empaquetado), 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 inició 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 del solicitud 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 empaquetadores (si se empaquetó el archivo); la información sobre la disponibilidad y validez de estas estadísticas; el identificador del modo para generar las estadísticas que se envían.

- Si se detectan amenazas o vulnerabilidades, además de la información sobre el objeto detectado, se proporciona información sobre el identificador, la versión y el tipo de registro en la base de datos antivirus, el nombre de la amenaza según la clasificación de Kaspersky, la fecha y hora de la última actualización de la base de datos antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de la aplicación que solicitó la URL donde se detectó la amenaza, la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador de vulnerabilidad y su nivel de amenaza, la URL y el referente de la página web donde se detectó la vulnerabilidad.

- Si se detecta un posible objeto malicioso, la información acerca de los datos se proveerá en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo atacante y número del puerto en la computadora del usuario al que ataca la red, identificador del protocolo de ataque, nombre y tipo de ataque.

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

- Las direcciones URL e IP de la página web en la que se detectó contenido dañino o sospechoso; el nombre, el tamaño y la suma de comprobación del archivo que solicitó la dirección URL; el identificador, el peso y el grado de la regla utilizada para llegar a un veredicto, el objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: estado de terminación de la tarea de actualización, tipo de error que puede ocurrir durante el proceso de actualización, cantidad de actualizaciones con errores, identificador del componente de la aplicación que realiza actualizaciones.

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

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se detectó el evento, tipo y categoría del evento, nombre del origen del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la que se solicita la reputación y la referencia, el 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 analizado (MD5), el tipo de amenaza detectada, la información sobre el registro usado para detectar una amenaza (el identificador de registro para la base de datos del antivirus y el tipo y la marca de tiempo del registro); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

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

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

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

- Información sobre el dispositivo: ID de dispositivo.

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

Cuando Kaspersky Security Center utiliza la infraestructura de KSN Privada y elige participar en Kaspersky Security Network en la configuración de directivas, Kaspersky Endpoint Security no envía estadísticas a Kaspersky desde los equipos cliente a los que se aplica la directiva.

Después de que una directiva se elimina o se vuelve inactiva, la configuración de KSN en un equipo cliente vuelve al estado inicial.

Paso 9. Configuración de los parámetros de interacción

En la ventana **Interacción con el usuario**, configure los parámetros de Kaspersky Endpoint Security para la interacción con el usuario del equipo cliente si es necesario.

Paso 10. Configurar parámetros de conexión de red

En la ventana **Red**, haga lo siguiente si es necesario:

- Configure la conexión a un servidor proxy.

- Habilite o deshabilite la exploración 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 supervisados por Kaspersky Endpoint Security.

Paso 11. Configuración de Informes y depósito de copias de seguridad

En la ventana **Informes y depósito de copias de seguridad**, haga lo siguiente si es necesario:

- Configure los parámetros para generar y almacenar informes.
- Configure los parámetros para almacenar objetos en Copia de seguridad.

Paso 12. Configurar el cifrado de disco FileVault

En la ventana **Cifrado de disco FileVault**, haga lo siguiente si es necesario:

- Habilite o deshabilite la administración de cifrado de disco FileVault para el disco de inicio del usuario.

  De manera predeterminada, la administración de cifrado de disco FileVault está deshabilitada.

- Elija la opción **Cifrar disco**, si desea cifrar el disco de inicio del usuario cuando la directiva se aplica a un equipo cliente.

Si se selecciona la casilla **Habilitar la administración de cifrado de disco FileVault**, los usuarios con derechos de administrador pueden cifrar y descifrar los discos de inicio de su Mac desde Configuración del sistema.

Si se seleccionan la casilla **Habilitar la administración de cifrado de disco FileVault** y la opción **Cifrar disco**, los usuarios con derechos de administrador no pueden descifrar el disco de inicio de su Mac desde Configuración del sistema.

Si se seleccionan la casilla **Habilitar la administración de cifrado de disco FileVault** y la opción **Descifrar disco**, los usuarios con derechos de administrador no pueden cifrar el disco de inicio de su Mac desde Configuración del sistema.

Paso 13. Configurar el Control Web

En la ventana **Control web**, haga lo siguiente si es necesario:

- Activar o desactivar 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 **El Control web está habilitado** 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 **Verificar conexiones seguras (HTTPS)** está seleccionada en la ventana **Red** del Asistente de nueva directiva.

- Agregue una nueva regla para el Control Web haciendo clic en **Agregar**.

  Puede ingresar un nombre de regla, elegir si la regla está activa, especificar un área de regla creando una lista de direcciones web específicas o seleccionando categorías de sitios web, y seleccionar una acción que Kaspersky Endpoint Security realiza cuando un usuario accede a un sitio web incluido en esta regla.

- Edite, elimine u organice las reglas creadas en la lista.

El orden en que se clasifican las reglas determina la prioridad de su aplicación por parte de Kaspersky Endpoint Security.

Paso 14. Configurar Managed Detection and Response

En la ventana **Managed Detection and Response**, haga lo siguiente si es necesario:

- Habilitar o deshabilitar el componente Managed Detection and Response

  De forma predeterminada, Managed Detection and Response está deshabilitado.

- Importe o elimine un archivo de configuración que se utiliza para activar el componente Managed Detection and Response en los dispositivos administrados.

Si la casilla **Habilitar Managed Detection and Response** está seleccionada y el archivo de configuración de MDR se importa, el componente Managed Detection and Response está activo e interactúa con el servicio 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 Expert (on-premise)

En la ventana **Endpoint Detection and Response Expert (on-premise)**, haga lo siguiente si es necesario:

- Habilite o deshabilite el componente Endpoint Detection and Response Expert (on-premise).

  De manera predeterminada, el componente Endpoint Detection and Response Expert (on-premise) está deshabilitado.

- Configure la conexión del servidor y agregue un certificado TLS.

- Agregue un servidor.

Si se selecciona la casilla **Habilitar Endpoint Detection and Response Expert (versión 7.1 o anteriores)** y se agregan un certificado TLS y un servidor, el componente Endpoint Detection and Response Expert (on-premise) está activo e interactúa con la solución Kaspersky Anti Targeted Attack Platform. Esta solución detecta con rapidez amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas, ataques de día cero y más.

Paso 16. Configurar Análisis de discos externos

En la ventana **Análisis de discos externos**, realice las siguientes configuraciones:

- 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 la detección de comportamiento

En la ventana **Detección de comportamiento**, haga lo siguiente si es necesario:

- Habilitar o deshabilitar la Detección de comportamiento.

  De forma predeterminada, la Detección de comportamiento está habilitada.

- Seleccione la acción que se realizará cuando se detecte actividad de malware.

- Habilite o deshabilite la protección de carpetas compartidas contra el cifrado externo.

  - Seleccione la acción que se realizará cuando se detecte actividad de malware.

Paso 18. Configurar la protección contra amenazas de correo

En la ventana **Protección contra amenazas de correo**, haga lo siguiente si es necesario:

- Habilite o deshabilite la Protección contra amenazas de correo.
  De manera predeterminada, la Protección contra amenazas de red está habilitada.
- Seleccione la acción que se realizará al detectar un objeto malicioso.
- Ajuste la configuración de Protección contra amenazas de correo.

Paso 19. Configurar la prevención de exploits

En la ventana **Prevención de exploits**, haga lo siguiente si es necesario:

- Habilite o deshabilite Prevención de exploits.
  De manera predeterminada, la Prevención de exploits está habilitada.
- Seleccione la acción que se realizará al detectar un exploit.

Paso 20. Configurar el motor de reparación

En la ventana **Motor de reparación**, haga lo siguiente si es necesario:

- Habilite o deshabilite el motor de reparación.
  De manera predeterminada, el motor de reparación está habilitado.

Paso 21. Configurar el Control de dispositivos

En la ventana **Control de dispositivos**, haga lo siguiente si es necesario:

- Habilite o deshabilite el Control de dispositivos.
  De manera predeterminada, el Control de dispositivos está habilitado.
- Ajuste la configuración de Control de dispositivos.

Paso 22. Configurar el Firewall

En la ventana **Firewall**, haga lo siguiente si es necesario:

- Habilite o deshabilite el Firewall.
  De manera predeterminada, el Firewall está habilitado.
- Ajuste la configuración del Firewall.

Paso 23. Definir el grupo de administración al que se aplicará la directiva

En la ventana **Grupo de destino**, haga clic en **Examinar** para seleccionar un grupo de administración al que desea aplicar la directiva.

Paso 24. Seleccionar el estado de la directiva y completar la creación de una directiva

En la ventana **Crear la 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:* la directiva no se aplica.
- *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 múltiples directivas para una aplicación en un grupo de administración, pero solo una de ellas 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 **Abrir las propiedades de la directiva en cuanto se haya creado** si desea revisar la configuración de la directiva una vez creada.
3. Haga clic en **Finalizar** para cerrar el Asistente de nueva directiva.

   La directiva que ha creado aparece en la pestaña **Directivas** en el espacio de trabajo del grupo de administración correspondiente. La directiva se aplica a los equipos cliente después de su primera sincronización con el Servidor de administración.

Puede editar la configuración de la directiva que ha creado. También puede prohibir o permitir cambios a cada grupo de configuraciones desde un equipo cliente con los botones y para cada grupo de configuraciones. El botón que se encuentra al lado de un grupo de configuraciones indica que el usuario de un equipo cliente no puede editar estas configuraciones en el equipo del usuario. El botón que se encuentra junto a un grupo de configuraciones indica que el usuario de un equipo cliente puede editar estas configuraciones en el equipo del usuario.

Vea la lista de directivas

Puede crear un número ilimitado de diversas directivas para aplicaciones instaladas en equipos en cada grupo de administración, pero solo se puede aplicar una directiva a cada aplicación a la 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 del **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 ficha **Directivas**.

   Se muestra la lista de directivas.

Edite la configuración de directivas

Puede realizar cambios en la directiva que creó en Kaspersky Security Center y bloquear cualquier cambio en su configuración en las directivas de subgrupos y en la configuración de tareas.

La configuración de la directiva de Kaspersky Endpoint Security incluye la configuración de la aplicación y la configuración de tareas.

Edite la configuración de directivas

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Directivas**.
5. Haga clic derecho en la directiva que desea configurar y elija **Propiedades**.
6. En la ventana **Propiedades: <Nombre de la directiva>**, configure los parámetros de la política:

   - En la sección **Protección básica contra amenazas**

     Configure los siguientes parámetros de Protección contra archivos peligrosos

     - Active o desactive la Protección contra archivos peligrosos.
     - Seleccione uno de los niveles de seguridad preestablecidos o configure los parámetros de seguridad manualmente.
     - Seleccione la acción que se realizará al detectar un objeto malicioso.

     Configure las siguientes opciones de Protección frente a amenazas en la web

     - Habilite o deshabilite la Protección contra amenazas web.
     - Seleccione uno de los niveles de seguridad preestablecidos o configure los parámetros de seguridad manualmente.
     - Habilite o deshabilite la comprobación de direcciones web en la base de datos de direcciones web maliciosas.
     - Configure los parámetros de Anti-Phishing.
     - Agregue direcciones confiables cuyo tráfico no analizará la Protección frente a amenazas en la web.
     - Seleccione la acción que se realizará al detectar un objeto malicioso en el tráfico web.

     Ajustar la siguiente configuración de Protección contra amenazas de correo

     - Habilite o deshabilite la Protección contra amenazas de correo.
     - Seleccione la acción que se realizará al detectar un objeto malicioso.
     - Ajuste la configuración de Protección contra amenazas de correo.

Configure los siguientes parámetros de Protección contra amenazas de red

- Habilite o deshabilite la Protección contra amenazas de red.
- Configure los parámetros de Protección contra amenazas de red.
- Especifique las direcciones IP de los equipos cuya actividad de red no se bloqueará.

Ajustar la siguiente configuración del Firewall

- Habilite o deshabilite el Firewall.
- Ajuste la configuración del Firewall.

- En la sección **Protección avanzada contra amenazas**

  Configure los siguientes parámetros de KSN

  - Lea el texto completo de la Declaración de Kaspersky Security Network haciendo clic en **Declaración de KSN**.
  - Active o desactive el uso de Kaspersky Security Network.
  - Habilite o deshabilite el modo KSN extendido.
  - Activar/desactivar el modo Nube.
  - Habilite o deshabilite el uso de un proxy de KSN.
  - Habilite o deshabilite el uso de los servidores de Kaspersky cuando el proxy de KSN no esté disponible.

  Nota: el uso de Kaspersky Security Network y de un proxy de KSN en equipos remotos solo está disponible si el Servidor de administración de Kaspersky Security Center se usa como servidor proxy. Para obtener información detallada sobre las propiedades del Servidor de administración, consulte la Ayuda de Kaspersky Security Center.

  Establezca la siguiente configuración de Detección de comportamiento

  - Habilitar o deshabilitar la Detección de comportamiento.

    De forma predeterminada, la Detección de comportamiento está habilitada.
  - Seleccione la acción que se realizará cuando se detecte actividad de malware.

  Ajustar la siguiente configuración de Prevención de exploits

  - Habilite o deshabilite Prevención de exploits.
  - Seleccione la acción que se realizará al detectar un exploit.

  Ajustar la siguiente configuración del Motor de reparación

  Habilite o deshabilite el motor de reparación.

- En la sección **Controles de seguridad**

Ajustar la siguiente configuración de Control de dispositivos

- Habilite o deshabilite el Control de dispositivos.
- Ajuste la configuración de Control de dispositivos.

Configure los siguientes parámetros de Control Web

- Activar o desactivar el Control Web.
- Agregue una nueva regla para el Control Web haciendo clic en **Agregar**.
- Edite, elimine u organice las reglas creadas en la lista.

- En la sección **Cifrado de datos**

  Configure los siguientes parámetros de cifrado de disco FileVault

  - Habilite o deshabilite la administración de cifrado de disco FileVault para equipos cliente.
  - Cifre o descifre el disco de inicio en los equipos cliente.

    Si se selecciona la casilla **Habilitar la administración de cifrado de disco FileVault**, los usuarios con derechos de administrador pueden cifrar y descifrar los discos de inicio de su Mac desde Configuración del sistema.

    Si se seleccionan la casilla **Habilitar la administración de cifrado de disco FileVault** y la opción **Cifrar disco**, los usuarios con derechos de administrador no pueden descifrar el disco de inicio de su Mac desde Configuración del sistema.

    Si se seleccionan la casilla **Habilitar la administración de cifrado de disco FileVault** y la opción **Descifrar disco**, los usuarios con derechos de administrador no pueden cifrar el disco de inicio de su Mac desde Configuración del sistema.

- En la sección **Detección y respuesta**

  Configure los siguientes ajustes de Managed Detection and Response

  - Habilitar o deshabilitar el componente Managed Detection and Response
  - Importe o elimine un archivo de configuración que se utiliza para activar el componente Managed Detection and Response en los dispositivos administrados.

  Configure los siguientes ajustes de Endpoint Detection and Response (KATA).

  - Habilite o deshabilite el componente Endpoint Detection and Response (KATA).
  - Configure la conexión del servidor y agregue un certificado TLS.
  - Agregue un servidor KATA.

- En la sección **Tareas locales**

  Configure los siguientes ajustes de 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 **Actualización**

Configure los siguientes parámetros de actualización

- Active o desactive la actualización de los módulos de la aplicación.
- Especifique los orígenes de actualizaciones.

- En la sección **Configuración adicional**

  Configure los siguientes parámetros de protección

  - Habilite o deshabilite la protección en tiempo real del equipo cliente.
  - Habilite o deshabilite el inicio de Kaspersky Endpoint Security cuando se inicie el equipo cliente.
  - Configure la Zona de confianza.
  - Configure las Aplicaciones de confianza.
  - Seleccione los tipos de objetos que desea detectar.
  - Deshabilite o habilite el inicio de tareas programadas cuando el equipo funciona con batería.

  Configure los siguientes parámetros de red

  - Habilite o deshabilite el uso de un servidor proxy.
  - Especifique la dirección del servidor proxy.
  - Habilite o deshabilite el uso de un servidor proxy para direcciones locales.
  - Especifique el nombre de usuario y la contraseña para la autenticación del servidor proxy.
  - Habilite o deshabilite la exploración 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.

  Configure las siguientes opciones de Informes y depósito de copias de seguridad

  - Habilite o deshabilite el almacenamiento de eventos no críticos en el informe.
  - Habilite o deshabilite solo el guardado de eventos recientes.
  - Habilite o deshabilite la eliminación de eventos después del período especificado.
  - Especifique el período para almacenar eventos.
  - Habilite o deshabilite la eliminación de objetos de la Copia de seguridad después del período especificado.
  - Especifique el período para almacenar objetos en Copia de seguridad.

Configure los siguientes parámetros de interacción del usuario

- Habilite o deshabilite las notificaciones de evento.
- Seleccione cómo Kaspersky Endpoint Security notificará al usuario sobre los eventos.
- Habilite o deshabilite la visualización del ícono de Kaspersky Endpoint Security en la barra de menús.
- Configure si un usuario puede abrir la ventana principal de Kaspersky Endpoint Security y utilizar la interfaz de la aplicación en un equipo cliente.
- Habilite o deshabilite la disponibilidad del elemento **Salir** en el menú de accesos directos del ícono de Kaspersky Endpoint Security en el equipo cliente.
- Seleccione el idioma utilizado para mostrar los eventos de Kaspersky Security Center.
- Configure los parámetros 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.

Cambie el estado de una directiva

El estado de una directiva define el funcionamiento de una directiva. La directiva puede tener un estado activo, fuera de la oficina, o inactivo. Puede cambiar el estado de la directiva en la configuración de la directiva.

Cambie el estado de una directiva

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Directivas**.
6. Haga clic derecho en la directiva cuyo estado desea cambiar 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 directiva:

   - **Directiva activa**. La directiva siempre se aplica 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>**.

Exporte una directiva a un archivo KLP

Puede exportar una directiva personalizada a un archivo para usar la directiva en otro Servidor de administración.

Exporte una directiva a un archivo KLP

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Directivas**.
6. Haga clic con el botón derecho en la directiva para mostrar su menú contextual y seleccione **Exportar**.
   Se abre la ventana **Guardar como**.
7. Seleccione la carpeta en la que desea guardar el archivo KLP para la directiva.
8. Especifique el nombre del archivo.
9. Haga clic en **Guardar** para guardar el archivo en la carpeta seleccionada.

Importe una directiva desde un archivo KLP

Puede importar una directiva existente con configuraciones predefinidas desde un archivo.

Importe una directiva desde un archivo KLP

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 ficha **Directivas**.

6. Abra la ventana de selección de archivos de una de las siguientes maneras:

   - Haciendo clic en el botón **Importar directiva desde archivo**.

   - Haciendo clic derecho en un área vacía en el espacio de trabajo para abrir el menú contextual y seleccionar el elemento **Importar**.

7. Seleccione un archivo KLP con una directiva y haga clic en **Abrir**.

La directiva importada se agrega a la lista de directivas en el espacio de trabajo.

Cree y administre perfiles de directivas.

Un perfil de directiva es un conjunto denominado de configuraciones variables para una directiva, que se activa en un equipo cliente cuando se cumplen condiciones determinadas. La activación de un perfil modifica la configuración de la directiva vigente en el dispositivo cuando se activa el perfil de la 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 ficha **Directivas**.

3. Siga uno de estos procedimientos para abrir las propiedades de la directiva para la que desea crear un perfil:

   - Haga doble clic en el nombre de la directiva.

   - Haga clic con el botón derecho 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 la directiva>**, seleccione la sección **Perfiles de directivas**.

5. En el espacio de trabajo, haga clic en **Agregar**.

6. En la ventana **Asignación de perfiles de directivas**, lea la información sobre las directivas y haga clic en **Siguiente**.

   Si no desea que se visualice esta ventana cuando crea nuevos perfiles de directivas, seleccione la casilla de verificación **No volver a mostrar esta ventana** antes de hacer clic en **Siguiente**.

7. En la ventana **Nombre del perfil de directiva**, haga lo siguiente para configurar el perfil de la directiva:

   - Ingrese 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 habilitado o deshabilitado.

- En la lista desplegable de la sección **Estado del perfil de directiva**, seleccione si el perfil de la directiva se puede editar.

- Si desea configurar reglas de activación para el perfil de directiva, seleccione la casilla de verificación **Después de cerrar el Asistente de nuevo perfil de directiva, proceder con la configuración de la regla de activación de perfiles de directivas**.

8. Haga clic en **Finalizar**.

9. Si seleccionó la casilla de verificación **Después de cerrar el Asistente de nuevo perfil de directiva, proceder con la configuración de la regla de activación de perfiles de directivas**, siga los pasos del Asistente de nueva regla de activación del perfil de directiva.

El perfil de directiva que creó aparece en la sección **Perfiles de directiva** de la ventana **Propiedades: <Nombre de la directiva>**.

Crear una regla de activación de perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración en el que desea crear una regla de activación de perfil de directiva.

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

3. Siga uno de estos procedimientos para abrir las propiedades de la directiva:

   - Haga doble clic en el nombre de la directiva.

   - Haga clic con el botón derecho 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 la directiva>**, seleccione la sección **Perfiles de directivas**.

5. En el espacio de trabajo, seleccione el perfil de directiva para el 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 nueva regla de activación del perfil de directiva.

Siga los pasos del Asistente de nueva regla de activación del perfil de directiva.

Modificar un perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración para el que desea modificar un perfil de directiva.

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

3. Siga uno de estos procedimientos para abrir las propiedades de la directiva para la que desea modificar un perfil:

   - Haga doble clic en el nombre de la directiva.
   - Haga clic con el botón derecho 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 la directiva>**, seleccione la sección **Perfiles de directivas**.

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**, cambie el nombre del perfil o habilite/deshabilite el perfil marcando/desmarcando la casilla **Habilitar 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.
   - Edite la configuración de la directiva en las secciones relevantes.

7. Haga clic en **Aceptar**.

Si el perfil de la directiva está activo, la configuración modificada se aplicará después de que el equipo cliente se sincronice con el Servidor de administración. Si el perfil de directiva está inactivo, se aplicará después de que se active la regla de activación.

Cambio de 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 ficha **Directivas**.

3. Siga uno de estos procedimientos 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 clic con el botón derecho 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 la directiva>**, seleccione la sección **Perfiles de directivas**.

5. En el espacio de trabajo, seleccione el perfil de directiva cuya prioridad desea cambiar.

6. Aumente/disminuya la prioridad del perfil seleccionado haciendo clic en los botones .

Eliminar un perfil de directiva

1. En el árbol de la consola, seleccione el grupo de administración para el que desea eliminar un perfil de directiva.
2. En el espacio de trabajo, seleccione la ficha **Directivas**.
3. Siga uno de estos procedimientos para abrir las propiedades de la directiva para la que desea eliminar un perfil:
   - Haga doble clic en el nombre de la directiva.
   - Haga clic con el botón derecho 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 la directiva>**, seleccione la sección **Perfiles de directivas**.
5. En el espacio de trabajo, seleccione el perfil que desea eliminar y haga clic en **Eliminar**.

Para obtener información detallada sobre los perfiles de directivas, consulte la Ayuda de Kaspersky Security Center.

Genere un informe sobre objetos detectados

Genere un informe sobre objetos detectados

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **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 con el botón derecho en el equipo seleccionado para abrir el menú contextual y seleccione **Todas las tareas** > **Ver informe de amenazas**.

El informe generado se abre en una ventana del navegador.

Puede encontrar información sobre otras formas de generar un informe sobre los objetos que la aplicación detecta en el equipo cliente en la Ayuda de Kaspersky Security Center.

Obtener una clave de recuperación para una unidad cifrada

Si un usuario de un equipo cliente olvida o pierde sus credenciales y no puede acceder a una unidad cifrada, puede obtener una clave de recuperación.

Obtenga una clave de recuperación

1. Inicie la Consola de administración de Kaspersky Security Center.
2. Maximice el nodo del **Servidor de administración <Nombre del servidor>**.
3. En el árbol de la consola, seleccione la carpeta **Avanzado**, luego la subcarpeta **Protección y cifrado de datos** y luego la subcarpeta **Unidades cifradas**.
4. En el espacio de trabajo, haga clic con el botón derecho en el dispositivo con el disco cifrado para mostrar el menú contextual y seleccione **Obtener clave de recuperación para macOS**.

   Se abre 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 a la unidad cifrada.

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 cuya finalidad es proporcionar una forma centralizada de realizar las tareas principales relacionadas con la administración y el mantenimiento de la 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 de 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.

Instale el 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 podrá abrir el Asistente de inicio rápido desde 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, agregue el archivo ZIP del paquete de distribución para el complemento web de Kaspersky Endpoint Security en la interfaz de Web Console: (**Configuración** → **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 **Configuración** → **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 12.2.1 en la lista y haga clic en su nombre.

  c. En la ventana con la descripción del complemento web, haga clic en el botón **Instale el 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 necesarios para instalar los complementos web se incluyen en el kit de distribución):

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

  b. En la ventana que se abre, especifique la ruta al archivo 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 (**Configuración** → **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.

Cree una directiva

Esta sección contiene información sobre cómo crear y configurar directivas para Kaspersky Endpoint Security utilizando Kaspersky Security Center Web Console y Cloud Console.

Una directiva determina los ajustes de una aplicación y administra la capacidad de configurar esa aplicación en dispositivos dentro de un grupo de administración. Se debe crear una directiva independiente para cada aplicación. Puede crear un número ilimitado de diversas directivas para aplicaciones instaladas en dispositivos en cada grupo de administración, pero solo se puede aplicar una directiva a cada aplicación a la vez dentro de un grupo de administración.

Nota: al crear y configurar una directiva, puede permitir o prohibir cambios en cualquier grupo de configuraciones en las directivas que utilizan el conmutador de alternancia **Imponer**.

Cree 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 que desea crear una directiva y haga clic en **Siguiente**.

   Se abre 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 **Configuración 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 directivas personalizadas:

- Cree directivas.
- Configure directivas.
- Copie o mueva directivas de un grupo a otro.
- Elimine directivas.
- Cambie 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 la directiva para una directiva de Kaspersky Endpoint Security utilizando Kaspersky Security Center Web Console y Cloud Console, debe verificar que la configuración se aplique correctamente en los equipos cliente.

Protección contra amenazas del host

Configurar el componente Protección contra amenazas de archivo

Puede configurar el componente Protección contra amenazas de archivo de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección contra amenazas de host** → **Protección contra amenazas de archivo**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de archivo**.
  6. Configure el componente Protección contra amenazas de archivo.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección básica contra amenazas** → **Protección contra amenazas de archivo**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de archivo**.
  6. Configure el componente Protección contra amenazas de archivo.
  7. Guarde los cambios.

Configuración de la Protección contra amenazas de archivo

Configuración	Descripción
Exclusiones del análisis	Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas. A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre las aplicaciones legítimas que los intrusos pueden utilizar para poner en riesgo su equipo o los datos de los usuarios están disponibles en el sitio web de la Enciclopedia TI de Kaspersky.
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección** Si esta opción está seleccionada, la aplicación intenta automáticamente desinfectar el archivo infectado que detecta. Si no se puede llevar a cabo la desinfección, la aplicación elimina el archivo. **Preguntar al usuario**. Kaspersky Endpoint Security despliega una ventana de notificación con información sobre el objeto malicioso que ha infectado el archivo y solicita al usuario que seleccione la acción que debe realizar la aplicación. Las acciones disponibles pueden variar según el estado del objeto.

Configuración	Descripción
Alcance de la protección	Contiene objetos que son analizados por el componente Protección contra archivos peligrosos. Los objetos de análisis pueden ser discos duros, unidades extraíbles o de red, carpetas, archivos individuales o máscaras que engloben varios archivos. De manera predeterminada, el componente Protección contra amenazas de archivos analiza los archivos iniciados en discos duros, unidades extraíbles o unidades de red. El alcance de protección de estos objetos no puede modificarse ni eliminarse. Solo es posible excluir un objeto (por ejemplo, unidades extraíbles) de los análisis.
Optimización de análisis	En **Optimización de análisis**, puede configurar Kaspersky Endpoint Security para un mayor rendimiento al analizar archivos. • **Analizar solo archivos nuevos y modificados**. Analiza solo los archivos nuevos y los archivos que se han modificado desde la última vez que se analizaron. Esto ayuda a reducir la duración del análisis. Este modo se aplica tanto a archivos simples como compuestos. • **Omitir análisis de volumen del sistema de solo lectura**. Si se selecciona esta casilla, la aplicación no analiza el volumen del sistema de solo lectura. Esto reduce significativamente el tiempo de análisis.
Análisis de archivos compuestos	Una técnica común para ocultar virus u otro malware es implantarlo en archivos compuestos, como archivos de almacenamiento o bases de datos. Para detectar virus u otro malware oculto de esta manera, es necesario descomprimir el archivo compuesto, lo que puede reducir la velocidad del análisis. Puede limitar los tipos de archivos compuestos que se analizarán y, de esta forma, aumentar la velocidad del análisis. • **Analizar archivos de almacenamiento**. Analizar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos de almacenamiento. La aplicación analiza los archivos no solo por su extensión, sino también por su formato. Al verificar archivos de almacenamiento, la aplicación realiza un descomprimido recursivo. Esto permite detectar amenazas dentro de archivos de almacenamiento multinivel (un archivo de almacenamiento dentro de un archivo de almacenamiento). • **Analizar paquetes de distribución y archivos de almacenamiento autoextraíbles**. Análisis de paquetes de instalación de aplicaciones de terceros y archivos autoextraíbles. Los archivos autoextraíbles incorporan un módulo de extracción ejecutable. Para analizar archivos autoextraíbles, debe seleccionar la casilla **Analizar archivos de almacenamiento**. • **Analizar archivos en formatos de Microsoft Office y objetos OLE incrustados**. Archivos de Microsoft Office (por ejemplo, DOC, DOCX, XLS, PPT) y objetos OLE incrustados en archivos (por ejemplo, tablas de Excel, macros, archivos adjuntos de correo electrónico).
Permitir la descompresión en segundo plano de archivos de almacenamiento de más de (MB)	Si esta casilla de verificación está seleccionada, la aplicación proporciona acceso a los archivos compuestos que son más grandes que el valor especificado antes de que se analicen estos archivos. En este caso, Kaspersky Endpoint Security descomprimirá y analizará los archivos compuestos en segundo plano. La aplicación proporciona acceso a los archivos compuestos que son más pequeños que este valor solo después de descomprimir y analizar estos archivos. Si esta casilla de verificación no está seleccionada, la aplicación proporciona acceso a archivos compuestos solo después de descomprimir y analizar los archivos, independientemente de su tamaño.
No analizar archivos comprimidos de más de (MB)	Si esta casilla de verificación está seleccionada, la aplicación no analiza los archivos compuestos si su tamaño excede el valor especificado. Si esta casilla está desactivada, la aplicación analiza los archivos compuestos de todos los tamaños. La aplicación analiza los archivos grandes extraídos de archivos de almacenamiento independientemente de si la casilla de verificación está seleccionada o no.

Configurar el Análisis de unidades extraíbles

Puede configurar el componente Análisis de unidades extraíbles de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección contra amenazas de host → Análisis de unidades extraíbles**.
  5. Habilite o deshabilite el componente usando el conmutador **Análisis de unidades extraíbles**.

6. Configure el componente Análisis de unidades extraíbles.
7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Tareas locales → Análisis de discos externos**.
5. Configure el componente Análisis de unidades extraíbles.
6. Guarde los cambios.

Configurar la detección de comportamiento

Puede configurar el componente Detección de comportamiento de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Detección de comportamiento**.
5. Habilite o deshabilite el componente usando el conmutador **Detección de comportamiento**.
6. Configure el componente Detección de comportamiento.
7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Protección avanzada contra amenazas → Detección de comportamiento**.
5. Habilite o deshabilite el componente usando el conmutador **Detección de comportamiento**.

6. Configure el componente Detección de comportamiento.
7. Guarde los cambios.

Configuración de Detección de comportamiento

Configuración	Descripción
Aplicaciones de confianza	La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de archivos y de red (incluida la actividad maliciosa) y el acceso al registro del sistema no son supervisados por Kaspersky Endpoint Security. De manera predeterminada, Kaspersky Endpoint Security supervisa las acciones y el tráfico de red de todas las aplicaciones y analiza los objetos que abren, ejecutan o guardan los procesos asociados a las mismas. Una vez que se agrega una aplicación a la lista de aplicaciones de confianza, Kaspersky Endpoint Security deja de supervisar la actividad de la aplicación.
Exclusiones del análisis	Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas. A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre las aplicaciones legítimas que los intrusos pueden utilizar para poner en riesgo su equipo o los datos de los usuarios están disponibles en el sitio web de la Enciclopedia TI de Kaspersky.
Acción al detectar una amenaza	**Solicitar acción**. Si se detecta actividad maliciosa, Kaspersky Endpoint Security le solicita al usuario que seleccione la acción que se realizará cuando se detecte actividad maliciosa. Las acciones disponibles pueden variar según el estado del objeto. **Bloquear**. Si se detecta actividad maliciosa, Kaspersky Endpoint Security bloquea la aplicación que realiza la actividad maliciosa y registra información sobre ella. **Eliminar**. Si se selecciona esta opción, al detectar actividad maliciosa, Kaspersky Endpoint Security elimina el archivo ejecutable de la aplicación maliciosa y crea una copia de seguridad del archivo en Copia de seguridad.

Configurar Anti-Cryptor

Puede configurar el componente Anti-Cryptor de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**
  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Anticifrador**.
  5. Habilite o deshabilite el componente usando el conmutador **Anti-Cryptor**.
  6. Configure el componente Anti-Cryptor.
  7. Guarde los cambios.
- **Usando el complemento de Kaspersky Endpoint Security**
  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección avanzada contra amenazas → Detección de comportamiento**.

5. Utilice el conmutador **Proteger carpetas compartidas contra el cifrado externo** para habilitar o deshabilitar el componente.
6. Configure el componente Anti-Cryptor.
7. Guarde los cambios.

Configuración de Anti-Cryptor

Parámetro	Descripción
Acción al detectar una amenaza	**Informar** Si se elige esta opción, cuando se detecta un intento de modificar los archivos de una carpeta compartida, Kaspersky Endpoint Security agrega información sobre el hecho a la lista de amenazas activas y agrega una entrada al informe. **Bloquear conexión por (min)**. Al detectar un intento de modificar archivos en carpetas compartidas, Kaspersky Endpoint Security bloquea el tráfico de red del dispositivo que lleva a cabo actividad maliciosa. La aplicación crea un evento de *Cifrado detectado* que contiene información sobre el dispositivo en riesgo.

Configuración del componente Prevención de exploits

Puede configurar el componente Prevención de exploits de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**
  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Prevención de exploits**.
  5. Habilite o deshabilite el componente usando el conmutador **Prevención de exploits**.
  6. Configure el componente Prevención de exploits.
  7. Guarde los cambios.
- **Usando el complemento de Kaspersky Endpoint Security**
  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección avanzada contra amenazas → Prevención de exploits**
  5. Habilite o deshabilite el componente usando el conmutador **Prevención de exploits**.
  6. Configure el componente Prevención de exploits.
  7. Guarde los cambios.

Configuración de Prevención de exploits

Configuración	Descripción
Acción al detectar una amenaza	**Informar**. Si se selecciona este elemento, cuando Kaspersky Endpoint Security detecta un exploit, registra una entrada que contiene información sobre el exploit y agrega información sobre él a la lista de amenazas activas. **Bloquear**. Si se ha seleccionado esta opción, al detectar un exploit, Kaspersky Endpoint Security bloquea la operación de este exploit y crea una entrada de registro con información sobre este exploit.

Configuración del componente Motor de reparación

Puede configurar el componente Motor de reparación de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Protección contra amenazas de host → Análisis de comportamiento → Motor de reparación**.
  5. Habilite o deshabilite el componente usando el conmutador **Motor de reparación**.
  6. Configure el componente Motor de reparación.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección avanzada contra amenazas → Motor de reparación**.
  5. Habilite o deshabilite el componente usando el conmutador **Motor de reparación**.
  6. Configure el componente Motor de reparación.
  7. Guarde los cambios.

Comunicación y protección web

Configurar la protección contra amenazas de correo

Puede configurar el componente Protección contra amenazas de correo de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Comunicación y Protección web** → **Protección contra amenazas de correo**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de correo**.
  6. Configure el componente Protección contra amenazas de correo.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección básica contra amenazas** → **Protección contra amenazas web**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de correo**.
  6. Configure el componente Protección contra amenazas de correo.
  7. Guarde los cambios.

Configuración de la Protección contra amenazas de correo

Configuración	Descripción
Acción al detectar una amenaza	**Desinfectar; eliminar si falla la desinfección** Cuando se detecta que un mensaje entrante o saliente contiene un objeto infectado, la aplicación intenta desinfectar el objeto. El usuario puede acceder al mensaje y al objeto seguro. Si el objeto no puede desinfectarse, la aplicación lo elimina. La aplicación agrega información sobre la acción realizada al asunto del mensaje, por ejemplo, *[Se procesó el mensaje] <asunto del mensaje>*. **Bloquear**. Cuando se detecta que un mensaje entrante contiene un objeto infectado, la aplicación agrega una advertencia al asunto del mensaje. El usuario podrá acceder al mensaje con el archivo adjunto original. Cuando se detecta que un mensaje saliente contiene un objeto infectado, la aplicación bloquea la transmisión del mensaje y el cliente de correo electrónico muestra un error.
No analizar archivos comprimidos de más de (MB)	Si esta casilla está seleccionada, el componente Protección contra amenazas de correo excluye del análisis los archivos adjuntos en los mensajes de correo electrónico si el tamaño excede el valor especificado. Si se desactiva la casilla, el componente Protección contra amenazas de correo analiza los archivos adjuntos de correo de cualquier tamaño.
Omitir archivo que se analice durante más de (s)	Si la casilla está seleccionada, el tiempo asignado al análisis de archivos adjuntos en los mensajes de correo se limita al período especificado.

Configurar el componente Protección contra amenazas web

Puede configurar el componente Protección contra amenazas de red de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Comunicación y Protección web** → **Protección contra amenazas web**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas web**.
  6. Configure el componente Protección contra amenazas web.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección básica contra amenazas** → **Protección contra amenazas web**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas web**.
  6. Configure el componente Protección contra amenazas web.
  7. Guarde los cambios.

Configuración	Descripción
Direcciones web de confianza	Lista de direcciones web que la Protección contra amenazas web considera de confianza. El componente no analiza el tráfico entrante y saliente de estas direcciones en busca de amenazas. Esta lista de direcciones de confianza se puede usar, por ejemplo, cuando el componente Protección contra amenazas web interfiere en la descarga de un archivo de un sitio web conocido.
Exclusiones del análisis	Una *exclusión de análisis* es un conjunto de condiciones que deben cumplirse para que Kaspersky Endpoint Security no analice un objeto en particular en busca de virus y otras amenazas. A su vez, la exclusión del análisis hacen posible el uso seguro de software legítimo que puede ser explotado por criminales para dañar el equipo o los datos de usuario. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre las aplicaciones legítimas que los intrusos pueden utilizar para poner en riesgo su equipo o los datos de los usuarios están disponibles en el sitio web de la Enciclopedia TI de Kaspersky.
Acción al detectar una amenaza	**Bloquear**. Cuando esta opción está seleccionada y se detecta un objeto infectado en el tráfico web, el componente Protección contra amenazas web bloquea el acceso al objeto y muestra un mensaje en el navegador. **Solicitar acción**. Kaspersky Endpoint Security muestra una notificación con información sobre el tipo de malware que infectó el objeto del tráfico web y le solicita que seleccione la acción que Kaspersky Endpoint Security debe realizar sobre este objeto. Las acciones disponibles pueden variar según el estado del objeto.

Configurar la Protección contra amenazas de red

Puede configurar el componente Protección contra amenazas de red de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Comunicación y Protección web** → **Protección contra amenazas de red**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de red**.
  6. Configure el componente Protección contra amenazas de red.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección básica contra amenazas** → **Protección contra amenazas de red**.
  5. Habilite o deshabilite el componente usando el conmutador **Protección contra amenazas de red**.
  6. Configure el componente Protección contra amenazas de red.
  7. Guarde los cambios.

Configuración de Protección contra amenazas de red

Configuración	Descripción
Direcciones IP de confianza	Lista de direcciones IP de dispositivos de confianza. El componente Protección contra amenazas de red no bloquea la actividad de red de estas direcciones.
Acción al detectar una amenaza	**Bloquear**. Cuando se detecta una amenaza, Protección contra amenazas de red bloquea el ataque. **Bloquear ataque y dispositivo atacante durante (min)**. Si se habilita esta opción, el componente Protección contra amenazas de red agrega el equipo atacante a la lista de elementos bloqueados. Esto significa que, cuando se detecte el primer intento de ataque, el componente Protección contra amenazas de red bloqueará la conexión al equipo agresor por el tiempo especificado. Este bloqueo protege automáticamente el equipo del usuario contra futuros posibles ataques de red de la misma dirección. El tiempo mínimo que un equipo atacante debe pasar en la lista de bloqueo es de un minuto. El tiempo máximo es de 999 minutos.

Configure el componente Firewall

Puede configurar el componente Firewall de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Comunicación y Protección web** → **Firewall**.
  5. Habilite o deshabilite el componente usando el conmutador **Firewall**.
  6. Configure el componente Firewall.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Protección básica contra amenazas** → **Firewall**.
  5. Habilite o deshabilite el componente usando el conmutador **Firewall**.
  6. Configure el componente Firewall.
  7. Guarde los cambios.

Configuración	Descripción
Reglas de paquetes de red	Tabla con una lista de reglas para paquetes de red. Las reglas de paquetes de red sirven para imponer restricciones en los paquetes de red, sin tener en cuenta la aplicación. Dichas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. La tabla enumera reglas de paquetes de red preconfiguradas recomendadas por Kaspersky para la protección óptima del tráfico de red de equipos que se ejecutan en sistemas operativos macOS. Firewall define la prioridad de ejecución de cada regla de paquetes de red. Firewall procesa las reglas de paquetes de red en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba a abajo. Cuando se detecta una conexión de red, el componente busca la primera regla de paquetes pertinente y la aplica a la actividad de red, que se permitirá o bloqueará según corresponda. Las reglas posteriores que también sean aplicables a la conexión de red se desestimarán. Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones.
Redes disponibles	Esta tabla contiene información sobre conexiones de red detectadas por el Firewall en el equipo. Están disponibles los siguientes tipos de conexión de red: • La red no está protegida por aplicaciones antimalware, firewalls ni filtros (como Wi-Fi en un café). Cuando el usuario opera un equipo que está conectado a dicha red, Firewall bloquea el acceso a los archivos y las impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos a través de carpetas compartidas y acceso remoto al escritorio de este equipo. El Firewall filtra la actividad de red de cada aplicación de acuerdo con las reglas de red definidas para ella. • Red para usuarios con acceso restringido a archivos e impresoras en este equipo (por ejemplo, para una LAN corporativa o una red doméstica). • Red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de las redes con este estado.

Controles de seguridad

Configurar el componente Control de dispositivos

Puede configurar el componente Control de dispositivos de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Controles de seguridad** → **Control de dispositivos**.
  5. Habilite o deshabilite el componente usando el conmutador **Control de dispositivos**.
  6. Configurar el Control de dispositivos
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Controles de seguridad → Control de dispositivos**.
  5. Habilite o deshabilite el componente usando el conmutador **Control de dispositivos**.
  6. Configurar el Control de dispositivos
  7. Guarde los cambios.

La configuración de Control de dispositivos

Configuración	Descripción
Dispositivos de confianza	Una lista con los dispositivos de confianza y los usuarios que tienen acceso a esos dispositivos.
Dispositivos y redes Wi-Fi	Una lista con todos los tipos de dispositivos disponibles según la clasificación del componente Control de dispositivos, junto con sus respectivos estados de acceso.

Configurar el componente Control web

Puede configurar el componente Control web de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Controles de seguridad → Control web**.
  5. Habilite o deshabilite el componente usando el conmutador **Control web**.
  6. Configure el componente Control web.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Controles de seguridad → Control web**.
5. Habilite o deshabilite el componente usando el conmutador **Control web**.
6. Configure el componente Control web.
7. Guarde los cambios.

Configuración de Control web

Configuración	Descripción
Lista de reglas	Lista con las reglas de acceso a recursos web. Cada regla tiene una prioridad. Cuanto más alta esté una regla en la lista, mayor será su prioridad. La regla de mayor prioridad es la que Control web utiliza para regular el acceso a sitios web que se han agregado a más de una regla.
Acción predeterminada	La regla de acceso a los recursos web que no están contemplados en ninguna otra regla. Las siguientes opciones están disponibles: • **Permitir todo lo que no esté en la lista de reglas**. • **Bloquear todo excepto la lista de reglas**.

Cifrado de datos

Puede configurar el componente Cifrado de datos de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**
  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. La sección **Cifrado de datos**.
  5. Habilite o deshabilite el componente usando el conmutador **Cifrado de datos**.
  6. Configure el componente Cifrado de datos.
  7. Guarde los cambios.
- **Usando el complemento de Kaspersky Endpoint Security**
  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. La sección **Cifrado de datos**.
  5. Habilite o deshabilite el componente usando el conmutador **Cifrado de disco FileVault**.

6. Configure el componente Cifrado de datos.
7. Guarde los cambios.

Configuración de cifrado de disco completo.

Configuración	Descripción
Acción en los dispositivos	**Cifrar todos los discos duros**. Si se selecciona esta opción, cuando se aplique la directiva, la aplicación cifrará todos los discos duros. **Descifrar todos los discos duros**. Si se selecciona esta opción, cuando se aplique la directiva, la aplicación descifrará todos los discos duros que se encuentren cifrados.

Configuración general

Configuración de detección

Puede ajustar la configuración de detección de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**
  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general** → **Configuración de detección**.
  5. Ajuste la configuración de detección.
  6. Guarde los cambios.
- **Usando el complemento de Kaspersky Endpoint Security**
  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración adicional** → **Protección**.
  5. Ajuste la configuración de detección.
  6. Guarde los cambios.

Configuración de detección

Configuración	Descripción
Detección de otros tipos de objetos	Independientemente de la configuración de la aplicación ajustada, Kaspersky Endpoint Security siempre detecta y bloquea virus, gusanos, troyanos y herramientas maliciosas. Estos pueden ocasionar daños importantes al equipo. Además, puede habilitar la detección de los siguientes tipos de objetos: • **Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales**. Estas aplicaciones no tienen funciones malintencionadas, pero un intruso podría utilizarlas con fines negativos. Los detalles sobre las aplicaciones legítimas que los intrusos pueden utilizar para poner en riesgo su equipo o los datos de los usuarios están disponibles en el sitio web de la Enciclopedia TI de Kaspersky.

Kaspersky Security Network

Puede configurar Kaspersky Security Network de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general** → **Kaspersky Security Network**.
  5. Use el conmutador **Kaspersky Security Network (KSN)** para habilitar o deshabilitar el componente.
  6. Configure el componente de Kaspersky Security Network.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
  5. Use el conmutador **Kaspersky Security Network** para habilitar o deshabilitar el componente.
  6. Configure el componente de Kaspersky Security Network.
  7. Guarde los cambios.

Configuración de detección

Configuración	Descripción
Utilizar el modo KSN extendido	El *modo KSN extendido* es un modo por el cual Kaspersky Endpoint Security remite información adicional a Kaspersky. Kaspersky Endpoint Security utiliza KSN para detectar amenazas independientemente del estado del interruptor.
Usar modo nube	*Modo nube* es el nombre que se le da a un modo de funcionamiento de Kaspersky Endpoint Security, en el cual la aplicación utiliza una versión reducida de las bases de datos antivirus. Utilizar estas bases de datos no afecta la capacidad de usar Kaspersky Security Network. Cuando la aplicación utiliza las bases de datos reducidas en lugar de las normales, su consumo de RAM disminuye a cerca de la mitad. Si ha optado por no participar en Kaspersky Security Network o si ha desactivado el modo nube, Kaspersky Endpoint Security descargará la versión completa de las bases de datos antivirus de los servidores de Kaspersky. Si la casilla está seleccionada, Kaspersky Endpoint Security usa una versión reducida de las bases de datos antivirus para tener un menor impacto en los recursos del sistema operativo. Kaspersky Endpoint Security descarga la versión ligera de bases de datos antivirus durante la siguiente actualización después de que la casilla se seleccionó. Si la casilla está desactivada, Kaspersky Endpoint Security usa la versión completa de las bases de datos antivirus. Kaspersky Endpoint Security descarga la versión completa de bases de datos antivirus durante la siguiente actualización después de que la casilla se desactivó.
Usar el Servidor de administración como servidor proxy de KSN	Cuando esta casilla está activada, Kaspersky Endpoint Security usa el servicio proxy de KSN. Los parámetros de este servicio se configuran a través de las propiedades del Servidor de administración.
Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible	Cuando esta casilla está seleccionada y el servicio KSN Proxy no está disponible, Kaspersky Endpoint Security usa los servidores de KSN. Los servidores de KSN pueden estar alojados tanto en la infraestructura de Kaspersky como en la de terceros (cuando se utiliza Kaspersky Private Security Network).

Interacción con el usuario

Puede ajustar la configuración de la interfaz de la aplicación, así como la configuración para la interacción de la aplicación con el usuario de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general** → **Interacción del usuario**.
  5. Ajuste la configuración de interacción con el usuario.
  6. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración adicional → Interacción con el usuario**.
  5. Ajuste la configuración de interacción con el usuario.
  6. Guarde los cambios.

Configuración de interacción con el usuario

Configuración	Descripción
Iniciar Kaspersky Endpoint Security en el arranque del equipo (recomendado)	Si esta función está habilitada, Kaspersky Endpoint Security se inicia después de cargado el sistema operativo y protege al equipo durante toda la sesión. Si esta función está deshabilitada, Kaspersky Endpoint Security no se inicia después de cargado el sistema operativo, sino cuando el usuario lo inicia manualmente. La protección del equipo está desactivada y los datos del usuario pueden estar expuestos a amenazas.
Mostrar el ícono de la aplicación	Esta casilla habilita o deshabilita la visualización del ícono de la aplicación en la barra de menús de un equipo remoto. Si la casilla está seleccionada, el ícono de la aplicación se muestra en la barra de menús. Si la casilla no está seleccionada, el ícono de la aplicación no se muestra en la barra de menús. Esta casilla está seleccionada por defecto.
Administrar actualizaciones de forma local	Si la casilla está seleccionada, se habilita la administración local de las actualizaciones de Kaspersky Endpoint Security en un equipo remoto. Si la casilla no está seleccionada, las actualizaciones de Kaspersky Endpoint Security en un equipo remoto solo se pueden administrar mediante el complemento de administración de Kaspersky Endpoint Security en Kaspersky Security Center.
Administrar claves de forma local	Si la casilla está seleccionada, se habilita la administración local de las claves de Kaspersky Endpoint Security en un equipo remoto. Si la casilla no está seleccionada, las claves de Kaspersky Endpoint Security en un equipo remoto solo se pueden administrar mediante el complemento de administración de Kaspersky Endpoint Security en Kaspersky Security Center.
Salir de la aplicación	Si la casilla está seleccionada, el comando **Salir** se muestra en el menú contextual del ícono de la aplicación. El usuario de un equipo remoto puede salir de Kaspersky Endpoint Security en el equipo. Si la casilla no está seleccionada, el comando **Salir** no se muestra en el menú contextual del ícono de la aplicación. El usuario de un equipo remoto no puede salir de Kaspersky Endpoint Security en el equipo.

Autoprotección

Puede ajustar la configuración de Autoprotección de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Autoprotección**.
5. Habilite o deshabilite el componente usando el conmutador **Protección con contraseña**.
6. Configure Autoprotección.
7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración adicional** → **Interacción con el usuario**.
5. Habilite o deshabilite el componente usando el conmutador **Protección con contraseña**.
6. Configure Protección con contraseña.
7. Guarde los cambios.

Configuración de Autoprotección

Configuración	Descripción
Protección con contraseña	Cuando este conmutador está activado y el usuario intenta realizar una acción alcanzada por la función Protección con contraseña, Kaspersky Endpoint Security solicita la contraseña en cuestión. El alcance de la protección con contraseña se compone de las acciones que se han prohibido (por ejemplo, la desactivación de los componentes de protección) y las cuentas de usuario para las que se han prohibido tales acciones. Cuando habilite la protección con contraseña, Kaspersky Endpoint Security le pedirá que establezca la contraseña para la cuenta de KLAdmin.

Rendimiento

Puede ajustar la configuración de rendimiento de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración general** → **Rendimiento**.

5. Ajuste la configuración de rendimiento.
6. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración adicional → Protección**.
  5. Ajuste la configuración de rendimiento.
  6. Guarde los cambios.

Configuración de rendimiento

Configuración	Descripción
Posponer u omitir las tareas programadas cuando el equipo funciona con carga de batería	Si esta función está habilitada, Kaspersky Endpoint Security pasa al modo de ahorro de energía. Kaspersky Endpoint Security *cancela* las tareas programadas. Las tareas de análisis y actualización podrán iniciarse manualmente cuando sea necesario.
Restringir el uso de CPU para las tareas del análisis	Para optimizar el rendimiento de Kaspersky Endpoint Security, puede limitar el uso de la CPU por parte de la tarea de análisis de malware. Si esta función está habilitada, la carga promedio en todos los núcleos de la CPU de la tarea de análisis de malware alcanza el valor especificado.

Informes y repositorios

Puede ajustar la configuración de Informes y repositorios de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general → Informes y repositorios**.
  5. Ajuste la configuración de Informes y repositorios.
  6. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración adicional → Informes y depósito de copias de seguridad**.
  5. Ajuste la configuración de Informes y repositorios.
  6. Guarde los cambios.

Configuración de Informes y repositorios

Configuración	Descripción
Eliminar informes después de (días)	Si la casilla está seleccionada, los informes se conservarán solo por el tiempo definido como máximo. Después de ese plazo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe.
Conservar solo eventos recientes	Si se selecciona esta casilla, cada vez que se inicia la tarea, Kaspersky Endpoint Security elimina la información sobre los eventos no críticos que se produjeron desde el inicio anterior de la tarea, pero conserva notas importantes en el informe (por ejemplo, información sobre los objetos maliciosos detectados).
Registrar los eventos no críticos	Si la casilla está seleccionada, Kaspersky Endpoint Security registra eventos no críticos en el informe (como eventos informativos). Los eventos no críticos no afectan la protección.
Eliminar objetos después de (días)	Si la casilla está seleccionada, los archivos se conservarán solo por el tiempo definido como máximo. Al caducar el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos de Copia de seguridad.

Configuración de red

Puede ajustar la configuración de red de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general → Configuración de red**.
  5. Ajuste la configuración de red.
  6. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.

3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Configuración adicional** → **Red**.
5. Ajuste la configuración de red.
6. Guarde los cambios.

Configuración de red

Configuración	Descripción
Certificados raíz de confianza	Lista de certificados raíz de confianza. Kaspersky Endpoint Security le permite instalar certificados raíz de confianza en equipos de usuarios si, por ejemplo, necesita desplegar un nuevo centro de certificados. La aplicación le permite agregar un certificado a un almacén de certificados especial de Kaspersky Endpoint Security. En este caso, el certificado se considera de confianza solo para la aplicación Kaspersky Endpoint Security. En otras palabras, el usuario puede acceder a un sitio web con el certificado nuevo en el navegador. Si otra aplicación intenta acceder al sitio web, es posible que se produzca un error de conexión debido a un problema de certificados.
Servidor proxy	La configuración del servidor proxy utilizado para el acceso a Internet de los usuarios de los equipos cliente. Kaspersky Endpoint Security utiliza estas opciones de configuración para ciertos componentes de protección, inclusive para la actualización de bases de datos y módulos de aplicación.
Autenticarse ante el servidor proxy	Si se selecciona esta casilla, la aplicación usa la autenticación con un nombre de usuario y una contraseña cuando se conecta al servidor proxy.
No usar el servidor proxy para las direcciones locales	Si la casilla está seleccionada, Kaspersky Endpoint Security no utiliza un servidor proxy cuando realiza una actualización desde una carpeta compartida.
Análisis de conexiones cifradas	Esta función permite que los componentes Protección contra amenazas web, Protección contra amenazas de correo y Control web supervisen y administren conexiones cifradas (HTTPS).

Configuración de telemetría

Puede ajustar la configuración de telemetría de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**
  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Configuración general** → **Configuración de telemetría**.
  5. Ajuste la configuración de telemetría.
  6. Guarde los cambios.
- **Usando el complemento de Kaspersky Endpoint Security**
  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.

4. Vaya a **Configuración adicional** → **Zona de confianza** → **Configuración de telemetría**.

5. Ajuste la configuración de telemetría.

6. Guarde los cambios.

Configuración de telemetría

Configuración	Descripción
Telemetría de EDR Expert (on-premise)	**Importar** y **Exportar**. Puede exportar la configuración de telemetría de EDR Expert (on-premise) a un archivo JSON. A continuación, puede modificar el archivo para, por ejemplo, agregar una gran cantidad de identificadores de eventos. También puede utilizar la función de exportación/importación para realizar una copia de seguridad de la configuración de eventos enviados o para migrar la lista a otra directiva.
Exclusiones generales	Para optimizar los datos transmitidos, puede configurar reglas de exclusión para ciertos tipos de eventos. Kaspersky Endpoint Security no recopila telemetría que se rija por dicha regla. Esto le permite reducir el tráfico y evitar el procesamiento de eventos de objetos y procesos de confianza.

Configuración de eventos

Mientras la aplicación está funcionando, ocurren varios *eventos*. Pueden ser puramente informativos o contener información crítica. Por ejemplo, la aplicación puede usar un evento para notificar sobre una actualización exitosa de la base de datos o señalar un error de un componente que debe repararse.

Los eventos de Kaspersky Endpoint Security pueden clasificarse en las siguientes clases de gravedad:

- *Eventos 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. Recomendamos que no deshabilite las notificaciones sobre eventos críticos.

- *Errores funcionales*: eventos que ocurren cuando Kaspersky Endpoint Security no funciona correctamente (error de procesamiento, error de configuración de la tarea). Dichos eventos no amenazan directamente la seguridad del equipo, pero requieren su intervención para asegurarse de que Kaspersky Endpoint Security funcione correctamente y proteja sus dispositivos.

- *Advertencias*: eventos que no precisan su atención inmediata, pero que más adelante pueden representar una amenaza para la seguridad del equipo.

- *Mensajes informativos*: eventos notificados para su información.

Independientemente de si las notificaciones están habilitadas o deshabilitadas, Kaspersky Endpoint Security registra información sobre todos los eventos de la aplicación en los informes de la aplicación.

Configuración de actualización

Puede ajustar la configuración de actualización de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

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

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

     Se abre la ventana de propiedades de la directiva.

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

4. Vaya a **Configuración general** → **Actualización**.
5. Ajuste la configuración de actualización.
6. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección Actualización.
5. Ajuste la configuración de actualización.
6. Guarde los cambios.

Configuración de actualización

Configuración	Descripción
Orígenes de actualizaciones	Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security. Como origen de actualizaciones, puede utilizar el servidor de Kaspersky Security Center, los servidores de actualizaciones de Kaspersky o una carpeta local o de red dispuesta para tal fin. Si los servidores de actualizaciones de Kaspersky no están disponibles, Kaspersky Endpoint Security puede usar dominios alternativos para recibir actualizaciones de bases de datos y módulos de aplicaciones. Para obtener los detalles, consulte la Base de conocimientos del Servicio de soporte técnico. La lista por defecto de orígenes de actualizaciones incluye a los servidores de actualización de Kaspersky Security Center y de Kaspersky. Puede agregar otros orígenes de actualizaciones a la lista. Puede especificar servidores HTTP/FTP y carpetas compartidas como origen de las actualizaciones. Kaspersky Endpoint Security no admite actualizaciones que provengan de servidores HTTPS, a menos que sean servidores de actualización de Kaspersky. Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno tras otro, comenzando por el principio de la lista, y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible. De manera predeterminada, Kaspersky Endpoint Security usa el servidor de Kaspersky Security Center como el primer origen de actualizaciones. Esto ayuda a conservar el tráfico al actualizar. Si no se aplica una directiva al equipo, los servidores de Kaspersky se seleccionan como el primer origen de actualizaciones en la configuración de la tarea local Actualizar, ya que es posible que la aplicación no tenga acceso al servidor de Kaspersky Security Center.

Agentes incorporados

Configurar Managed Detection and Response

Puede configurar el componente Managed Detection and Response de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Configuración de agentes integrados** → **Managed Detection and Response**.
  5. Habilite o deshabilite el componente usando el conmutador **Managed Detection and Response**.
  6. Configure el componente Managed Detection and Response
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Detection and Response** → **Managed Detection and Response**.
  5. Habilite o deshabilite el componente usando el conmutador **Managed Detection and Response**.
  6. Configure el componente Managed Detection and Response
  7. Guarde los cambios.

Configuración del componente Managed Detection and Response

Configuración	Descripción
Archivo de configuración de MDR	El archivo BLOB contiene la ID de cliente e información sobre la licencia de Kaspersky Managed Detection and Response. El archivo BLOB se encuentra en el archivo comprimido ZIP del archivo de configuración de MDR. Puede obtener el archivo comprimido ZIP en la consola de Kaspersky Managed Detection and Response. Para más información sobre el archivo BLOB, consulte la ayuda de Kaspersky Managed Detection and Response.

Configurar Endpoint Detection and Response

Puede configurar el componente Endpoint Detection and Response de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Configuración de agentes integrados** → **Endpoint Detection and Response**.
  5. Habilite o deshabilite el componente usando el conmutador **Managed Detection and Response**.
  6. Configure el componente Endpoint Detection and Response.
  7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

  1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.
     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a **Detection and Response** > **Endpoint Detection and Response**.
  5. Habilite o deshabilite el componente usando el conmutador **Endpoint Detection and Response**.
  6. Configure el componente Endpoint Detection and Response.
  7. Guarde los cambios.

Configuración de Endpoint Detection and Response

Configuración	Descripción
Aislamiento de la red	Aislamiento automático del equipo de la red en respuesta a amenazas detectadas. Cuando el aislamiento de la red está activado, la aplicación corta todas las conexiones activas y bloquea todas las conexiones nuevas de TCP/IP del equipo. La aplicación solo deja activas las siguientes conexiones: • Conexiones que figuran en Exclusiones del aislamiento de la red. • Conexiones iniciadas por los servicios de Kaspersky Endpoint Security. • Conexiones iniciadas por el Agente de red de Kaspersky Security Center.
Desbloquear automáticamente el dispositivo aislado en (horas)	Aislamiento de la red se puede desactivar de forma automática después de un tiempo especificado o manualmente.

Configuración	Descripción
Exclusiones de aislamiento de la red	Lista de reglas para las exclusiones del aislamiento de la red. Las conexiones de red que coinciden con las reglas no se bloquean en los equipos cuando el aislamiento de la red está activado. Para configurar las exclusiones de aislamiento de la red, puede utilizar una lista de *perfiles de la red estándar*. De manera predeterminada, las exclusiones incluyen perfiles de red con reglas que garantizan el funcionamiento ininterrumpido de los dispositivos con el servidor DNS/DHCP y los roles de cliente DNS/DHCP. También puede modificar la configuración de los perfiles de red estándar o definir exclusiones manualmente. Las exclusiones especificadas en las propiedades de la directiva se aplican solo si el aislamiento de la red se activa automáticamente en respuesta a una amenaza detectada. Las exclusiones especificadas en las propiedades del equipo se aplican solo si Aislamiento de la red se activa manualmente en las propiedades del equipo en la consola de Kaspersky Security Center o en los detalles de la alerta.
Prevención de ejecución	Controle la ejecución de los archivos ejecutables y scripts y la apertura de archivos en formato de Office. Por ejemplo, puede evitar la ejecución de aplicaciones que se consideran inseguras en el equipo seleccionado. La prevención de la ejecución es compatible con un conjunto de extensiones de archivos de Office y un conjunto de intérpretes de script. Para usar el componente Prevención de ejecución, debe agregar reglas de prevención de ejecución.
Acción ante operaciones de ejecución o apertura de un objeto prohibido	**Bloquear y agregar al registro de eventos**. En este modo, la aplicación bloquea la ejecución de objetos o la apertura de documentos que coinciden con los criterios de la regla de prevención. La aplicación también publica un evento sobre los intentos de ejecutar objetos o abrir documentos en el registro de eventos del sistema y en Kaspersky Security Center. **Agregar a registros de eventos**. En este modo, Kaspersky Endpoint Security publica un evento sobre los intentos de ejecutar objetos ejecutables o abrir documentos que coinciden con los criterios de la regla de prevención en el registro de eventos del sistema y en Kaspersky Security Center, pero no bloquea el intento de ejecutar o abrir el objeto o documento. Este modo está seleccionado de manera predeterminada.
Reglas de prevención de ejecución	La opción *Regla de prevención de ejecución* es un conjunto de criterios que la aplicación tiene en cuenta al reaccionar a la ejecución de un objeto, por ejemplo, al bloquear la ejecución de un objeto. La aplicación identifica archivos por las rutas o sumas de control que se calculan mediante algoritmos hash MD5 y SHA256.
Cloud Sandbox	*Cloud Sandbox* es una tecnología que le permite detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Cloud Sandbox para su análisis. Cloud Sandbox ejecuta estos archivos en un entorno aislado para identificar actividades maliciosas y decide sobre su reputación. Los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Cloud Sandbox detectó un archivo malicioso, Kaspersky Endpoint Security realiza la acción adecuada para eliminar esta amenaza en todos los equipos donde se detecte este archivo. Se necesita una conexión de KSN para obtener información sobre los objetos que se analizan.

Configurar Endpoint Detection and Response Expert (on-premise)

Puede configurar el componente Endpoint Detection and Response Expert (on-premise) de una de las siguientes maneras:

- **Usando el Unified Protection and Management Plug-in**

  1. En la ventana principal de Web Console, seleccione **Administración de activos → Directivas**.
  2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

     Se abre la ventana de propiedades de la directiva.
  3. Seleccione la pestaña **Configuración de la aplicación**.
  4. Vaya a la sección **Configuración de agentes integrados → Endpoint Detection and Response Expert (on-premise)**.

5. Habilite o deshabilite el componente usando el conmutador **Managed Detection and Response Expert (on-premise)**.
6. Configure el componente Managed Detection and Response Expert (on-premise)
7. Guarde los cambios.

- **Usando el complemento de Kaspersky Endpoint Security**

1. En la ventana principal de Web Console, seleccione **Administración de activos** → **Directivas**.
2. Haga clic en el nombre de la directiva de Kaspersky Endpoint Security.

   Se abre la ventana de propiedades de la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Detection and Response** → **Endpoint Detection and Response Expert (on-premise)**.
5. Habilite o deshabilite el componente usando el conmutador **Managed Detection and Response Expert (on-premise)**.
6. Configure el componente Managed Detection and Response Expert (on-premise)
7. Guarde los cambios.

Configuración del componente Endpoint Detection and Response Expert (on-premise)

Configuración	Descripción
Solución Endpoint Detection and Response Expert	Soluciones de Endpoint Detection and Response Expert con las que Kaspersky Endpoint Security puede integrarse. • **Endpoint Detection and Response Expert (versión 7.1 o anterior)** • **Endpoint Detection and Response Expert (versión 8.0 o posterior)**
Configuración de conexión	Administre la siguiente configuración de conexión con el servidor de recopilación de telemetría o KATA: • **Tiempo de espera de la conexión al servidor**. Tiempo de espera máximo de respuesta del servidor de Central Node. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse a un servidor de Central Node diferente. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de Central Node. Puede obtener un certificado TLS en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la ayuda de Kaspersky Anti Targeted Attack Platform). • **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de Central Node. Para usar la autenticación bidireccional, debe habilitarla en la configuración del servidor de Central Node y, a continuación, obtener un contenedor criptográfico y establecer una contraseña para proteger el contenedor criptográfico. Un contenedor criptográfico es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la ayuda de Kaspersky Anti Targeted Attack Platform). Después de configurar los ajustes de Central Node, también debe habilitar la autenticación bidireccional en los ajustes de Kaspersky Endpoint Security y cargar un contenedor criptográfico protegido con contraseña. El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor de cifrado sin una contraseña.
Enviar solicitud de sincronización al servidor cada (min) *(Solo está disponible para Endpoint Detection and Response Expert versión 7.1 o anteriores).*	Frecuencia de las solicitudes de sincronización enviadas al servidor. Durante la sincronización, Kaspersky Endpoint Security envía información sobre las tareas y la configuración de la aplicación modificada.

Configuración	Descripción
Conexión a servidores KATA/Conexión a servidores de recopilación de telemetría	Ingrese la dirección IP y el puerto de conexión con el servidor de Kaspersky Anti Targeted Attack Platform o con el servidor de recopilación de telemetría. Puede agregar varias direcciones de Central Node (para KATA) o del servidor de recopilación de telemetría. Kaspersky Endpoint Security intenta conectarse al servidor en la primera dirección IP. Si no se pude establecer una conexión, Kaspersky Endpoint Security intenta conectarse a la segunda dirección IP de la lista y así sucesivamente. Las soluciones EDR (KATA) y EDR Expert (on-premise) tienen arquitecturas diferentes. Para el procesamiento de telemetría, EDR Expert (on-premise) usa un servidor de recopilación de telemetría; EDR (KATA) usa un servidor de Central Node. Por lo tanto, si está integrando la aplicación con EDR Expert (on-premise), debe agregar un servidor de recopilación de telemetría.
Enviar telemetría a KATA/Enviar telemetría a servidores de recolección de telemetría	Esta función permite evitar por completo el envío de telemetría al servidor de KATA o al servidor de recopilación de telemetría, según la solución seleccionada. Por ejemplo, si está usando Kaspersky Anti Targeted Attack Platform junto con otra solución que también usa telemetría, puede desactivar el envío de telemetría para KATA (EDR). Esto le permite optimizar la carga del servidor para estas soluciones. Si tiene implementada la solución Managed Detection and Response y KATA (EDR), puede usar la telemetría de MDR y crear tareas de Respuesta ante amenazas en KATA (EDR).
Retraso máximo de transmisión de eventos (s)	La aplicación se sincroniza con el servidor para enviar eventos después de que caduque el intervalo de sincronización.
Habilitar regulación de solicitudes	Esta función permite optimizar la carga en el servidor. Si la casilla de verificación está seleccionada, la aplicación restringe los eventos transmitidos. Si la cantidad de eventos supera los límites configurados, Kaspersky Endpoint Security deja de enviar eventos. **Cantidad máxima de eventos por hora**. La aplicación analiza la secuencia de datos de telemetría y restringe el envío de eventos si la secuencia de eventos supera el límite configurado de eventos por hora. Kaspersky Endpoint Security reanuda el envío de eventos después de una hora. Si la aplicación está instalada en un servidor, el flujo de datos de telemetría es mayor. Para los servidores, se recomienda aumentar el valor a 60 000 eventos por hora. **Porcentaje de exceso de límite de eventos**. La aplicación ordena los eventos por tipo (por ejemplo, eventos de "cambios en el registro") y restringe la transmisión de eventos si la proporción de eventos del mismo tipo con respecto al número total de eventos supera el porcentaje límite configurado. Kaspersky Endpoint Security reanuda el envío de eventos cuando la proporción entre otros eventos y el número total de eventos vuelve a ser lo suficientemente grande.
Conexión a servidores de respuesta *(Solo está disponible para Endpoint Detection and Response Expert versión 8.0 o posteriores).*	Configuración de la conexión a servidores de respuesta. Ingrese la dirección IP del servidor de respuesta (IPv4 o IPv6) y el puerto para conectarse con el servidor. Puede agregar varias direcciones de servidores de respuestas. Kaspersky Endpoint Security intenta conectarse al servidor en la primera dirección IP. Si no se pude establecer una conexión, Kaspersky Endpoint Security intenta conectarse a la segunda dirección IP de la lista y así sucesivamente.
Configuración de conexión *(Solo está disponible para Endpoint Detection and Response Expert versión 8.0 o posteriores).*	Configure los siguientes parámetros para la conexión con el servidor de respuesta: • **Tiempo de espera de la conexión al servidor**. Tiempo de espera máximo de respuesta del servidor de respuesta. Cuando se agota el tiempo de espera, Kaspersky Endpoint Security intenta conectarse con otro servidor de respuesta. • **Certificado del servidor**. Certificado TLS para establecer una conexión de confianza con el servidor de respuesta. • **Usar autenticación bidireccional**. Autenticación bidireccional al establecer una conexión segura entre Kaspersky Endpoint Security y el servidor de respuesta. Para usar la autenticación bidireccional, debe habilitarla en la configuración del servidor de respuesta y, a continuación, obtener un criptocontenedor y establecer una contraseña para protegerlo. Un *contenedor criptográfico* es un archivo de almacenamiento PFX con un certificado y una clave privada. Puede obtener un contenedor criptográfico en la consola de Kaspersky Anti Targeted Attack Platform (consulte las instrucciones en la Ayuda de Kaspersky Anti Targeted Attack Platform). Después de configurar el servidor de respuesta, también debe habilitar la autenticación bidireccional en la configuración de Kaspersky Endpoint Security y cargar un criptocontenedor protegido con contraseña. El contenedor criptográfico debe tener protección con contraseña. No es posible agregar un contenedor de cifrado sin una contraseña.

Crear una tarea

Esta sección indica 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 por 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
- Reversión
- Agregar clave

Crear una tarea

1. En la sección **Dispositivos** a la izquierda, seleccione la sección **Tareas**.
2. Haga clic en **Agregar**.
   Se inicia el Asistente para agregar tareas.
3. En la lista desplegable **Aplicación**, seleccione **Kaspersky Endpoint Security for Mac 12.2.1**.
4. En la lista desplegable **Tipo de tarea**, seleccione la tarea que desea crear.
5. Si es necesario, edite el nombre de la tarea en el campo **Nombre de la tarea**.
6. Seleccione dispositivos a los que se asignará la tarea.
7. Configure los parámetros 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 la tarea**, puede proceder a modificar la configuración predeterminada de la tarea. Si no selecciona esta casilla de verificación, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada de la tarea más tarde, en cualquier momento.

Puede realizar las siguientes acciones en las tareas:

- Inicie y detenga las tareas.
- Configure los parámetros de la tarea.
- Realice un seguimiento del progreso de una tarea.
- Copie y mueva tareas de un grupo a otro.
- Elimine 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.

Configuración de la tarea Analizar

En la pestaña **Configuración 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 Analizar

1. Vaya a **Dispositivos** > **Tareas**.
2. Haga doble clic en una tarea con el tipo de tarea **Análisis**.
3. Seleccione la pestaña **Configuración de la aplicación**.

Haga lo siguiente si es necesario:

- Determine un alcance del análisis.
- Especifique la acción que realiza Kaspersky Endpoint Security cuando detecta un objeto infectado.
- Seleccione qué tipos de archivos analizará Kaspersky Endpoint Security al ejecutar la tarea Analizar.
- Configure los ajustes de rendimiento de 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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Configuración de la tarea Agregar clave

En la pestaña **Configuración de la aplicación**, puede configurar la tarea **Agregar 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 **Agregar clave**.
3. Seleccione la pestaña **Configuración de la aplicación**.

Haga lo siguiente si es necesario:

- Convertir la clave de licencia actual en una clave de reserva.
- Seleccionar otra clave para activar Kaspersky Endpoint Security en el equipo de un usuario.
- Agregar una nueva clave de licencia al repositorio de Kaspersky Security Center.

Configuración de la tarea Actualizar

En la pestaña **Configuración de la aplicación**, puede configurar la tarea **Actualización** de Kaspersky Endpoint Security en equipos remotos.

Abra la configuración de la tarea Actualizar

1. Vaya a **Dispositivos** > **Tareas**.
2. Haga doble clic en una tarea con el tipo de tarea **Actualización**.
3. Seleccione la pestaña **Configuración de la aplicación**.

Los servidores de actualizaciones de Kaspersky dedicados son el origen principal de actualizaciones para Kaspersky Endpoint Security. Kaspersky Endpoint Security también puede usar puntos de distribución, 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 actualizaciones de Kaspersky y los servidores de Kaspersky Security Center de manera predeterminada. Kaspersky Endpoint Security descarga actualizaciones primero de los servidores de Kaspersky Security Center y luego de los servidores de actualizaciones de Kaspersky.

Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la lista de orígenes de actualizaciones incluye servidores de actualizaciones y puntos de distribución de Kaspersky de forma predeterminada. Kaspersky Endpoint Security descarga actualizaciones primero de los puntos de distribución y luego de los servidores de actualizaciones de Kaspersky. Para obtener información detallada sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

Haga lo siguiente si es necesario:

- Active o desactive la actualización 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 olvida o pierde sus credenciales y no puede acceder a una unidad cifrada, puede obtener una clave de recuperación.

Obtenga una clave de recuperación

1. En la ventana principal de Kaspersky Security Center Web Console o Cloud Console, seleccione **Configuración** → **Opciones de interfaz**.
2. Active el conmutador **Mostrar protección y cifrado de datos** para habilitar la administración del cifrado de datos y haga clic en **Guardar**.

3. Vaya a **Operaciones → Protección y cifrado de datos → Unidades cifradas**.

   Se abre la lista de dispositivos cifrados.

4. Seleccione la casilla junto al dispositivo con la unidad cifrada.

5. Haga clic en **Otorgar acceso al dispositivo en modo sin conexión**.

6. En el cuadro de diálogo **Otorgar acceso al dispositivo en modo sin conexión offline**, seleccione el complemento web para Kaspersky Endpoint Security y haga clic en **Aceptar**.

7. Haga clic en **Obtener clave de recuperación**.

   Aparece una clave de recuperación en la ventana de diálogo actual.

8. 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.

Administrar la aplicación desde la línea de comandos

Puede administrar la aplicación Kaspersky Endpoint Security desde la línea de comandos.

Nota: una vez que se instalan las actualizaciones de los módulos de Kaspersky Endpoint Security, la versión del cliente de la aplicación 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 intervalo de parámetros admitidos.

Ver la ayuda de la línea de comandos

Use el siguiente comando para ver la información de la sintaxis de línea de comandos de la aplicación:

```
kav -? | help
```

Ejecutar análisis de malware

Sintaxis del comando:

```
kav scan <objeto analizado> <acción> <tipos de archivo> <exclusiones> <parámetros del informe> <parámetros avanzados>
```

Nota: Para hacer un análisis de malware, también puede abrir la línea de comandos e iniciar una de las tareas creadas en la aplicación. La tarea se iniciará con los parámetros especificados en la interfaz de Kaspersky Endpoint Security.

Descripción de parámetros

`<alcance del análisis>`: este parámetro especifica una lista de objetos que se analizarán en busca de código malicioso. Puede incluir varios parámetros, siempre separados 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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Los siguientes valores son posibles:

- `<archivos>`: lista de rutas de acceso a los archivos o carpetas que se analizarán. Puede especificar rutas absolutas o relativas a los archivos. Los elementos en la lista están separados por un espacio.

  > **Nota:** si el nombre o la ruta de un objeto incluye un espacio o caracteres especiales (por ejemplo, `$`, `&` o `@`), se debe incluir el nombre entre comillas simples (`' '`) o agregar una barra diagonal inversa (`\`) inmediatamente antes de cada uno de los caracteres especiales. Si se hace referencia a una carpeta específica, se analizan todos los archivos y carpetas que contiene.

- `-all`: análisis completo del equipo.
- `-remdrives`: todas las unidades extraíbles.
- `-fixdrives`: todas las unidades internas.
- `-netdrives`: todas las unidades de red.
- `-@:<filelist.lst>`: ruta de acceso al archivo que contiene la lista de objetos y carpetas dentro del alcance del análisis. El archivo debe estar en formato de texto y cada objeto del análisis debe figurar en una línea independiente. Solo se puede escribir una ruta absoluta de acceso al archivo.

`<acción>`: este parámetro determina la acción que se debe realizar con los objetos maliciosos detectados durante el análisis. Si no se define esta configuración, la acción predeterminada es la que coincide con el valor `-i8`.

Los siguientes valores son posibles:

- `-i0`: no realizar ninguna acción con el objeto; solo guardar información sobre este en un informe.
- `-i1`: desinfectar los objetos infectados, omitirlos si no se pueden desinfectar.
- `-i2`: desinfectar los objetos infectados, eliminarlos si no se pueden desinfectar; no se deben eliminar los contenedores, excepto aquellos con encabezados ejecutables (archivos comprimidos .sfx).
- `-i3`: desinfectar los objetos infectados, eliminarlos si no se pueden desinfectar; eliminar por completo los contenedores si no se pueden eliminar los archivos infectados.
- `-i4`: eliminar los objetos infectados; eliminar por completo los contenedores si no se pueden eliminar los archivos infectados que contienen.
- `-i8`: solicitar acción al usuario si se detecta un objeto infectado (valor predeterminado).
- `-i9`: preguntar al usuario qué acción se debe realizar al completar el análisis.

`<tipos de archivo>`: este parámetro define los tipos de archivos que se someten a análisis de malware. De forma predeterminada, si este parámetro no está definido, solo se analizan los archivos que podrían estar infectados (según el contenido del archivo).

Los siguientes valores son posibles:

- `-fe`: analizar solo los archivos que podrían estar infectados (según la extensión del archivo).
- `-fi`: analizar solo los archivos que podrían estar infectados (según el contenido del archivo). Este parámetro se usa por defecto.
- `-fa`: analizar todos los archivos.

`<exclusiones>`: este parámetro define qué objetos se excluirán del análisis. Puede incluir varios parámetros, siempre separados por un espacio.

Los siguientes valores son posibles:

- `-e:a`: no analizar archivos de almacenamiento.
- `-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 los objetos que se ajusten a la máscara especificada.
- `-e: <segundos>`: omitir objetos que se analizan durante un valor de tiempo mayor al especificado (en segundos).
- `-es: <tamaño>`: omitir los objetos cuyo tamaño supere el valor especificado (en megabytes).

`<parámetros del informe>`: estos parámetros definen el formato del informe sobre los resultados del análisis. Puede especificar una ruta absoluta o relativa hacia el archivo de informe. Si no se define este parámetro, los resultados de la reversión aparecen en la pantalla y se muestran todos los eventos.

Los siguientes valores son posibles:

- `-r: <archivo del informe>`: registra solamente los eventos importantes en el archivo del informe especificado.
- `-ra: <archivo del informe>`: registra todos los eventos en el archivo del informe especificado.

`<parámetros avanzados>`: parámetros que definen el uso de las tecnologías de análisis de malware y los archivos de configuración:

- `-iSwift=<on|off>`: activa o desactiva el uso de la tecnología iSwift.
- `-c: <archivo de configuración>`: define la ruta del archivo de configuración que contiene la configuración de la aplicación para realizar las tareas de análisis de malware. Puede especificar una ruta absoluta o relativa hacia el archivo. Si no se especifica el parámetro, se utilizan los valores establecidos en la interfaz de la aplicación, junto con los valores ya especificados en la línea de comandos.

Ejemplo:
Inicie el análisis de las carpetas ~/Documentos, /Aplicaciones y del archivo denominado my test.exe:

```
kav scan ~/Documentos/Aplicaciones 'my test.exe'
```

Analizar la lista de objetos del archivo objects2scan.txt Utilizar el archivo de configuración scan_settings.txt. Al finalizar el análisis, crear un informe para registrar todos los eventos:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Ejemplo de archivo de configuración:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Actualizar la aplicación

Sintaxis del comando:

```
kav update <origen de actualizaciones> <parámetros del informe> <parámetros avanzados>
```

Descripción de parámetros

`<origen de actualizaciones>`: servidor HTTP o carpeta local o de red desde la que se descargan las actualizaciones. Si no se selecciona 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 sobre los resultados del análisis. Puede especificar una ruta absoluta o relativa hacia el archivo de informe. Si no se define este parámetro, los resultados de la reversión aparecen en la pantalla y se muestran todos los eventos.

Los siguientes valores son posibles:

- `-r: <archivo del informe>`: registra solamente los eventos importantes en el archivo del informe especificado.
- `-ra: <archivo del informe>`: registra todos los eventos en el archivo del informe especificado.

`<parámetros avanzados>`: parámetro que define el uso del archivo de configuración.

`-c: <archivo de configuración>`: define la ruta a un archivo de configuración que contiene la configuración de la aplicación para actualizar la aplicación. Puede especificar una ruta absoluta o relativa hacia el archivo. Si este parámetro no está definido, se utilizarán los valores configurados en la interfaz de la aplicación.

Ejemplo:
Actualizar las bases de datos de la aplicación desde la origen predeterminada y registrar todos los eventos en el informe:

```
kav update -ra:avbases_upd.txt
```

Actualizar los módulos de Kaspersky Endpoint Security con los parámetros del archivo de configuración updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

Revertir la última actualización

Sintaxis del comando:

`kav rollback <parámetros del informe>`

Importante: se requieren derechos de administrador para ejecutar este comando.

Descripción de parámetros

`<parámetros del informe>`: este parámetro define el formato del informe sobre los resultados de la reversión de la actualización. Puede especificar una ruta absoluta o relativa hacia el archivo de informe. Si no se define este parámetro, los resultados de la reversión aparecen en la pantalla y se muestran todos los eventos.

Los siguientes valores son posibles:

- `-r: <archivo del informe>`: registra solamente los eventos importantes en el archivo del informe especificado.
- `-ra: <archivo del informe>`: registra todos los eventos en el archivo del informe especificado.

Ejemplo:
```
kav rollback -ra:rollback.txt
```

Iniciar/detener un componente o tarea

La sintaxis del comando start:

`kav start` <nombre de la tarea o el componente> `<parámetros del informe>`

La sintaxis del comando stop:

`kav stop <nombre de la tarea o el componente>`

Importante: se requieren derechos de administrador para ejecutar el comando stop.

Descripción de parámetros

`<nombre de la tarea o el componente>`: especifique uno de los siguientes valores:

- `fm` o `file_monitoring`: Protección contra archivos peligrosos
- `wm` o `web_monitoring`: Protección frente a amenazas en la web
- `mail_monitoring`: Protección contra amenazas de correo
- `ids`: Protección contra amenazas de 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 Análisis completo
- `scan_objects`: tarea Análisis personalizado
- `quick` o `scan_critical_areas`: tarea Análisis rápido
- `externalstoragesscanner`: tarea Análisis de disco extraíble
- `updater`: tarea de actualización
- `rollback`: tarea Reversión
- `diskencryption`: cifrado de disco FileVault
- `edroptimum`: Endpoint Detection and Response Optimum
- `edrkata`: Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox`: Cloud Sandbox
- `mdr`: Managed Detection and Response

`<parámetros del informe>`: estos parámetros definen el formato del informe sobre los resultados de la tarea o el componente. Puede especificar una ruta absoluta o relativa hacia el archivo de informe. Si no se define este parámetro, Kaspersky Endpoint Security muestra los resultados según los parámetros establecidos en la interfaz gráfica de usuario.

Nota: `<parámetros del informe>` solo está disponible para el `actualizador scan_objects` y los valores de `reversión`.

Los siguientes valores son posibles:

- `-r: <archivo del informe>`: registra solamente los eventos importantes en el archivo del informe especificado.
- `-ra: <archivo del informe>`: registra todos los eventos en el archivo del informe especificado.

Nota: los componentes y las tareas iniciados desde el símbolo del sistema se ejecutan con los parámetros configurados en la interfaz gráfica de usuario.

Ejemplo:
Para habilitar el componente Protección contra archivos peligrosos, escriba lo siguiente en la línea de comandos:

```
kav start fm
```

Para detener una tarea Análisis completo desde la línea de comandos, escriba lo siguiente:

```
kav stop scan_my_computer
```

Ver estado y estadísticas de un componente o tarea

Sintaxis de comando del estado:

```
kav status <nombre de la tarea o el componente>
```

Sintaxis de comando de las estadísticas:

```
kav statistics <nombre de la tarea o el componente>
```

Descripción de parámetros

`<nombre de la tarea o el componente>`: especifique uno de los siguientes valores:

- `fm` o `file_monitoring`: Protección contra archivos peligrosos
- `wm` o `web_monitoring`: Protección frente a amenazas en la web
- `mail_monitoring`: Protección contra amenazas de correo
- `ids`: Protección contra amenazas de 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 Análisis completo
- `scan_objects`: tarea Análisis personalizado
- `quick` o `scan_critical_areas`: tarea Análisis rápido
- `externalstoragesscanner`: tarea Análisis de disco extraíble
- `updater`: tarea de actualización
- `rollback`: tarea Reversión
- `diskencryption`: cifrado de disco FileVault
- `edroptimum`: Endpoint Detection and Response Optimum
- `edrkata`: Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox`: Cloud Sandbox
- `mdr`: Managed Detection and Response

Nota: si el comando de estado se ejecuta sin asignar un valor al parámetro `<nombre de la tarea o el componente>`, se muestra el estado de todas las tareas y de todos los componentes de la aplicación. En el caso del comando de estadísticas, es obligatorio asignar un valor al parámetro `<nombre de la tarea o el componente>`.

Exportar la configuración de la protección

Sintaxis del comando:

```
kav export <nombre de la tarea o el componente> <archivo de exportación>
```

Descripción de parámetros

`<nombre de la tarea o el componente>`: especifique uno de los siguientes valores:

- `fm` o `file_monitoring`: Protección contra archivos peligrosos
- `wm` o `web_monitoring`: Protección frente a amenazas en la web
- `mail_monitoring`: Protección contra amenazas de correo
- `ids`: Protección contra amenazas de 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 Análisis completo
- `scan_objects`: tarea Análisis personalizado
- `quick` o `scan_critical_areas`: tarea Análisis rápido
- `externalstoragesscanner`: tarea Análisis de disco extraíble
- `updater`: tarea de actualización
- `rollback`: tarea Reversión
- `diskencryption`: cifrado de disco FileVault
- `edroptimum`: Endpoint Detection and Response Optimum
- `edrkata`: Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox`: Cloud Sandbox
- `mdr`: Managed Detection and Response

`<archivo de exportación>`: ruta del archivo al que se exporta la configuración de la aplicación. Puede especificar una ruta absoluta o relativa hacia el archivo.

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 de claves>
```

Descripción de parámetros

`<archivo de claves>`: archivo de claves de la aplicación con extensión .key.

`<código de activación de 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 del sistema

Sintaxis del comando:

```
kav activatesystemextension /sysext
```

Nota: Debe otorgar 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 de Protección contra amenazas web y Protección contra amenazas de red.

Sintaxis del comando:

```
kav activatesystemextension /webav
```

Nota: debe otorgar a Kaspersky Endpoint Security permisos de filtrado de contenido de la red para finalizar la configuración.

Eliminar claves de licencia

Puede eliminar todas las claves de licencia que se agregan actualmente a la aplicación.

Sintaxis del comando:

```
kav license /del
```

Importante: se requieren derechos de administrador para ejecutar este comando.

Códigos de retorno de la línea de comandos

Desde la línea de comandos, pueden obtenerse códigos de retorno generales con cualquier comando. Entre los códigos de retorno se incluyen códigos generales y también códigos específicos para una tarea determinada.

Sintaxis del comando para recibir el código de retorno:

```
echo $?
```

Códigos de retorno generales:

- `0`: operación completada satisfactoriamente
- `1`: valor de parámetro inválido
- `2`: error desconocido
- `3`: error al completar la tarea
- `4`: tarea cancelada

Códigos de retorno de la tarea de análisis de malware:

- `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 no es posible hacerlo mediante la consola de Kaspersky Security Center.

Administrar Prevención de ejecución

Puede ver la configuración de la Prevención de ejecución del equipo cliente y deshabilitar la Prevención de ejecución en el equipo cliente.

Sintaxis del comando:

```
kav prevention </disable | /show>
```

Descripciones de los comandos

`/disable`: el comando para deshabilitar la Prevención de ejecución en el equipo cliente.

`/show`: comando para mostrar la configuración actual de Prevención de ejecución, incluido el modo y la lista de reglas de Prevención de ejecución.

Administrar Aislamiento de la red

Puede ver la configuración de Aislamiento de la red del host y deshabilitar Aislamiento de la red en el host.

Sintaxis del comando:

```
kav isolation </off | /status>
```

Descripciones de los comandos

`/off`: comando para desactivar Aislamiento de la red.

Importante: se requieren derechos de administrador para ejecutar este comando.

`/status`: comando para mostrar el estado de Aislamiento de la red y las exclusiones.

Nota: Estos comandos deben ejecutarse simultáneamente.

Contactarse con el Soporte Técnico

Esta sección describe cómo obtener soporte técnico y los términos que rigen la prestación del servicio.

Cómo obtener soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Endpoint Security ni en una de las fuentes de información sobre Kaspersky Endpoint Security, comuníquese con el Servicio de soporte técnico de Kaspersky. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas sobre la instalación y el uso de Kaspersky Endpoint Security.

Nota: Kaspersky ofrece soporte técnico de Kaspersky Endpoint Security durante su ciclo de vida (consulte la página de ciclo de vida de soporte técnico de la aplicación). Antes de comunicarse con el Servicio de soporte técnico, le pedimos que lea las reglas de soporte técnico.

Puede comunicarse con los especialistas del Servicio de soporte técnico de las siguientes maneras:

- Visitando el sitio web del Servicio de soporte técnico
- Enviando una solicitud al Servicio de soporte técnico desde el portal de Kaspersky CompanyAccount

Soporte técnico mediante Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para las compañías que usan las aplicaciones de Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialistas de Kaspersky mediante solicitudes en línea. Puede usar Kaspersky CompanyAccount para seguir el estado de sus solicitudes en línea y guardar un historial de estas.

Puede registrar a todos los empleados de su organización en una única cuenta en Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas por los empleados registrados a Kaspersky y además administrar los privilegios de estos empleados a través de Kaspersky CompanyAccount.

El portal de Kaspersky CompanyAccount está disponible en los siguientes idiomas:

- Inglés
- Español
- Italiano
- Alemán
- Polaco
- Portugués

- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del Soporte técnico.

Obtener información para el Soporte técnico

Para un soporte y una resolución de problemas de la aplicación más efectivos, los especialistas del Servicio de soporte técnico pueden pedirle que cambie temporalmente la configuración de la aplicación para la depuración durante el diagnóstico. Esto puede requerir hacer lo siguiente:

- Activar una función que permitirá extraer la información de diagnóstico extendida.
- Realizar pequeños ajustes en la configuración de los componentes individuales de la aplicación, que no están disponibles a través de los elementos estándar de la interfaz de usuario.
- Cambiar la configuración de transmisión de información de diagnóstico que se extrae.

Los especialistas del Soporte técnico le proporcionarán toda la información necesaria para realizar las operaciones enumeradas y le informarán sobre el alcance de los datos que se adquirirán con fines de depuración. Luego de que la información de diagnóstico extendida se extrae, se guarda en el equipo del usuario. Los datos no se envían a Kaspersky de forma automática.

Usar un archivo de rastreo

Después de reportar un problema a los especialistas del Soporte técnico de Kaspersky, es posible que le pidan que genere y envíe un informe sobre el funcionamiento de Kaspersky Endpoint Security. 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 los errores.

Crear un archivo de seguimiento

El seguimiento o rastreo (tracing) es un modo efectivo de registrar información detallada sobre las actividades de la aplicación. Los especialistas del Soporte técnico usan archivos de seguimiento para solucionar los problemas.

Crear un archivo de seguimiento

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Rastreo**, seleccione la casilla **Habilitar rastreo**.

Importante: recomendamos que active el rastreo solo si se lo pide un especialista del Soporte técnico de Kaspersky.

Los archivos de seguimiento pueden requerir mucho espacio de disco. Cuando ya no necesite archivos de seguimiento, deshabilite la función de rastreo.

Deshabilitar la función de rastreo

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

   Se abre la ventana de configuración de la aplicación.

2. En la pestaña **Interfaz**, en la sección **Rastreo**, desmarque la casilla **Habilitar rastreo**.

Kaspersky Endpoint Security guarda la siguiente información en los archivos de rastreo:

- Información sobre el dispositivo y el sistema operativo (ID único del dispositivo, tipo de dispositivo, direcciones MAC de dispositivos de red, tipo de sistema operativo, versión del sistema operativo).
- Información sobre el funcionamiento de la aplicación y sus módulos.
- Información sobre la suscripción (tipo de suscripción, región).
- Información sobre la configuración regional del idioma, ID de aplicación, personalización de la aplicación, versión de la aplicación, ID único de instalación de la aplicación, ID único del equipo.
- Información sobre el estado de protección contra malware de la computadora y la totalidad de objetos detectados y procesados (nombre del objeto detectado, fecha y la hora de la detección, dirección web desde la que se lo descargó, nombres, tamaños y rutas de los archivos infectados, dirección IP del equipo atacante y número de puerto del equipo al que estuvo dirigido el ataque de red, lista de actividades realizadas por el malware y direcciones web no deseadas). También se informará sobre las decisiones y las medidas pertinentes que hayan tomado la aplicación y el usuario.
- Información sobre las aplicaciones descargadas por el usuario (direcciones web, atributos, tamaño de los archivos, información sobre los procesos que descargaron los archivos).
- Información sobre las aplicaciones ejecutadas y sus módulos (tamaño, atributos, fecha de creación, detalles de encabezado PE, región, nombre, ubicación, empaquetadores).
- Información sobre los errores y el uso de la interfaz de la aplicación de Kaspersky instalada.
- Información sobre las conexiones de red: dirección IP de la computadora remota y de la computadora del usuario, los números de los puertos a través de los cuales se estableció la conexión y el protocolo de red de la conexión.
- Información sobre los paquetes de red recibidos y enviados por el equipo a través de redes de TI y telecomunicaciones.
- Información sobre correos electrónicos y mensajes de mensajería instantánea enviados o recibidos.
- Información sobre las direcciones web visitadas: la hora en que se estableció la conexión mediante un protocolo abierto, datos sobre el nombre de usuario y contraseña del sitio web y el contenido de las cookies.
- Certificado público del servidor.

Los archivos de rastreo contienen solo la información necesaria para solucionar 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, se desactiva la creación de archivos de rastreo. Puede habilitar la generación de archivos de rastreo en la configuración de la aplicación.

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

Puede elegir el modo en que los archivos de rastreo se envían a Kaspersky.

Antes de enviar archivos de rastreo a Kaspersky, revise 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 contenidos en los archivos de rastreo que envía, y brinda su consentimiento para el método usado para enviarlos.

Fuentes de información sobre la aplicación

Sección que describe las fuentes de información sobre la aplicación.

Puede elegir la fuente de información más conveniente dependiendo de la importancia y urgencia del tema en cuestión.

Página de Kaspersky Endpoint Security en el sitio web de Kaspersky

En la página de Kaspersky Endpoint Security del sitio web de Kaspersky, puede ver información general sobre la aplicación, sus funciones y sus características.

La página de Kaspersky Endpoint Security contiene un vínculo a la tienda en línea. Allí podrá adquirir o renovar la aplicación.

Página de Kaspersky Endpoint Security en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web del Soporte técnico de Kaspersky.

En la página de Kaspersky Endpoint Security de la Base de conocimientos, encontrará artículos con información útil, recomendaciones y respuestas a las dudas más frecuentes sobre la compra, la instalación y el uso de la aplicación.

Los artículos de la Base de conocimientos pueden brindar respuestas a preguntas relacionadas tanto con Kaspersky Endpoint Security 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. Seleccione **Ayuda** → **Soporte**.
2. Haga clic en **Servicio de soporte técnico**.

Hable sobre las aplicaciones de Kaspersky en nuestro Foro

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky y otros usuarios en nuestro Foro.

En el Foro, puede ver temas de debate, publicar comentarios y crear temas de debate nuevos.

Ir al Foro desde el menú desplegable Ayuda

1. Seleccione **Ayuda** → **Soporte**.
2. Haga clic en **Comunidad**.

Apéndices

Esta sección proporciona información que complementa el texto del documento.

Problemas y limitaciones conocidas

Kaspersky Endpoint Security tiene los siguientes problemas y limitaciones conocidos:

- Si una aplicación que recopila información y la envía para su proceso se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis si configura la aplicación Kaspersky Endpoint Security tal como se describe en este documento.
- La configuración funcional de la aplicación se puede modificar mediante la edición de 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 deshabilita la ejecución automática de la tarea.
- Si inicia una tarea de reinicio del equipo 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 la Mac.
- Para excluir el tráfico de red de Safari del análisis de Kaspersky Endpoint Security, debe agregar las rutas siguientes a la lista de exclusiones:
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- Para excluir el tráfico de red de Google Chrome del análisis de Kaspersky Endpoint Security, debe agregar la ruta siguiente 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 la directiva para una directiva de Kaspersky Endpoint Security utilizando Kaspersky Security Center Web Console y Cloud Console, debe verificar que la configuración se aplique correctamente en los equipos cliente.
- Al habilitar 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 la Configuración del sistema (Preferencias del Sistema).

- Los cambios en las opciones del servidor proxy se aplicarán una vez que reinicie Kaspersky Endpoint Security.
- Es posible que Safari no se conecte a un sitio web que tenga un certificado no confiable. Puede agregar ese 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 equipo. Después de eso, en algunos casos inusuales, es posible que se produzca un error con el permiso acceso total al disco al instalar Kaspersky Endpoint Security. En este caso, le recomendamos que desinstale la aplicación de manera local y la vuelva a instalar.
- Es posible que las aplicaciones que necesitan Rosetta no se instalen si Kaspersky Endpoint Security está en ejecución. Para resolver el problema, salga de Kaspersky Endpoint Security e intente volver a instalar la aplicación.
- Los detalles de alerta para amenazas detectadas en objetos compuestos solo contienen información sobre el objeto detectado en sí, sin un gráfico de la cadena de desarrollo de la amenaza.
- Al guardar una contraseña para Protección con contraseña, puede ocurrir un error. En este caso, recomendamos desinstalar y volver a instalar la aplicación.
- Kaspersky Endpoint Security no analiza archivos ubicados en OneDrive, iCloud, u otros almacenamientos en la nube. Excluya estos archivos del alcance 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 equipo y el nombre del host son los mismos.

Problemas solucionados

La tabla de abajo enumera todos los problemas descubiertos en versiones anteriores de Kaspersky Endpoint Security y solucionados en la versión actual.

Lista de problemas solucionados en la versión 12.2.1, parche E

Identificador	Descripción
10052935	Se mostraba un número excesivo de eventos de conexión a los servidores de Endpoint Detection and Response Expert entre los eventos de los endpoints en Kaspersky Security Center.
10500552	La regla de IOA no se activaba si al menos un carácter del GUID estaba escrito en minúscula.
10781813	Tras un uso prolongado de Kaspersky Endpoint Security, podían producirse problemas al abrir páginas en los navegadores.
10747233	Si los filtros del sistema se cambiaban con mucha rapidez y de forma reiterada, podían producirse problemas para obtener una dirección IP.
10787641	Al intentar ver en Kaspersky Security Center una clave de cifrado enviada desde un dispositivo con macOS 27, podía producirse un error.
10787643	Cuando se seleccionaba el idioma chino simplificado, la descripción de una de las notificaciones de Control web aparecía duplicada.
10787639	Tras un uso muy prolongado de Kaspersky Endpoint Security, podía aumentar el consumo de espacio en el disco duro.
10797191	Podían producirse errores en la lógica de procesamiento de los eventos de cierre de archivos.

Identificador	Descripción
10865705	Podían producirse problemas de compatibilidad con Codex CLI y Cisco VPN.
10563302	Es posible que el sitio web no se abra si la cadena de certificados contiene un certificado cuya confianza no puede verificar el navegador.

Lista de problemas solucionados en el complemento web 12.2.1.8289

Identificador	Descripción
10576132	Después de aplicar el perfil de la directiva, el componente Kaspersky Security Network habilitado en la directiva principal podía permanecer deshabilitado.

Lista de problemas solucionados en la versión 12.2.1, parche D

Identificador	Descripción
10563302	Es posible que el sitio web no se abra si la cadena de certificados contiene un certificado cuya confianza no puede verificar el navegador.

Lista de problemas solucionados en la versión 12.2.1, parche B

Identificador	Descripción
9723123	Cuando el componente Protección contra amenazas de correo está habilitado, los mensajes entrantes no se reciben en el cliente de correo integrado de macOS.
9773561	No se puede eliminar un objeto malicioso del sistema de archivos debido a un error al crear una copia en Copia de seguridad.
9740193	Estado incorrecto de Endpoint Detection and Response Expert (on-premises) cuando se selecciona el modo Integración con Endpoint Detection and Response Expert (versión 8.0 o posterior) en la configuración de la directiva.
9835045	Cuando se selecciona el modo Integración con Endpoint Detection and Response Expert (versión 8.0 o posterior) en la configuración de la directiva, se envía telemetría redundante.
9431735	Error al cargar páginas web en los navegadores debido a un procesamiento incorrecto del tráfico de red por parte de la aplicación.
9799626	La aplicación se inicia tras reiniciar el equipo, incluso cuando la opción "Iniciar la aplicación al arrancar el equipo" está deshabilitada.

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 las aplicaciones y los documentos por extensión**, Kaspersky Endpoint Security realiza análisis de malware en objetos sin extensiones y objetos con las siguientes extensiones:

Formatos generales:

- txt
- csv
- htm
- html

Archivos multimedia (audio/video):

- 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
- clase
- 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 coincidir con la extensión de su nombre de archivo.

Máscaras en rutas de archivos y carpetas

Una máscara de nombre de archivo o una máscara de nombre de carpeta representa el nombre y la extensión de un archivo o el nombre de una carpeta que utiliza símbolos comunes.

Puede usar estos símbolos cuando especifique el alcance de la protección, el alcance del análisis y la Zona de confianza:

- El símbolo de tilde `~` reemplaza `/Usuarios/<nombre de usuario>` en la ruta de un archivo o de una carpeta. Por ejemplo, la ruta `~/Escritorio` significa que el alcance de la protección incluye las carpetas de `Escritorio` de todos los usuarios en los equipos que desea proteger.

- El símbolo de asterisco `*` reemplaza cualquier conjunto de caracteres en el nombre del archivo o la carpeta, excepto los caracteres `\` y `/` (que delimitan los nombres de archivos y carpetas en las rutas a archivos y carpetas). Por ejemplo, la máscara `/*/*.db*` incluirá todas las rutas a los archivos con una extensión que empiece con `db` que se encuentran en las carpetas del disco interno, pero no en las subcarpetas.

- Dos símbolos consecutivos de asterisco `**` reemplazan cualquier conjunto de caracteres (incluido un conjunto vacío) en el nombre del archivo o la 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` que se encuentran 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 `?` reemplaza cualquier carácter del nombre del archivo o la 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 de todos los archivos que se encuentran 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 los archivos de IOC tienen el mismo identificador, puede afectar los resultados de la ejecución de la tarea.

- Un solo archivo de IOC no debe exceder los 2 MB de tamaño. El uso de archivos más grandes hará que las tareas de análisis de IOC finalicen con un error. El tamaño total de todos los archivos agregados a la colección IOC no debe exceder los 10 MB. Si el tamaño total de todos los archivos supera los 10 MB, debe dividir la colección IOC y crear varias tareas de Análisis de IOC.

- Se recomienda crear un archivo de IOC por amenaza. Esto facilita el análisis de los resultados de la tarea de Análisis de IOC.

En la siguiente tabla, se muestran las funciones y limitaciones de la compatibilidad de la aplicación con los archivos de IOC.

Funciones y limitaciones de la compatibilidad con los documentos de IOC.

Condiciones admitidas	OpenIOC 1.0:
	
	`is`
	`isnot` (como una excepción del conjunto)
	`contains`
	`containsnot` (como una 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 admitidos	`AND` `OR`
Tipos de datos admitidos	`"date"`: fecha (condiciones válidas: `is`, `greater-than` y `less-than`) `"int"`: entero (condiciones válidas: `is`, `greater-than` y `less-than`) `"string"`: cadena (condiciones válidas: `is`, `contains`, `matches`, `starts-with` y `ends-with`) `"duration"`: duración en segundos (condiciones válidas: `is`, `greater-than` y `less-than`)

Características de la interpretación de tipos de datos	Los tipos de datos `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` y `"base64Binary"` se interpretan como cadena.
	
	La aplicación admite la interpretación de `Content setting` 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 `date` y `duration` si los indicadores se configuran en `ISO 8601`, `Zulu Time Zone` o `UTC format`.

Intérpretes de scripts compatibles con 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 abren el script especificado en la regla de Prevención de ejecución, no se bloqueará la ejecución del script.

Cómo agregar 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 agregar el certificado de Kaspersky a este almacenamiento de certificados manualmente. De lo contrario, el navegador no podrá abrir páginas HTTPS.

Exportar 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 seleccione **Exportar "Autoridad de certificación de Kaspersky Web Anti-Virus"**.
5. Seleccione una ubicación para guardar el certificado y haga clic en **Guardar**.

Se guarda el certificado de Kaspersky.

Agregue 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 del menú y seleccione **Configuración**.
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. Elija 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. Eso significa que deberá completar el procedimiento después de cada vez que reinstale la aplicación Kaspersky Endpoint Security.

Configuración de red para la interacción con servicios externos

Kaspersky Endpoint Security utiliza la siguiente configuración de red para interactuar con servicios externos.

Configuración de red

Dirección	Descripción
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocolo: `HTTPS` Puerto: `443`	Activación de la aplicación.

Dirección	Descripción

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTPS`
Puerto: `443`
	Actualización de bases de datos y módulos de software de la aplicación.

`downloads.upd.kaspersky.com` Protocolo: `HTTPS` Puerto: `443`	• Actualización de bases de datos y módulos de software de la aplicación. • Verificación del acceso a los servidores de Kaspersky. Si el acceso a los servidores mediante el DNS del sistema no es posible, la aplicación utiliza el DNS público. Esto es necesario para asegurarse de que las bases de datos antivirus estén actualizadas y se mantenga el nivel de seguridad del equipo. Kaspersky Endpoint Security utiliza la siguiente lista de servidores DNS públicos en el siguiente orden: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).

Dirección	Descripción
	Importante: Las solicitudes emitidas por la aplicación pueden contener direcciones de dominios y la dirección IP pública del usuario, ya que la aplicación establece una conexión TCP/UDP con el servidor DNS. Esta información es necesaria, por ejemplo, para validar el certificado de un recurso web cuando se utiliza HTTPS. Si Kaspersky Endpoint Security usa un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio correspondiente. **Cómo evitar que Kaspersky Endpoint Security use un servidor DNS público** 1. Salga de la aplicación Kaspersky Endpoint Security en el dispositivo del usuario. 2. Agregue la variable `ForceUseSystemDNS` y establezca el valor en `1` en el archivo de configuración de la aplicación de Kaspersky Endpoint Security ubicado en `/Library/Application Support/Kaspersky Lab/KAV/Binaries/config.xml`. 3. Inicie la aplicación Kaspersky Endpoint Security. Como resultado, la aplicación Kaspersky Endpoint Security usará solo el DNS del sistema.
`touch.kaspersky.com` Protocolo: `HTTP`	• Recibiendo el tiempo de confianza para revisar el periodo de validez del certificado (conexión TLS). • Advertencia sobre el acceso denegado a un recurso web en el navegador cuando se está ejecutando Protección contra amenazas web.

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTP`
Puerto: `80`
	Actualización de bases de datos y módulos de software de la aplicación.

Dirección	Descripción

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocolo: `HTTPS`
Puerto: `443`
	Al usar Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocolo: `KSN`
Puerto: `443`, `1443`
	Al usar Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protocolo: `HTTPS`
Puerto: `443`
	Haga clic en los vínculos de la interfaz.

Configuración usada para el cifrado

Dirección	Descripción

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocolo: `HTTP`
Puerto: `80`
	Infraestructura de clave pública (PKI).

Información acerca de código de terceros

La información acerca del código de terceros se incluye en el archivo legal_notices.txt de la carpeta de instalación de la aplicación.

Avisos de marca registrada

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

ActiveSync, Active Directory, Excel, IIS, Microsoft, Outlook, Windows, Windows Installer y WMI son marcas comerciales del grupo de empresas de Microsoft.

Apple, Apple Remote Desktop, FileVault, iCloud, Keychain, Launchpad, Mac, macOS, Rosetta, Safari y Xcode son marcas comerciales de Apple Inc.

Chrome, Gmail, Google, Google Chrome y Google Public DNS son marcas comerciales de Google LLC.

Cisco es una marca registrada o una marca comercial de Cisco Systems, Inc. y/o sus filiales en Estados Unidos y en otros países.

Cloudflare, el logotipo de Cloudflare y Cloudflare Workers son marcas comerciales y/o marcas registradas de Cloudflare, Inc. en Estados Unidos y otras jurisdicciones.

Composer y JAMF son marcas comerciales registradas o de derecho consuetudinario de JAMF SOFTWARE, LLC en los EE. UU. y otros países.

Firefox, Mozilla y Thunderbird son marcas comerciales de Mozilla Foundation en EE. UU. y otros países.

Intel es una marca comercial de Intel Corporation o sus subsidiarias.

JavaScript es una marca comercial registrada de Oracle o sus empresas afiliadas.

Linux es la marca comercial registrada de Linus Torvalds en los EE. UU. y otros países.

Parallels, el logotipo de Parallels y Coherence son marcas comerciales o marcas comerciales registradas de Parallels International GmbH.

VMware y VMware Fusion son marcas registradas o marcas comerciales de VMware, Inc. en los Estados Unidos o en otros países.

La ventana Soporte al usuario

Esta ventana proporciona la siguiente información:

- Versión de Kaspersky Endpoint Security
- Fecha de lanzamiento de las bases de datos que Kaspersky Endpoint Security utiliza actualmente
- Versión del sistema operativo instalado en el equipo

Servicio de soporte técnico

Al hacer clic en este botón, se abre la Base de conocimientos del Soporte técnico de Kaspersky, donde puede encontrar artículos sobre Kaspersky Endpoint Security publicados por especialistas de Kaspersky.

Comunidad

Al hacer clic en este botón, se abre la comunidad donde puede conversar 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 al usuario.

La ventana Configuración del certificado

En la pestaña **General**, puede seleccionar el almacenamiento del certificado para verificar el tráfico HTTPS cifrado en el navegador Mozilla Firefox:

- **Llavero Raíz del sistema (recomendado)**
- **Configuración de la tienda de certificados del navegador Mozilla Firefox**

  En este caso, debe agregar manualmente el certificado de Kaspersky Endpoint Security al almacenamiento de certificados del navegador Mozilla Firefox. Para obtener más información, consulte Cómo agregar 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 está vacía de manera predeterminada.

+

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede agregar los certificados que se considerarán de confianza.

–

Al hacer clic en este botón, se elimina el certificado elegido de la lista de computadoras de confianza.

Nombre del 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.

Agregar a la lista de confianza

Al hacer clic en este botón, se agrega 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 usarlo 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, continúa conectándose al servidor utilizando el certificado seleccionado.

La ventana “Archivo comprimido protegido con contraseña detectado”

Si Kaspersky Endpoint Security debe analizar un archivo comprimido protegido con contraseña mientras se están ejecutando la Protección contra archivos peligrosos o una tarea de análisis, aparecerá una ventana de notificación.

Archivo comprimido

Ruta al archivo.

Contraseña

Campo para escribir la contraseña.

Si se escribe la contraseña, Kaspersky Endpoint Security analiza el archivo comprimido en busca de malware y otros tipos de amenazas de seguridad.

Omitir archivos comprimidos protegidos

Si hace clic en este botón, se omiten el objeto y todos los de su tipo.

Omitir

Cuando se hace clic en este botón, se omite el objeto.

El cuadro de diálogo Objeto detectado

Cuando Kaspersky Endpoint Security detecta un virus u otra amenaza para la seguridad del equipo, 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 en 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 donde se detectó el objeto.

Aplicar a todo

Esta casilla habilita o deshabilita el uso de la acción seleccionada para todos los objetos del mismo tipo durante la sesión actual de la Protección contra archivos peligrosos, la Protección contra amenazas web o una tarea de análisis de malware.

La casilla está desactivada de forma predeterminada.

La sesión actual de la Protección contra archivos peligrosos o la Protección contra amenazas web comprende desde el momento en que se inicia hasta que se detiene el componente o hasta que se cierra o se reinicia la aplicación. La sesión actual de tareas de análisis de malware se define como el tiempo desde el inicio de una tarea del análisis de malware hasta su finalización.

Los botones con las acciones que se pueden realizar en los objetos detectados varían según el tipo de objeto detectado.

Puede seleccionar una de las siguientes acciones:

- **Desinfectar**. Desinfectar el objeto malicioso. Antes de realizar la desinfección, Kaspersky Endpoint Security crea una copia de seguridad del archivo en caso de que necesite restaurar el archivo original.
- **Eliminar**. Eliminar el objeto. Antes de realizar la eliminación, Kaspersky Endpoint Security crea una copia de seguridad del archivo en caso de que necesite restaurar el archivo original.
- **No bloquear**. Permitir el acceso a un sitio web que se considera un objeto peligroso de tráfico web.
- **Bloquear**. Rechazar el acceso a un sitio web que se considera un objeto peligroso de tráfico web.
- **Eliminar archivo comprimido**. Eliminar el archivo de almacenamiento que contiene el objeto malicioso.
- **Omitir archivos comprimidos protegidos**. Omitir los archivos de almacenamiento protegidos con contraseña durante los análisis de malware.
- **Omitir**. Bloquear el acceso al objeto malicioso pero no aplicarle ninguna acción.

La ventana “Análisis”



Al hacer clic en este botón, vuelve a la ventana anterior de Kaspersky Endpoint Security.



Al hacer clic en este botón, avanza a 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 malware de la ventana **Análisis**.

Programar análisis

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede programar las tareas Análisis rápido o Análisis completo.

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 malware seleccionada.

Este botón se muestra si hay una tarea de análisis de malware en ejecución.

Configuración

Al hacer clic en este botón, se abre la pestaña **Análisis**, donde puede configurar las tareas de análisis.

Elegir

Si hace clic en este botón, se abre un cuadro de diálogo donde puede elegir un archivo o carpeta para analizar.

En la parte inferior de la sección **Archivos y carpetas**, puede ver los registros de todas las tareas de análisis de malware que se realizaron para los archivos o las carpetas seleccionados.

Detalles

Al hacer clic en este botón, se abre la ventana de informes de las tareas de análisis de malware.

Este botón aparece cuando pasa el puntero por encima de una tarea de escaneo.

Borrar historial de análisis

Al hacer clic en este botón, se eliminan todos los registros de todas las tareas de análisis de malware.

Mostrar todo

Si hace 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 del alcance 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

Si se hace clic en este botón, se inicia la desinfección de todos los objetos maliciosos que se han detectado.

Ignorar todo

Cuando se hace clic en este botón, se eliminan todos los objetos maliciosos de la lista de objetos maliciosos en la sección **Objetos detectados**.

•••

Cuando se hace clic en este botón, se abre un menú desplegable en el que puede seleccionar una de las siguientes acciones que se realizan con un objeto malicioso:

- **Desinfectar**. Desinfectar el objeto malicioso. Antes de la desinfección, la aplicación Kaspersky Endpoint Security crea una copia de seguridad del archivo, de manera que se lo pueda restaurar o desinfectar más tarde sin riesgo de perder datos.
- **Ignorar**. El objeto se elimina de la lista de objetos detectados.

La sección **Otros objetos** contiene objetos detectados que no son maliciosos, pero podrían usarse para dañar su equipo o sus datos.

Eliminar todo

Cuando se hace clic en este botón, se eliminan todos los objetos detectados en el equipo.

Ignorar todo

Cuando se hace clic en este botón, se eliminan todos los objetos detectados de la lista de objetos detectados en la sección **Otros objetos**.

•••

Cuando se hace clic en este botón, se abre un menú desplegable en el que puede seleccionar una de las siguientes acciones que se realizan con un objeto detectado:

- **Eliminar**. Se elimina el objeto detectado del equipo.
- **Ignorar**. El objeto se elimina de la lista de objetos detectados.

La sección **Depósito de copias de seguridad** contiene copias de seguridad de los objetos detectados.

Eliminar todo

Cuando se hace clic en este botón, se eliminan todas las copias de seguridad de los objetos detectados en el equipo.

•••

Cuando se hace clic en este botón, se abre un menú desplegable en el que puede seleccionar una de las siguientes acciones que se realizan con un objeto respaldado:

- **Eliminar copia de seguridad**. Se elimina del equipo la copia de seguridad del objeto detectado.
- **Restaurar archivo**. Se restaura la copia de seguridad del objeto seleccionado en la lista a su ubicación original con el mismo nombre que tenía el archivo original 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 desinfectarlo o si desinfectó el archivo original) se mostrará una advertencia. Puede cambiar la ubicación del objeto que se restaura, o cambiar su nombre.

La ventana Licencia



Al hacer clic en este botón, vuelve a la ventana anterior de Kaspersky Endpoint Security.



Al hacer clic en este botón, avanza a la siguiente ventana de Kaspersky Endpoint Security.

Nota: esta ventana varía según si Kaspersky Endpoint Security está habilitado y del tipo de licencia o suscripción utilizada.

Esta ventana puede contener la siguiente información:

- Estado de la licencia o suscripción
- Claves activas
- Claves de reserva (si tiene)
- El tipo de licencia y la cantidad de equipos en los que se puede usar la aplicación de acuerdo con la licencia actual o a la suscripción
- Funciones de la aplicación que están disponibles bajo la licencia o suscripción actual
- Fecha y hora de caducidad de la licencia
- Cantidad de días restantes hasta que la licencia caduque

En esta ventana, puede realizar una de las siguientes acciones:

- Active la aplicación con 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 con la información sobre la renovación de la suscripción.
- Actualice el estado de su suscripción.

Para obtener más información sobre las licencias de Kaspersky Endpoint Security, comuníquese con el administrador del sistema de su organización.

Ventana Alcance de la protección

En la sección **Alcance de la protección**, puede ver y editar el alcance de la protección.

Todos los discos extraíbles

Esta casilla habilita o deshabilita la protección en tiempo real de todos los discos extraíbles.

La casilla de verificación está activada de forma predeterminada.

Todos los discos internos

Esta casilla habilita o deshabilita la protección en tiempo real de todos los discos internos.

La casilla de verificación está activada de forma predeterminada.

Todos los discos de red

Esta casilla habilita o deshabilita la protección en tiempo real de todos los discos de red.

La casilla de verificación está activada de forma predeterminada.

+

Si hace clic en este botón, se abre una lista en la que puede seleccionar los elementos para crear el alcance de la protección:

- **Archivos y carpetas**. Al seleccionar este elemento, se abre un diálogo para agregar un archivo o una carpeta al alcance de la protección.
- **Todos los discos**. Al seleccionar este elemento, se agregan todos los discos extraíbles, discos internos y discos de red del equipo al alcance de la protección.
- **Todos los discos extraíbles**. Al seleccionar este elemento, se agregan todos los discos extraíbles del equipo al alcance de la protección.
- **Todos los discos internos**. Al seleccionar este elemento, se agregan todos los discos internos del equipo al alcance de la protección.
- **Todos los discos de red**. Al seleccionar este elemento, se agregan todos los discos de red del equipo al alcance de la protección.
- **Memoria**. Al seleccionar este elemento, se agrega la memoria del equipo al alcance de la protección.
- **Objetos de inicio**. Si selecciona este elemento, se agregan todos los archivos ejecutables ejecutados durante el inicio del sistema operativo al alcance de la protección. El análisis de los objetos de inicio hace posible detectar rootkits.

Las casillas junto a los elementos de la lista habilitan o deshabilitan la protección en tiempo real de los objetos asociados a estos elementos.

–

Al hacer clic en este botón, se eliminan todos los elementos seleccionados de la lista del alcance de protección.

Los elementos incluidos en la lista del alcance de la protección de forma predeterminada no pueden eliminarse.

En la sección **Optimización**, puede configurar si Kaspersky Endpoint Security analiza el volumen del sistema de solo lectura.

Omitir análisis de volumen del sistema de solo lectura

La casilla habilita o deshabilita el análisis del volumen de sistema de solo lectura de Kaspersky Endpoint Security.

La casilla de verificación está activada de forma predeterminada.

Importante: la optimización puede estar deshabilitada por razones de seguridad.

Ventana Alcance del análisis

En esta ventana, puede ver y editar el alcance del análisis de la tarea Análisis rápido.

La casilla junto a cada objeto de la lista habilita o deshabilita el análisis de ese objeto.

+

Al hacer clic en este botón, se abre una lista que permite ajustar el alcance del análisis:

- **Archivos y carpetas**. Al seleccionar este elemento, se abre un diálogo para agregar un archivo o una carpeta a la cobertura del análisis.
- **Todos los discos**. Al seleccionar este elemento, se agregan todos los discos extraíbles, discos internos y discos de red del equipo al alcance del análisis.
- **Todos los discos externos**. Al seleccionar este elemento, se agregan todos los discos extraíbles del equipo al alcance del análisis.
- **Todos los discos internos**. Al seleccionar este elemento, se agregan todos los discos internos del equipo a la cobertura del análisis.
- **Todos los discos de red**. Al seleccionar este elemento, se agregan todos los discos de red a la cobertura del análisis del equipo.
- **Memoria**. Al seleccionar este elemento, se agregan la memoria del equipo al alcance de análisis.
- **Objetos de inicio**. Al seleccionar este elemento, se agregan todos los archivos ejecutables del inicio del sistema operativo al alcance de análisis del equipo. El análisis de los objetos de inicio hace posible detectar rootkits.

–

Al hacer clic en este botón, se eliminan todos los elementos seleccionados de la lista del alcance del análisis.

Los elementos incluidos en la lista del alcance del análisis de forma predeterminada no pueden eliminarse.

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 análisis de volumen del sistema de solo lectura

La casilla habilita o deshabilita el análisis del volumen de sistema de solo lectura de Kaspersky Endpoint Security.

Si la casilla está seleccionada, Kaspersky Endpoint Security no analiza el volumen de sistema de solo lectura. Esto reduce significativamente el tiempo de análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza el volumen de sistema de solo lectura.

Esta casilla está seleccionada por defecto.

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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

La pestaña Esencial

En la sección **General**, puede habilitar o deshabilitar la protección del equipo contra malware y otras amenazas de seguridad.

Habilitar protección

Esta casilla de verificación habilita o deshabilita la protección en tiempo real contra malware y otras amenazas de la seguridad informática.

La casilla de verificación está activada de forma predeterminada.

Verificar conexiones seguras (HTTPS)

Esta casilla de verificación habilita/deshabilita el análisis de conexiones cifradas (HTTPS) por Kaspersky Endpoint Security y muestra notificaciones cuando el Control Web bloquea el acceso del usuario a recursos web peligrosos.

La casilla está desactivada 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 malware.

Configuración

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 contra amenazas de archivo** puede habilitar o deshabilitar la Protección contra archivos peligrosos y seleccionar la acción que Kaspersky Endpoint Security realiza cuando detecta un archivo infectado.

Habilitar la Protección contra amenazas de archivo

Esta casilla habilita o deshabilita la Protección contra archivos peligrosos.

La casilla de verificación está activada de forma predeterminada.

Alcance de la protección

Cuando hace clic en este botón, se abre una ventana donde puede crear el alcance de la protección.

Desinfectar o eliminar los 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 la desinfección se realiza correctamente, Kaspersky Endpoint Security guarda el archivo en su ubicación original con el nombre del archivo original. Si la desinfección falló, Kaspersky Endpoint Security mantiene el archivo infectado en estado bloqueado en su ubicación inicial. La información sobre la detección del objeto infectado se registra en el informe **Objetos procesados**.

Preguntar al usuario

Kaspersky Endpoint Security despliega una ventana de notificación con información sobre el objeto malicioso sospechado de haber infectado el archivo y solicita al usuario que seleccione la acción que debe realizar la aplicación. Las acciones disponibles pueden variar según el estado del objeto.

Esta acción está seleccionada de forma predeterminada.

En la sección **Protección contra amenazas web**, puede habilitar o deshabilitar la Protección contra amenazas web y seleccionar la acción que Kaspersky Endpoint Security realizará cuando detecte objetos peligrosos del tráfico web.

Habilitar Protección contra amenazas web

Esta casilla habilita o deshabilita la Protección contra amenazas web.

La casilla de verificación está activada de forma predeterminada.

Bloquear los objetos peligrosos del tráfico web automáticamente

Kaspersky Endpoint Security bloquea el acceso al sitio web donde se detectó un objeto peligroso de tráfico web sin solicitar confirmación.

Preguntar al usuario

Kaspersky Endpoint Security despliega una ventana de notificación con información sobre el objeto peligroso de tráfico web detectado y solicita al usuario que seleccione la acción que debe realizar la aplicación. Las acciones disponibles pueden variar según el estado del objeto.

Esta acción está seleccionada de forma predeterminada.

En la sección **Protección contra amenazas de correo** puede habilitar o deshabilitar la Protección contra amenazas de correo y seleccionar la acción que Kaspersky Endpoint Security realiza cuando detecta un objeto malicioso.

Habilitar Protección contra amenazas de correo

Esta casilla de verificación habilita o deshabilita el componente Protección frente a amenazas en el correo.

La casilla de verificación está activada 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 contra amenazas de red**, puede habilitar o deshabilitar la Protección contra amenazas de red.

Habilitar Protección contra amenazas de red

Esta casilla habilita o deshabilita la Protección contra amenazas de red.

La casilla de verificación está activada de forma predeterminada.

Configuración

Al hacer clic en este botón, se abre una ventana donde puede crear una lista de equipos de confianza o ver y editar 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.



Si hace clic en este botón, se abre una indicación para ingresar las credenciales del administrador. Después de ingresar las credenciales de administrador, la configuración de la aplicación se puede editar.

Pestaña Aplicaciones de confianza

En la pestaña **Aplicaciones de confianza**, puede crear una lista de aplicaciones que no desee que supervise la aplicación Kaspersky Endpoint Security.

La lista de objetos de la Zona de confianza está vacía de forma predeterminada.

+

Si hace clic en este botón, se abre una ventana donde puede ingresar la ruta a una aplicación, especificar el requisito de firma de código y seleccionar los tipos de actividad que no supervisará Kaspersky Endpoint Security.

–

Al hacer clic en este botón, se elimina de la Zona de confianza la aplicación seleccionada.

Editar

Al hacer clic en este botón, se abre una ventana en la que puede editar los parámetros de la aplicación de confianza.

Ventana Agregar aplicación de confianza

Ruta

La ruta a una aplicación cuya actividad de red o archivo no se supervisará a través de Kaspersky Endpoint Security.

Nota: Los vínculos 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 mediante 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 supervise la aplicación Kaspersky Endpoint Security.

No supervisar la actividad de archivos

Esta casilla habilita o deshabilita la supervisión de las operaciones con archivos de una aplicación en un equipo cliente.

Si la casilla está seleccionada, Kaspersky Endpoint Security no supervisa la actividad de archivos de la aplicación.

Si la casilla no está seleccionada, Kaspersky Endpoint Security supervisa la actividad de archivos de la aplicación.

Esta casilla está seleccionada por defecto.

No supervisar la actividad de red

Esta casilla habilita o deshabilita la supervisión del tráfico de Internet entrante y saliente en un equipo cliente.

Si la casilla está seleccionada, Kaspersky Endpoint Security no supervisa la actividad de red de la aplicación.

Si la casilla no está seleccionada, Kaspersky Endpoint Security supervisa la actividad de red de la aplicación.

Esta casilla está seleccionada por defecto.

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 las aplicaciones de confianza y se cierra la ventana.

Pestaña Archivos y carpetas de confianza

En la pestaña **Archivos y carpetas**, puede crear una lista de los archivos y las carpetas que no desea que la aplicación Kaspersky Endpoint Security supervise.

La lista de objetos de la Zona de confianza está vacía de forma predeterminada.

+
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 eliminan los objetos seleccionados de la Zona de confianza.

Pestaña Direcciones web de confianza

En la pestaña **Direcciones web**, puede crear una lista de las direcciones web que no desea que la aplicación Kaspersky Endpoint Security supervise.

La lista de objetos de la Zona de confianza está vacía de forma predeterminada.

+
Al hacer clic en este botón, se agrega un campo para escribir 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 en el nombre del archivo o carpeta, excepto los caracteres `\` y `/`.

–
Al hacer clic en este botón, se elimina de la Zona de confianza la dirección web seleccionada.

La ventana configuración de Protección contra amenazas de correo

Omitir los archivos más grandes que <valor> MB

Si esta casilla de verificación está seleccionada, Protección frente a amenazas en el correo excluye del análisis los archivos adjuntos a 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 por defecto es 8 MB.

La casilla de verificación está activada de forma predeterminada.

Limitar el tiempo para analizar archivos a <valor> 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 por defecto es de 5 segundos.

La casilla de verificación está activada de forma predeterminada.

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.

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

+

Al hacer clic en este botón, se agrega un campo para escribir la dirección IP del equipo de confianza.

–

Al hacer clic en este botón, se elimina la dirección IP seleccionada de la lista de equipos de confianza.

Editar

Al hacer clic en este botón, se puede editar la dirección IP seleccionada.

En la pestaña **Equipos bloqueados**, puede ver y editar la lista de equipos bloqueados.

La aplicación Kaspersky Endpoint Security bloquea el equipo con esta dirección IP por una hora luego de detectar una actividad de red peligrosa que proviene de este.

Dirección IP

Esta columna muestra la dirección IP del equipo bloqueado.

Hora del incidente

Esta columna muestra la fecha y hora en que se detectó 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 Reglas de paquete de red

Nombre de regla

Nombre de la regla de paquetes de red.

En la sección **Acción**, puede seleccionar la acción que realiza Kaspersky Endpoint Security al detectar 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 la 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 habilita o deshabilita el registro de eventos de Firewall.

Si esta casilla está seleccionada, Kaspersky Endpoint Security registra eventos de Firewall en el informe.

Si esta casilla no está seleccionada, Kaspersky Endpoint Security no registra eventos de Firewall en el informe.

La casilla está desactivada 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 seleccionar 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 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 del 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 del DNS. Este campo está disponible solo si selecciona **Dirección IP o nombre del 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 del 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 plantillas de regla de red.

La pestaña Reglas de paquete de red

Nombre

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 direcciones IP de la red.

La ventana Red disponible

Nombre de la 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 a la que desea que se aplique la regla de red.

Dirección MAC

Campo de entrada de dirección MAC. Este campo está disponible solo si selecciona **Dirección MAC** en la lista desplegable **Tipo**.

Máscara

Campo de entrada de 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 **Intervalo de direcciones MAC** en la lista desplegable **Tipo**.

Final del rango

Campo de entrada del final del rango de direcciones MAC. Este campo está disponible solo si selecciona **Intervalo de direcciones MAC** en la lista desplegable **Tipo**.

La pestaña Avanzado

En la sección **KSN**, puede leer los términos de la Declaración de Kaspersky Security Network y decidir participar o no participar en Kaspersky Security Network.

Mostrar la Declaración de KSN

Al hacer clic en este botón, se abre una ventana con el texto completo de la Declaración de Kaspersky Security Network.

Kaspersky Endpoint Security puede utilizar una infraestructura de KSN Global o Privada. Si participa en Kaspersky Security Network, Kaspersky Endpoint Security utiliza la información sobre la reputación de los archivos, los recursos web y las aplicaciones que recibe de Kaspersky Security Network y proporciona los datos necesarios a Kaspersky Security Network para el funcionamiento de los servicios de detección.

Participar en Kaspersky Security Network

Esta casilla habilita o deshabilita la participación en Kaspersky Security Network.

Participar en Kaspersky Private Security Network

Esta casilla habilita o deshabilita 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 de su organización.

Habilitar el modo KSN extendido

Esta casilla habilita/deshabilita el suministro de datos adicionales a Kaspersky Security Network. Estos datos se utilizan para mejorar la protección de su equipo y la usabilidad 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 se selecciona automáticamente si se marca la casilla **Participar en Kaspersky Security Network**.

Habilitar 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 habilitada. 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 habituales. 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 habilitar/deshabilitar el componente Detección de comportamiento y seleccionar una acción para realizar cuando se detecta actividad de malware.

Habilitar Detección de comportamiento

Esta casilla habilita/deshabilita el componente Detección de comportamiento, que recibe información sobre las acciones de las aplicaciones en su equipo y la proporciona a otros componentes de protección para mejorar su rendimiento.

Bloquear la actividad del malware

Si se selecciona esta opción, Kaspersky Endpoint Security finaliza una aplicación cuando detecta 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 según el 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.



Si hace clic en este botón, se abre una indicación para ingresar las credenciales del administrador. Después de ingresar las credenciales de administrador, la configuración de la aplicación se puede editar.

Pestaña Análisis

Lista de las tareas del análisis de malware

Contiene las tareas de análisis de malware preestablecidas:

- **Análisis completo**. Un análisis de malware de la memoria del equipo, los objetos de inicio y todos los discos internos.
- Análisis rápido. Análisis de malware limitado a las áreas críticas del equipo: memoria, objetos de inicio y carpetas del sistema.
- **Análisis personalizado**. Un análisis de malware de un objeto específico (archivo, carpeta, disco interno o disco extraíble).
- **Análisis de discos externos**. Un análisis de malware de los discos externos que se realiza cuando se conecta un disco externo al equipo.

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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

En la sección **Alcance del análisis**, puede ver y editar el alcance del análisis de la tarea Análisis rápido.

Editar

Al hacer clic en este botón, se abre una ventana donde puede ver y editar el alcance del análisis.

Este botón solo aparece cuando se selecciona la tarea Análisis rápido en la lista.

En la sección **Acción**, puede seleccionar la acción que Kaspersky Endpoint Security debe realizar cuando detecta un archivo infectado y programar una tarea.

Desinfectar o eliminar los 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 la desinfección se realiza correctamente, Kaspersky Endpoint Security guarda el archivo en su ubicación original con el nombre del archivo original. Si la desinfección falló, Kaspersky Endpoint Security mantiene el archivo infectado en estado bloqueado en su ubicación inicial. La información sobre la detección del objeto infectado se registra en el informe **Objetos procesados**.

Preguntar al usuario al completarse el análisis

Kaspersky Endpoint Security espera a que finalice el análisis antes de procesar los objetos infectados que se han detectado. Cuando se completa el análisis, Kaspersky Endpoint Security muestra ventanas de notificación que le informan sobre cada objeto infectado que se detectó y le ofrece una serie de acciones adicionales para realizar. Las acciones disponibles pueden variar según el estado del objeto.

Esta acción está seleccionada de forma predeterminada.

En la sección **Cuando se conecta un disco externo** de la pestaña **Análisis de discos externos**, puede seleccionar la acción que Kaspersky Endpoint Security debe realizar al conectar un disco externo.

Análisis

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

Esta opción está seleccionada por defecto.

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 analiza el volumen del sistema de solo lectura al realizar una tarea de Análisis rápido o Análisis completo.

Omitir análisis de volumen del sistema de solo lectura

La casilla habilita o deshabilita el análisis del volumen de sistema de solo lectura 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: la optimización puede estar deshabilitada por razones de seguridad.

Uso de CPU

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede habilitar o deshabilitar 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 para 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.

Habilitar esta opción puede afectar negativamente al rendimiento de Kaspersky Endpoint Security.

Por defecto, esta opción está desactivada.

Programación

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede programar las tareas Análisis rápido o Análisis completo.



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.



Si hace clic en este botón, se abre una indicación para ingresar las credenciales del administrador. Después de ingresar las credenciales de administrador, la configuración de la aplicación se puede editar.

Pestaña Amenazas

En la sección **Objetos para detectar**, puede configurar la lista de objetos que desea detectar.

Virus, gusanos, programas troyanos, utilidades maliciosas, adware y marcadores automáticos

Esta categoría incluye los siguientes tipos de programas:

- Todos los tipos de malware.
- Aplicaciones que muestran publicidades (por ejemplo, anuncios) en el equipo o remplazan los resultados de búsqueda del navegador con sitios web de publicidad.
- Aplicaciones que subrepticiamente establecen conexiones telefónicas a través del módem de un equipo.

Kaspersky Endpoint Security siempre controla programas de este tipo.

La casilla está siempre activada y no se puede desmarcar.

Software legítimo que los intrusos pueden usar para dañar su equipo o sus datos personales

Esta casilla habilita o deshabilita el control de aplicaciones legítimas que un intruso puede aprovechar para dañar el equipo o los datos de un usuario, como por ejemplo las aplicaciones de administración remota.

La casilla está desactivada de forma predeterminada.

En la sección **Depósito**, puede especificar cuánto tiempo se pueden almacenar los objetos en el depósito de copias de seguridad.

Eliminar objetos con copia de seguridad después de <valor> días

Esta casilla habilita o deshabilita la eliminación de objetos del depósito de copias de seguridad después del período especificado.

Si la casilla está activada, la aplicación elimina los objetos almacenados en el Depósito de copias de seguridad cuando finaliza el plazo indicado en el campo numérico junto a la casilla. Si la casilla está desmarcada, los objetos se almacenan en el Depósito de copias de seguridad durante tiempo indeterminado.

De forma predeterminada, la casilla está marcada 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 que considera de confianza y que no desea analizar para detectar malware.

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 malware.

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



Si hace clic en este botón, se abre una indicación para ingresar las credenciales del administrador. Después de ingresar las credenciales de administrador, la configuración de la aplicación se puede editar.

Pestaña Actualización

En la sección **Bases de datos**, puede configurar el modo de actualización de bases de datos de Kaspersky Endpoint Security.

Descargar actualizaciones automáticamente

Esta casilla habilita o deshabilita la actualización automática de las bases de datos de la aplicación.

La casilla de verificación está activada de forma predeterminada.

En la sección **Proxy**, puede configurar el uso de un servidor proxy para actualizar Kaspersky Endpoint Security.

Usar servidor proxy

Esta casilla de verificación habilita o deshabilita 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.

La casilla de verificación está activada de forma predeterminada.

Configuración

Al hacer clic en este botón, se abre una ventana en la que se puede establecer la configuración de conexión del servidor proxy.

En la sección **Reversión**, puede retroceder a la versión anterior de las bases de datos de la aplicación. Es posible que deba revertir las actualizaciones cuando la nueva versión de las bases de datos de la aplicación contenga una firma incorrecta que haga que Kaspersky Endpoint Security bloquee una aplicación segura.

Revertir actualización

Al hacer clic en este botón, se ejecuta la reversión 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.



Si hace clic en este botón, se abre una indicación para ingresar las credenciales del administrador. Después de ingresar las credenciales de administrador, la configuración de la aplicación se puede editar.

La ventana Ajustes del servidor proxy

Usar configuración del servidor proxy del sistema

Kaspersky Endpoint Security utiliza la configuración del servidor proxy especificada en la configuración del sistema de su Mac.

Esta acción está seleccionada de forma predeterminada.

Usar configuración específica del servidor proxy

Kaspersky Endpoint Security utiliza la configuración del servidor proxy especificada en esta ventana.

Dirección

Campo para escribir la dirección IP o el nombre del dominio de un servidor proxy.

Este campo está disponible si la opción **Usar configuración específica del servidor proxy** está seleccionada.

Puerto

Campo de entrada para el número del puerto del servidor proxy utilizado para actualizar Kaspersky Endpoint Security.

Este campo está disponible si la opción **Usar configuración específica del servidor proxy** está seleccionada.

El valor por defecto es 80.

Usar autenticación

La autenticación es el proceso de verificar el nombre de usuario y la contraseña al conectarse a un servidor proxy.

Esta casilla de verificación habilita/deshabilita la autenticación cuando se conecta a un servidor proxy.

La casilla está desactivada de forma predeterminada.

Nombre de usuario

Campo para ingresar el nombre de usuario para realizar la autenticación al conectarse al servidor proxy.

El campo está disponible si se selecciona la casilla de verificación **Usar autenticación**.

Contraseña

Campo para ingresar la contraseña para la autenticación al conectarse al servidor proxy.

El campo está disponible si se selecciona la casilla de verificación **Usar autenticación**.

Si no ha especificado el nombre de usuario y la contraseña, o si el servidor proxy rechaza el nombre de usuario y la contraseña especificados, se abrirá una ventana donde debe ingresar el nombre de usuario y la contraseña para la autenticación en el servidor proxy. Si la autenticación se realiza correctamente y la casilla **Recordar contraseña** está seleccionada en la ventana de solicitud, el nombre de usuario y la contraseña que especificó se aplicarán en todos los casos en el futuro. Si la casilla de verificación **Recordar contraseña** en la ventana de entrada de nombre de usuario y contraseña no está seleccionada, se le solicitará el nombre de usuario y la contraseña nuevamente en la próxima conexión al servidor proxy.

Omitir el servidor proxy para las direcciones locales

Esta casilla de verificación habilita/deshabilita el uso de un servidor proxy al actualizar la aplicación desde una carpeta local o de red.

La casilla de verificación está activada de forma predeterminada.

El cuadro de diálogo Se necesita autentificación de servidor proxy

Nombre de usuario

Campo para ingresar el nombre de usuario para conectarse al servidor proxy.

Contraseña

Campo para escribir la contraseña.

Recordar contraseña

Esta casilla habilita o deshabilita el uso del nombre de usuario y la contraseña especificados para la autenticación en el servidor proxy en el futuro.

La casilla está desactivada de forma predeterminada.

La pestaña Interfaz

En la sección **Notificaciones**, puede configurar las notificaciones que Kaspersky Endpoint Security muestra para informarle sobre diferentes eventos.

Habilitar notificaciones

Esta casilla habilita o deshabilita las notificaciones sobre los eventos de la aplicación.

La casilla de verificación está activada de forma predeterminada.

Activar los sonidos de alerta al detectar malware

Mediante esta casilla se activan o desactivan las alertas de sonido cuando Kaspersky Endpoint Security detecta un objeto malicioso.

La casilla de verificación está activada de forma predeterminada.

En la sección del **Ícono de la aplicación**, puede configurar el ícono de la aplicación para que se muestre en la barra de menús.

Mostrar en la barra de menús

Esta casilla de verificación habilita/deshabilita la visualización del ícono de la aplicación en la barra de menús.

En la sección **Informes**, puede habilitar o deshabilitar el registro de eventos no críticos en los informes de Kaspersky Endpoint Security.

Registrar eventos no críticos

Esta casilla habilita o deshabilita el registro de eventos informativos en los informes. Generalmente, estos eventos no son importantes para la seguridad del equipo.

En la sección **Rastreo**, puede habilitar o deshabilitar la función de rastreo.

El rastreo es un modo de registrar información detallada sobre la actividad de la aplicación. Los especialistas del Soporte técnico de Kaspersky usan archivos de rastreo para solucionar problemas. Puede habilitar 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 deshabilitado.

Importante: active el rastreo solo cuando un especialista del Soporte técnico se lo indique.

Habilitar rastreo

Esta casilla permite habilitar o deshabilitar la creación de archivos de seguimiento.

La casilla está desactivada de forma predeterminada.

En la sección **Protección con contraseña**, puede habilitar la protección con contraseña sobre acciones no deseadas en el equipo.

Habilitar protección con contraseña

Esta casilla habilita o deshabilita la protección con contraseña respecto de acciones no deseadas.

La casilla está desactivada de forma predeterminada.

Al seleccionar esta casilla, se abre una ventana en la que puede establecer y configurar la contraseña de administrador.

Configuración

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.



Si hace clic en este botón, se abre una indicación para ingresar las credenciales del administrador. Después de ingresar las credenciales de administrador, la configuración de la aplicación se puede editar.

Ventana Configurar contraseña de administrador

Contraseña

Campo para ingresar una contraseña que limite las acciones no deseadas en el dispositivo.

Confirmar contraseña

Campo para ingresar una contraseña por segunda vez a fin de confirmarla.

Opciones

La lista de acciones que pueden protegerse con la contraseña. Seleccione las casillas necesarias para proteger las acciones correspondientes en el dispositivo. Debe seleccionar al menos una.

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 pedirá que ingrese la contraseña cuando intente realizar una acción no deseada en el dispositivo.

El informe de Eventos del sistema

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de Kaspersky Endpoint Security.

Hora

Esta columna muestra la fecha y hora del evento.

Evento

Esta columna 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 desde la que puede guardar el informe en un archivo TXT.

Informe Objetos procesados

El panel derecho de la ventana contiene la lista de todos los objetos infectados y objetos peligrosos de tráfico web que detectó la aplicación Kaspersky Endpoint Security.

Hora

Esta columna muestra la hora en que se detectó el objeto.

Objeto

Esta columna muestra la ruta de la ubicación donde se detectó el objeto en la dirección web del objeto.

Estado

Esta columna muestra la acción que realizó la aplicación tras detectar el objeto.

Detectado

Esta columna muestra el tipo de objeto detectado de acuerdo con la clasificación de la Enciclopedia de virus de Kaspersky.

Nombre

Esta columna muestra el nombre del objeto detectado de acuerdo con la clasificación de la Enciclopedia de virus de Kaspersky.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de Actualización de las bases de datos

El panel derecho de la ventana contiene informes sobre las tareas de actualización que realiza la aplicación.

Iniciado

Esta columna muestra la fecha y hora de inicio de cada tarea de actualización. Si se expande la lista de operaciones, esta columna también enumera las operaciones realizadas durante la actualización de la aplicación y muestra la hora en que se realizaron.

Estado

Esta columna muestra el estado de una tarea de actualización.

Tamaño

Esta columna muestra el tamaño de los archivos de actualización descargados.

Velocidad promedio

Esta columna muestra la velocidad de la descarga de archivos de actualización.

Hora de finalización

Esta columna muestra la hora en que se completó una tarea de actualización.

Al hacer clic en este botón, se expande la lista de las operaciones incluidas en una tarea de actualización.

Al hacer clic en este botón, se repliega la lista de las operaciones incluidas en una tarea de actualización.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

Informe de Análisis

El panel derecho de la ventana contiene informes sobre las tareas de análisis que realiza Kaspersky Endpoint Security.

Tarea

Esta columna muestra el nombre de una tarea de análisis.

Estado

Esta columna muestra el estado de una tarea de análisis o el estado de los objetos analizados.

Fecha

Esta columna muestra la fecha y hora de una tarea de análisis.

Iniciador

Esta columna muestra el usuario, la aplicación o el proceso que inició una tarea de análisis.

Al hacer clic en este botón, se expande 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 desde la que puede guardar el informe en un archivo TXT.

El informe de la Protección frente a amenazas en archivos

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de la Protección contra archivos peligrosos.

Fecha

Esta columna muestra la fecha y hora en la que la aplicación accedió a un objeto analizado.

Ruta

Esta columna muestra la ruta de la ubicación original de un objeto analizado.

Estado

Esta columna muestra el estado de un objeto analizado.

Nombre del programa

Esta columna muestra la aplicación a la que accedió un objeto analizado.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de Protección frente a amenazas en la web

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de la Protección frente a amenazas en la web.

Fecha

Esta columna muestra la fecha y hora en las que los objetos de tráfico web se detectaron.

URL

Esta columna muestra los objetos de tráfico web que han sido detectados mediante la Protección frente a amenazas en la web. Para cada objeto del tráfico web detectado, la columna especifica la dirección web donde se detectó.

Estado

Esta columna muestra el estado de objetos de tráfico web que se han detectado.

Nombre del programa

Esta columna muestra el programa al que accedieron los objetos de tráfico web detectados.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de la Protección contra amenazas de correo

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de la Protección contra amenazas de correo.

Fecha

Esta columna muestra la fecha y hora en que se detectó un objeto infectado en un mensaje de correo electrónico.

Ruta

Esta columna muestra información sobre el mensaje de correo electrónico donde se detectó el objeto infectado.

Estado

Esta columna muestra la acción realizada por Kaspersky Endpoint Security al 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 desde la que puede guardar el informe en un archivo TXT.

El informe de Protección frente a amenazas en la red

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de la Protección contra amenazas de red.

Fecha

Esta columna muestra la fecha y hora en que se detectó actividad de red peligrosa en el equipo.

Dirección IP

Esta columna muestra la lista de direcciones IP de equipos en los que Kaspersky Endpoint Security detectó actividad de red peligrosa.

Estado

Esta columna muestra la acción realizada por Kaspersky Endpoint Security al detectar actividad de red peligrosa.

Tipo de ataque

Esta columna muestra el tipo de ataque de red detectado.

Puerto local

Esta columna muestra el número de puerto local a través del cual se intentó ingresar.

Protocolo

Esta columna muestra el tipo de protocolo usado para cometer el ataque.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en 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

Esta columna muestra la fecha y hora de los eventos.

Evento

Esta columna muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de Firewall

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de Firewall.

Fecha

Esta columna muestra la fecha y hora de los eventos.

Evento

Esta columna muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de Prevención de exploits

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de la Prevención de exploits.

Fecha

Esta columna muestra la fecha y hora de los eventos.

Evento

Esta columna muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de Control de dispositivos

En el panel derecho de la ventana se muestra un informe sobre el funcionamiento de Control de dispositivos.

Fecha

Esta columna muestra la fecha y hora de los eventos.

Evento

Esta columna muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

El informe de la Vigía proactiva

El panel derecho de la ventana contiene un informe sobre el funcionamiento del componente Vigía proactiva.

Fecha

Esta columna muestra la fecha y hora de los eventos.

Evento

Esta columna muestra el estado de los eventos.



Al hacer clic en este botón, se abre una ventana desde la que puede guardar el informe en un archivo TXT.

La ventana Tipo de instalación

En la sección **Paquetes a instalar**, puede seleccionar los componentes de la aplicación que se instalarán en un equipo cliente.

Análisis

Esta casilla agrega el componente Análisis al paquete de instalación de Kaspersky Endpoint Security.

La casilla está seleccionada de forma predeterminada y no se puede desmarcar.

Protección contra amenazas de archivo

Esta casilla habilita o deshabilita la adición del componente Protección contra archivos peligrosos al paquete de instalación de Kaspersky Endpoint Security.

Si la casilla está seleccionada, el componente Protección contra archivos peligrosos se incluye en el paquete de instalación de Kaspersky Endpoint Security.

Si la casilla no está seleccionada, el componente Protección contra archivos peligrosos no se incluye en el paquete de instalación de Kaspersky Endpoint Security.

Esta casilla está seleccionada por defecto.

Protección contra amenazas web

Esta casilla habilita o deshabilita la adición del componente Protección contra amenazas web al paquete de instalación de Kaspersky Endpoint Security.

Si la casilla está seleccionada, el componente Protección contra amenazas web se incluye en el paquete de instalación de Kaspersky Endpoint Security.

Si la casilla no está seleccionada, el componente Protección contra amenazas web no se incluye en el paquete de instalación de Kaspersky Endpoint Security.

Esta casilla está seleccionada por defecto.

Protección contra amenazas de red

Esta casilla habilita o deshabilita la adición del componente Protección contra amenazas de red al paquete de instalación de Kaspersky Endpoint Security.

Si la casilla está seleccionada, el componente Protección contra amenazas de red se incluye en el paquete de instalación de Kaspersky Endpoint Security.

Si la casilla no está seleccionada, el componente Protección contra amenazas de red no se incluye en el paquete de instalación de Kaspersky Endpoint Security.

Esta casilla está seleccionada por defecto.

Conector del Agente de red

Esta casilla agrega el componente Conector del Agente de red al paquete de instalación de Kaspersky Endpoint Security.

La casilla está seleccionada de forma predeterminada y no se puede desmarcar.

La ventana Configuración de protección con contraseña

Contraseña

Campo para ingresar una contraseña que limite las acciones no deseadas en los dispositivos de los usuarios.

Haga clic en **Mostrar** para ver los símbolos ingresados.

Confirmar contraseña

Campo para ingresar una contraseña por segunda vez a fin de confirmarla.

Haga clic en **Mostrar** para ver los símbolos ingresados.

Solicitar contraseña para

La lista de acciones que pueden protegerse con la contraseña. Seleccione las casillas de verificación necesarias para proteger las acciones correspondientes en el dispositivo del usuario.

El cuadro de diálogo “Otorgar acceso”

Obtener clave de recuperación

Al hacer clic en este botón, se genera una clave de recuperación necesaria para acceder a un disco cifrado en un equipo cliente.

La sección Protección avanzada contra amenazas

En la sección **Configuración de KSN**, puede configurar el uso de Kaspersky Security Network.

Kaspersky Security Network

El conmutador de alternancia **Kaspersky Security Network** habilita o deshabilita la participación en Kaspersky Security Network.

Si el conmutador de alternancia **Kaspersky Security Network** está activado, los equipos cliente a los que se aplica la directiva participan en Kaspersky Security Network.

Si el conmutador de alternancia **Kaspersky Security Network** no está activado, los equipos cliente a los que se aplica la directiva no participan en Kaspersky Security Network.

Este conmutador de alternancia está desactivado de manera predeterminada.

Modo de KSN extendido

El conmutador de alternancia **Modo KSN extendido** habilita/deshabilita el envío de datos adicionales desde el equipo remoto a Kaspersky. Estos datos se utilizan para mejorar la protección de los equipos cliente y la usabilidad de Kaspersky Endpoint Security.

Si **Modo ampliado de KSN** está habilitado, los equipos cliente a los que se aplica la directiva proporcionan tanto los datos necesarios para el funcionamiento de los servicios de detección como datos adicionales a Kaspersky Security Network.

Si **Modo KSN extendido** está deshabilitado, los equipos cliente a los que se aplica la directiva proporcionan solo los datos necesarios para el funcionamiento de los servicios de detección. No se proporcionan datos adicionales a Kaspersky Security Network.

El conmutador de alternancia **Modo de KSN extendido** está desactivado de manera predeterminada.

El conmutador de alternancia se activa automáticamente si activa el conmutador de alternancia **Kaspersky Security Network**, pero puede desactivarlo.

Datos proporcionados a Kaspersky mediante Kaspersky Security Network en la infraestructura de KSN Global

Si el conmutador de alternancia de **Kaspersky Security Network** está habilitado y el conmutador de **Modo ampliado de KSN** está deshabilitado, el software Kaspersky Endpoint Security que se ejecuta en los equipos cliente proporciona a Kaspersky los siguientes datos:

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

- Versión completa del Software instalado;
  tipo del Software instalado;
  identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador único del dispositivo; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

Si los conmutadores de alternancia de **Kaspersky Security Network** y **Modo ampliado de KSN** están habilitados, el software Kaspersky Endpoint Security que se ejecuta en los equipos cliente proporciona a Kaspersky los siguientes datos:

- información acerca de la versión del sistema operativo (SO) y los paquetes de servicio instalados en la computadora, la versión y las sumas de comprobación (MD5, SHA2-256, SHA1) del archivo de kernel del SO, y los parámetros del modo de ejecución del SO; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información ampliada de 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 del procesamiento del evento acerca de la acción del SO en el subsistema de defensa proactivo; cantidad de eventos de acción procesados del SO; 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 del procesamiento del evento acerca de la acción del SO en el subsistema de almacenamiento del evento recurrente; 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 de una acción en el SO.

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

- Información acerca de la aplicación del Titular de los derechos que se instaló y acerca del estado de protección antivirus: identificador de la instalación (PCID) del software; 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 del Software instalado; identificador de actualización del Software; identificador del servicio de reputación; identificador del tipo de protocolo; identificador de un centro de activación regional; versión de la lista de decisiones revocadas del servicio del Software; identificador del registro desencadenado 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 de las bases de datos antivirus del software; identificador exclusivo de instalación del Software en la computadora; 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 para el 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; identificador del software; suma de comprobación del archivo de clave del software; identificador del modelo de información usado para proporcionar la licencia del software; identificador del certificado usado para firmar el encabezado de la solicitud de la licencia del software; la fecha y hora de creación de la solicitud de licencia del software; la suma de comprobación de la solicitud de licencia del software; la versión de la solicitud de licencia del software; la versión del código de activación del software; formato de los datos en la solicitud a la infraestructura del titular de los derechos; identificador de la solicitud de licencia actual; identificador 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 de puerto; dirección web del origen de la solicitud de servicio web (referenciador); 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; identificador de actualización del Software; tipo del Software instalado; fecha y hora de inicio de la Vigía proactiva; fecha y hora de instalación del software; probabilidad de que la Vigía proactiva envíe estadísticas; código del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo de procesamiento de la base de datos del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; tiempo máximo permitido para el procesamiento de un evento por parte de la Vigía proactiva; tiempo de procesamiento del evento que demoró más del tiempo estándar en ser procesado por la Vigía proactiva; cantidad total de eventos que demoraron más del tiempo estándar en ser procesados por la Vigía proactiva.

- Información sobre todos los objetos y operaciones analizados: veredicto del software sobre el 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 la Vigía proactiva; fecha y hora de detección de software por la Vigía proactiva; características de detección; identificador del registro desencadenado en las bases de datos antivirus del software; motivo por el que la Vigía proactiva detectó el software; 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 desencadenado de las bases de datos antivirus del software; ruta hacia el objeto que se procesa; el nombre del objeto analizado; la fecha y la hora del análisis; las direcciones URL y del referido desde las que se descargó; el tamaño de los archivos analizados y la ruta 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 empacador (si se empacó el archivo); 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 valor de la suma de control complementaria del objeto; datos acerca de la firma digital del objeto (certificado): 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 de firma del archivo; el nombre, el tipo, el tipo de identificador, la suma de comprobación (MD5) y el tamaño de la aplicación que cargó el objeto que se está validando; la ruta de la aplicación y las rutas de las plantillas; un atributo que indique la presencia en la Lista de ejecución automática; la fecha de entrada; la lista de atributos; el nombre del empaquetador; la información acerca de la firma digital de la aplicación: el certificado del editor, el nombre del archivo cargado en formato MIME, la fecha y la 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 empaquetador (si el archivo estaba empaquetado), 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 inició 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 del solicitud 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 empaquetadores (si se empaquetó el archivo); la información sobre la disponibilidad y validez de estas estadísticas; el identificador del modo para generar las estadísticas que se envían.

- Si se detectan amenazas o vulnerabilidades, además de la información sobre el objeto detectado, se proporciona información sobre el identificador, la versión y el tipo de registro en la base de datos antivirus, el nombre de la amenaza según la clasificación de Kaspersky, la fecha y hora de la última actualización de la base de datos antivirus, el nombre del archivo ejecutable, la suma de comprobación (MD5) del archivo de la aplicación que solicitó la URL donde se detectó la amenaza, la dirección IP (IPv4 o IPv6) de la amenaza detectada, el identificador de vulnerabilidad y su nivel de amenaza, la URL y el referente de la página web donde se detectó la vulnerabilidad.

- Si se detecta un posible objeto malicioso, la información acerca de los datos se proveerá en la memoria de los procesos.

- Información sobre ataques de red: dirección IP del equipo atacante y número del puerto en la computadora del usuario al que ataca la red, identificador del protocolo de ataque, nombre y tipo de ataque.

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

- Las direcciones URL e IP de la página web en la que se detectó contenido dañino o sospechoso; el nombre, el tamaño y la suma de comprobación del archivo que solicitó la dirección URL; el identificador, el peso y el grado de la regla utilizada para llegar a un veredicto, el objetivo del ataque.

- Información sobre actualizaciones de la aplicación instalada y bases de datos antivirus: estado de terminación de la tarea de actualización, tipo de error que puede ocurrir durante el proceso de actualización, cantidad de actualizaciones con errores, identificador del componente de la aplicación que realiza actualizaciones.

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

- Información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se detectó el evento, tipo y categoría del evento, nombre del origen del evento y descripción del evento.

- Información para determinar la reputación de archivos y direcciones URL: la dirección URL en la que se solicita la reputación y la referencia, el 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 analizado (MD5), el tipo de amenaza detectada, la información sobre el registro usado para detectar una amenaza (el identificador de registro para la base de datos del antivirus y el tipo y la marca de tiempo del registro); clave pública del certificado; huella digital del certificado digital del objeto analizado y algoritmo de dispersión.

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

- Información sobre la licencia en uso: el tipo y la validez del período de licencia, la cantidad de días restantes hasta el vencimiento de la licencia, el identificador del partner desde el cual se adquirió la licencia, el identificador del Centro de Activación Regional, la suma de comprobación del código de activación, el hash del cuerpo de la tarjeta que se calculó mediante el uso del algoritmo SHA1, la fecha y hora de la creación de la tarjeta de la licencia, el identificador de la información de la licencia, el identificador de la tarjeta de la licencia, el identificador de la secuencia de la tarjeta de la licencia, el identificador único de la computadora del usuario, la fecha desde la cual se considera válida la tarjeta de la licencia, la fecha en la que la tarjeta de la licencia es válida, el estado actual de la tarjeta de la licencia, la versión del encabezado de la licencia, la versión de la licencia, el identificador del certificado de la firma en el encabezado de la tarjeta, la suma de comprobación del archivo de clave, el número de serie del signatario en el encabezado de la tarjeta, el token de autenticación.

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

- Información sobre el dispositivo: ID de dispositivo.

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

Modo nube

El conmutador de alternancia del **modo nube** habilita/deshabilita 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 habilitada. 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 habituales. 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 donde puede leer el texto de la Declaración de Kaspersky Security Network y aceptar los términos de participación en Kaspersky Security Network.

Nota: si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Web Console y, según la configuración 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 del proxy de KSN**, puede configurar las opciones del proxy de KSN.

Usar el proxy de KSN

Esta casilla habilita o deshabilita el uso de un servidor proxy cuando se conecta a Kaspersky Security Network.

Si la casilla está seleccionada, Kaspersky Endpoint Security utiliza un servidor proxy para conectarse a Kaspersky Security Network.

Si la casilla no está seleccionada, Kaspersky Endpoint Security se conecta a Kaspersky Security Network directamente.

Esta casilla está desactivada por defecto.

Usar los servidores de Kaspersky cuando el proxy de KSN no esté disponible

Esta casilla habilita o deshabilita el uso de los servidores de Kaspersky si el Proxy de KSN no está disponible.

Si se selecciona esta casilla, Kaspersky Endpoint Security usa los servidores de Kaspersky cuando el Proxy de KSN no está disponible.

Si no se selecciona esta casilla, Kaspersky Endpoint Security no usa los servidores de Kaspersky cuando el Proxy de KSN no está disponible.

Esta casilla está desactivada por defecto.

Esta casilla está disponible si la casilla **Usar el proxy de KSN** está seleccionada.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Participación en Kaspersky Security Network/Kaspersky Private Security Network”

Más información

Al hacer clic en este vínculo, se abre una nueva ventana del navegador donde puede leer el texto de la Declaración de Kaspersky Security Network o la Declaración de Kaspersky Private Security Network.

Acepto los términos de participación en Kaspersky Security Network/Kaspersky Private Security Network

Los equipos a los que se aplica la directiva participan en Kaspersky Security Network/Kaspersky Private Security Network.

No acepto los términos de participación en Kaspersky Security Network/Kaspersky Private Security Network

Los equipos a los que 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 está disponible. Para obtener información detallada sobre la participación en Kaspersky Private Security Network, consulte la Ayuda de Kaspersky Security Center.

La sección Protección básica contra amenazas

Protección contra amenazas de archivo

Al hacer clic en este vínculo, se abre una ventana donde puede ajustar la configuración de Protección contra archivos peligrosos.

Protección contra amenazas web

Al hacer clic en este vínculo, se abre una ventana donde puede ajustar la Configuración de Protección contra amenazas web.

Protección contra amenazas de red

Al hacer clic en este vínculo, se abre una ventana donde puede configurar los parámetros de la Protección contra amenazas de red.

Protección contra amenazas de correo

Al hacer clic en este vínculo, se abre una ventana donde puede ajustar la configuración de Protección contra amenazas de correo.

Firewall

Al hacer clic en este vínculo, se abre una ventana donde puede ajustar la configuración del Firewall.

La ventana Protección contra amenazas de archivo

Protección contra archivos peligrosos

El conmutador de alternancia **Protección contra archivos peligrosos** habilita o deshabilita la Protección contra archivos peligrosos.

Si el conmutador de alternancia **Protección contra archivos peligrosos** está activado, Kaspersky Endpoint Security realiza una supervisión en tiempo real del sistema de archivos de los equipos cliente a los que se aplica la directiva.

Si el conmutador de alternancia **Protección contra archivos peligrosos** está desactivado, Kaspersky Endpoint Security no protege el sistema de archivos de los equipos cliente a los que se aplica la directiva.

Este conmutador de alternancia está activado de forma predeterminada.

En la sección **Alcance de la protección**, puede configurar un alcance de la protección si selecciona uno de los elementos preestablecidos o agrega archivos o carpetas de su elección.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede especificar un archivo, carpeta o máscara que se agregará a la lista de objetos incluidos en el alcance de la protección.

Eliminar

Si hace clic en el botón, se quita un objeto del alcance de la protección.

Este botón está disponible si se selecciona un objeto en la lista de objetos protegidos.

No se puede eliminar los objetos predeterminados incluidos en el alcance de la protección.

Alcance de la protección

Esta columna contiene los objetos que Kaspersky Endpoint Security analiza cuando la Protección contra archivos peligrosos está habilitada.

De forma predeterminada, Kaspersky Endpoint Security analiza los siguientes objetos:

- **Todos 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 de alternancia en esta columna está activado, Kaspersky Endpoint Security analiza el objeto correspondiente en la columna **Alcance de la protección** cuando la Protección contra archivos peligrosos está habilitada.

Si el conmutador de alternancia en esta columna está desactivado, Kaspersky Endpoint Security no analiza el objeto correspondiente en la columna **Alcance de la protección** cuando la Protección contra archivos peligrosos está habilitada.

Adicional

Esta columna indica si Kaspersky Endpoint Security analiza las subcarpetas del objeto correspondiente.

En la sección **Si se detecta un objeto malicioso**, puede seleccionar la acción que realiza Kaspersky Endpoint Security al detectar un objeto malicioso.

Solicitar acción

Kaspersky Endpoint Security despliega una ventana de notificación con información sobre el objeto malicioso que ha infectado el archivo y solicita al usuario que seleccione la acción que debe realizar la aplicación. Las acciones disponibles pueden variar según el estado del objeto.

Esta opción está seleccionada por defecto.

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 la desinfección se realiza correctamente, Kaspersky Endpoint Security guarda el archivo en su ubicación original con el nombre del archivo original. Si falla la desinfección, 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 la desinfección se realiza correctamente, Kaspersky Endpoint Security guarda el archivo en su ubicación original con el nombre del archivo original. Si la desinfección falló, Kaspersky Endpoint Security mantiene el archivo infectado en estado bloqueado en su ubicación inicial.

En la sección **Optimización**, puede configurar el rendimiento del análisis y seleccionar el algoritmo de análisis.

Analizar solo los archivos nuevos y modificados

Esta casilla habilita o deshabilita el análisis de solo los archivos que Kaspersky Endpoint Security reconoce como nuevos o modificados desde el último análisis.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza solo los archivos que reconoce como nuevos o modificados desde el último análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza todos los archivos.

Esta casilla está seleccionada por defecto.

Omitir análisis de volumen del sistema de solo lectura

La casilla habilita o deshabilita el análisis del volumen de sistema de solo lectura de Kaspersky Endpoint Security.

Si la casilla está seleccionada, Kaspersky Endpoint Security no analiza el volumen de sistema de solo lectura. Esto reduce significativamente el tiempo de análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza el volumen de sistema de solo lectura.

Esta casilla está seleccionada por defecto.

Usar iSwift

Esta casilla habilita o deshabilita el uso de la tecnología iSwift durante el análisis. iSwift permite que Kaspersky Endpoint Security use un algoritmo especial para excluir ciertos objetos del análisis, lo que aumenta la velocidad de análisis.

Si la casilla está seleccionada, Kaspersky Endpoint Security usa iSwift durante el análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no usa iSwift durante el análisis.

Esta casilla está seleccionada por defecto.

En la sección **Tipos de archivo**, puede seleccionar qué archivos serán analizados por Kaspersky Endpoint Security cuando la Protección contra archivos peligrosos está habilitada.

Analizar todos los archivos

Kaspersky Endpoint Security analiza todos los objetos del sistema de archivos que se ejecutan, abren o guardan.

Analizar las aplicaciones y los documentos por contenido

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados en función de su contenido.

Analizar las aplicaciones y los documentos por extensión

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados en función de la extensión del archivo.

Kaspersky define la lista de extensiones, la cual 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 analiza Kaspersky Endpoint Security cuando la Protección contra archivos peligrosos está habilitada.

Analizar archivos comprimidos

Esta casilla habilita o deshabilita el análisis de los archivos comprimidos. Para ver la lista de extensiones, consulte la ayuda de Kaspersky Endpoint Security.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los archivos comprimidos.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los archivos comprimidos durante el análisis.

Analizar paquetes de instalación

Esta casilla habilita o deshabilita el análisis de los paquetes de instalación.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los paquetes de instalación.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los paquetes de instalación durante el análisis.

Analizar objetos OLE incrustados

Esta casilla habilita o deshabilita el análisis de objetos incrustados en archivos, como hojas de cálculo Excel, macros o archivos adjuntos de correo electrónico.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los objetos OLE incrustados.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los objetos OLE incrustados durante el análisis.

No extraer archivos comprimidos más grandes que MB

Esta casilla habilita o deshabilita un límite en el tamaño de los archivos comprimidos a analizar.

Si la casilla está seleccionada, Kaspersky Endpoint Security omite los archivos comprimidos mayores que el tamaño especificado durante el análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security extrae y analiza los archivos comprimidos sin importar su tamaño.

Esta casilla está disponible si la casilla **Analizar archivos comprimidos** está seleccionada.

Posponer la extracción de archivos comprimidos más grandes que MB

Una opción que limita el tamaño de los archivos comprimidos a analizar.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza todos los archivos comprimidos cuyo tamaño excede el límite establecido, pero lo hace con una prioridad más baja dos minutos después de detectarlos.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza todos los archivos comprimidos con la misma prioridad.

Esta casilla está disponible si la casilla **Analizar archivos comprimidos** está seleccionada.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar alcance de la protección”

Ingrese un nombre de archivo, nombre de carpeta o campo de entrada de máscara

Ruta a un archivo, carpeta o máscara de archivo/carpeta.

El objeto es una carpeta

Esta casilla habilita o deshabilita el análisis de un objeto como una carpeta.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza el objeto que ha especificado en el campo **Introduzca un nombre de archivo, de carpeta o máscara** como una carpeta.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza el objeto que ha especificado en el campo **Introduzca un nombre de archivo, de carpeta o máscara** como un archivo.

Esta casilla está seleccionada por defecto.

Incluir subcarpetas

Esta casilla habilita o deshabilita el análisis de las subcarpetas de la carpeta especificada en el campo **Introduzca un nombre de archivo, de carpeta o máscara**.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza las subcarpetas durante los análisis de malware.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza solo los archivos que se encuentran directamente en la carpeta especificada en **Introduzca un nombre de archivo, de carpeta o máscara** durante los análisis de malware.

Esta casilla está seleccionada por defecto.

La ventana “Protección contra amenazas web”

Protección contra amenazas web

El conmutador de alternancia de **Protección contra amenazas web** habilita o deshabilita la Protección contra amenazas web.

Si el conmutador de alternancia de **Protección contra amenazas web** está activado, la Protección contra amenazas web analiza los datos que su equipo envía y recibe a través de los protocolos HTTP y HTTPS en Safari, Google Chrome o Firefox.

Si el conmutador de alternancia de **Protección contra amenazas web** está desactivado, la Protección contra amenazas web no analiza los datos que su equipo envía y recibe a través de los navegadores web.

Este conmutador de alternancia está activado de forma predeterminada.

En la sección **Si se detecta un objeto malicioso**, puede seleccionar la acción que realiza Kaspersky Endpoint Security al detectar un objeto malicioso.

Solicitar acción

Kaspersky Endpoint Security muestra una ventana de notificaciones con información sobre el tipo de malware que infectó el objeto del tráfico web y le solicita que seleccione la acción que Kaspersky Endpoint Security debe realizar sobre este objeto. Las acciones disponibles pueden variar según el estado del objeto.

Esta acción está seleccionada de forma predeterminada.

Bloquear automáticamente

Kaspersky Endpoint Security bloquea automáticamente el acceso a objetos peligrosos de tráfico web.

En la sección **Direcciones web de confianza**, puede crear o editar una lista de direcciones web de confianza y habilitar o deshabilitar el análisis del tráfico proveniente de las direcciones web en esta lista.

No analizar el tráfico web de direcciones web de confianza

Esta casilla habilita o deshabilita el análisis del tráfico web desde direcciones web de confianza.

Si la casilla está seleccionada, Kaspersky Endpoint Security no analiza el tráfico web de direcciones web de confianza.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza el tráfico web de direcciones web de confianza.

Esta casilla está desactivada por defecto.

Lista de direcciones web

Esta lista contiene direcciones web de confianza.

Puede desmarcar la casilla junto a una dirección web de la lista. Si la casilla no está seleccionada, la Protección contra amenazas web analiza el tráfico web de las direcciones web.

La lista está disponible si selecciona la casilla **No analizar el tráfico web de direcciones web de confianza**.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede introducir una dirección web o una máscara de direcciones web para agregar a la lista de direcciones web de confianza.

Eliminar

Al hacer clic en este botón, se elimina la dirección web o la máscara de direcciones web seleccionadas en la lista.

Este botón está disponible cuando se selecciona una dirección web o una máscara de direcciones web en la lista de direcciones web de confianza.

Dirección web

Esta columna contiene direcciones web de confianza.

Estado

Si el conmutador de alternancia en esta columna está activado, Kaspersky Endpoint Security no analiza el objeto correspondiente de la columna **Dirección web** cuando la Protección contra amenazas web está habilitada y la casilla de verificación **No analizar el tráfico web de direcciones web de confianza** está seleccionada.

Si el conmutador de alternancia en esta columna está desactivado, Kaspersky Endpoint Security analiza el objeto correspondiente de la columna **Dirección web** cuando la Protección contra amenazas web está habilitada y la casilla de verificación **No analizar el tráfico web de direcciones web de confianza** está seleccionada.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar dirección web”

Campo de entrada Dirección web

Una dirección web o máscara de direcciones web cuyo tráfico no será analizado por la Protección contra amenazas web.

En la sección **Estado**, puede definir si Kaspersky Endpoint Security analiza el tráfico desde esta dirección web o grupo de direcciones web.

Deshabilitar

La dirección web o la máscara de direcciones web se agrega a la lista de **Direcciones web de confianza**, pero Kaspersky Endpoint Security analiza su tráfico.

Habilitar

La dirección web o la máscara de direcciones web se agrega a la lista de **Direcciones web de confianza** y Kaspersky Endpoint Security no analiza su tráfico.

La ventana “Protección contra amenazas de red”

Protección contra amenazas de red

El conmutador de alternancia de **Protección contra amenazas de red** habilita o deshabilita la Protección contra amenazas de red.

Si el conmutador de alternancia **Protección contra amenazas de red** está activado, Kaspersky Endpoint Security protege el equipo remoto contra ataques de red.

Si el conmutador de alternancia **Protección contra amenazas de red** está desactivado, Kaspersky Endpoint Security no protege el equipo remoto contra ataques de red.

Este conmutador de alternancia está activado de forma predeterminada.

En la sección **Configuración de protección contra amenazas de red**, puede modificar el período durante el cual Kaspersky Endpoint Security bloquea los equipos atacantes.

Bloquear los equipos atacantes por min

Esta casilla habilita o deshabilita la adición de equipos atacantes a la lista de equipos bloqueados durante el período especificado.

Si la casilla está seleccionada, Kaspersky Endpoint Security agrega equipos atacantes a la lista de equipos bloqueados durante el período especificado.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no bloquea los equipos atacantes.

Esta casilla está seleccionada por defecto.

De forma predeterminada, los equipos atacantes se bloquean durante 60 minutos.

En la sección **Exclusiones**, puede crear o editar una lista de direcciones IP de equipos remotos cuya actividad de red nunca será bloqueada por Kaspersky Endpoint Security.

Lista de direcciones IP

Esta lista contiene direcciones IP de equipos remotos cuya actividad de red nunca es bloqueada por Kaspersky Endpoint Security.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede ingresar la dirección IP de un equipo remoto.

Eliminar

Al hacer clic en este botón, se elimina de la lista la dirección IP seleccionada.

Para que este botón esté disponible, deberá seleccionar la dirección IP de un equipo remoto en la lista de direcciones IP.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar exclusión”

Campo de entrada Dirección IP

La dirección IP de un equipo remoto.

La sección “Controles de seguridad”

Control Web

El conmutador de alternancia **Control Web** habilita o deshabilita el Control Web.

Si el conmutador de alternancia **Control Web** está activado, puede crear reglas para administrar los sitios web que los usuarios visitan en equipos remotos.

Si el conmutador de alternancia **Control Web** está desactivado, no puede administrar los sitios web que los usuarios visitan en equipos remotos.

Este conmutador de alternancia está desactivado de manera predeterminada.

Lista de reglas

Esta lista contiene reglas que ha creado para administrar sitios web que los usuarios visitan en equipos remotos.

El orden en que se clasifican las reglas determina la prioridad de su aplicación por parte de Kaspersky Endpoint Security.

Agregar

Al hacer clic en este botón, se abre una ventana en la que puede crear una nueva regla para Control Web.

Eliminar

Al hacer clic en este botón, se elimina la regla seleccionada de la lista de reglas.

Este botón está disponible si la casilla de verificación junto a la regla está seleccionada.

Subir

Al hacer clic en este botón, la regla seleccionada sube en la lista de reglas y aumenta la prioridad de su aplicación por parte de Kaspersky Endpoint Security.

Bajar

Al hacer clic en este botón, la regla seleccionada baja en la lista de reglas y disminuye la prioridad de su aplicación por parte de Kaspersky Endpoint Security.

Nombre

El nombre de la regla.

Estado

El conmutador de alternancia de esta columna define si la regla está activa o no.

Puede activar o desactivar el conmutador de alternancia junto a una regla correspondiente para cambiar el estado de la regla.

Acción

Una acción que Kaspersky Endpoint Security realiza cuando el usuario visita una determinada dirección web, grupo de direcciones web o categoría de sitios web afectados por la regla.

Puede cambiar la acción asignada si selecciona otra opción en el menú contextual correspondiente en esta columna.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Editar regla”

Campo de entrada Nombre de regla

El nombre de la regla.

En la sección **Estado**, puede configurar la regla para que esté activa o inactiva.

Activa

Si se selecciona esta opción, se crea una regla activa. Se aplicará al equipo remoto inmediatamente después de que se aplique la directiva.

Inactiva

Si se selecciona esta opción, se crea una regla inactiva. Quedará pendiente cuando se aplique la directiva.

En la sección **Acción**, puede seleccionar la acción que Kaspersky Endpoint Security realiza cuando el usuario visita una determinada dirección web, grupo de direcciones web o categoría de sitios web afectados por la regla.

Permitir

Si se selecciona esta opción, Kaspersky Endpoint Security permite al usuario visitar la dirección web, el grupo de direcciones web o la categoría de sitios web afectados por la 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 por defecto.

Bloquear

Si se selecciona esta opción, Kaspersky Endpoint Security evita que el usuario visite la dirección web, el grupo de direcciones web o la categoría de sitios web afectados por la 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 se selecciona esta opción, Kaspersky Endpoint Security muestra una advertencia cuando el usuario trata de visitar la dirección web, el grupo de direcciones web o la categoría de sitios web afectados por la regla.

En la sección **Área de la regla**, puede elegir crear una regla para una dirección web, grupo de direcciones web o categorías de sitios web en particular.

Categorías

Si se selecciona esta opción, se crea una regla para las categorías de sitios web.

Seleccione las categorías

Al hacer clic en este vínculo, se abre un cuadro de diálogo donde puede seleccionar las categorías de sitios web afectadas por la regla.

Direcciones individuales

Si se selecciona esta opción, se crea una regla para una dirección web o un grupo de direcciones web en particular.

Esta opción está seleccionada por defecto.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede especificar una dirección web o máscara de direcciones web afectadas por la regla.

Eliminar

Al hacer clic en este botón, se elimina la dirección web o la máscara de direcciones web seleccionadas de la lista de direcciones web afectadas por la regla.

Este botón está disponible si la casilla de verificación junto a la dirección web o la máscara de direcciones web está seleccionada.

Dirección

Las direcciones web o máscaras de direcciones web afectadas por la regla.

El cuadro de diálogo "Agregar dirección web"

Campo de entrada Dirección web

Dirección web o máscara de direcciones web que se verá afectada por la regla.

El cuadro de diálogo "Categorías de contenido"

Lista de categorías de contenido

Esta lista contiene la lista de categorías de sitios web que puede agregar a la regla.

La casilla junto al nombre de la categoría de sitios web agrega/elimina de la regla los sitios web que pertenecen a esta categoría.

Todas las casillas están desmarcadas de manera predeterminada.

La sección Detection and Response

Managed Detection and Response

Al hacer clic en este vínculo, se abre una ventana en la que puede configurar Managed Detection and Response.

Endpoint Detection and Response

Al hacer clic en este vínculo, se abre una ventana en la que puede configurar Endpoint Detection and Response.

Endpoint Detection and Response Expert (on-premise)

Al hacer clic en este vínculo, se abre una ventana en la que puede configurar Endpoint Detection and Response Expert (on-premise).

La ventana "Managed Detection and Response"

Managed Detection and Response

El conmutador de alternancia de **Managed Detection and Response** habilita o deshabilita 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 conmutador de alternancia de **Managed Detection and Response** está activado y se importa el archivo de configuración de MDR, se habilita el componente Managed Detection and Response.

Si el conmutador de alternancia de **Managed Detection and Response** está desactivado, el componente Managed Detection and Response está deshabilitado.

Este conmutador de alternancia está desactivado de manera predeterminada.

Importar

Al hacer clic en este botón, se abre la ventana que permite importar el archivo de configuración de MDR en la política de Kaspersky Endpoint Security.

Eliminar archivo de configuración

Al hacer clic en este botón, se elimina el archivo de configuración MDR de la directiva de Kaspersky Endpoint Security.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Endpoint Detection and Response

Endpoint Detection and Response

El conmutador de alternancia **Endpoint Detection and Response** habilita o deshabilita el componente Endpoint Detection and Response, que interactúa con la solución Kaspersky Endpoint Detection and Response. Esta solución protege los equipos contra amenazas complejas, incluidos nuevos exploits, ransomware y ataques sin archivos.

Si el conmutador de alternancia de **Endpoint Detection and Response** está activado, el componente Endpoint Detection and Response está habilitado.

Si el conmutador de alternancia de **Endpoint Detection and Response** está desactivado, el componente Endpoint Detection and Response está deshabilitado.

Este conmutador de alternancia está desactivado de manera predeterminada.

En la sección **Aislamiento de la red**, puede establecer la configuración para aislar los equipos de la red en respuesta a la detección de un indicador de vulneración.

Establezca la configuración del desbloqueo del equipo

Al hacer clic en este vínculo, se abre una ventana en la que puede especificar el retraso para desactivar automáticamente el Aislamiento de la red.

Exclusiones

Al hacer clic en este vínculo, se abre una ventana en la que puede especificar las conexiones de red que no se bloquean en el equipo una vez que se habilita automáticamente el Aislamiento de la red.

En la sección **Prevención de ejecución**, puede establecer la configuración para el funcionamiento de archivos ejecutables y scripts, y la apertura de archivos Office.

Prevención de ejecución

El conmutador de alternancia **Prevención de ejecución** habilita o deshabilita la Prevención de ejecución.

Si el conmutador de alternancia **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 de alternancia **Prevención de ejecución** está desactivado, no puede administrar los objetos que los usuarios ejecutan o abren en sus dispositivos.

Este conmutador de alternancia está desactivado de manera predeterminada.

Acción ante operaciones de ejecución o apertura de un objeto prohibido

Bloquear y escribir 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.

Registrar solo eventos

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.

Edición

Al hacer clic en este botón, se abre un cuadro 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 Cloud Sandbox**, puede habilitar o deshabilitar el componente Cloud Sandbox.

Cloud Sandbox

El conmutador de alternancia **Cloud Sandbox** habilita o deshabilita la tecnología Cloud Sandbox que ayuda a detectar amenazas avanzadas en un equipo. Kaspersky Endpoint Security reenvía automáticamente los archivos detectados a Cloud Sandbox para su análisis. Cloud Sandbox ejecuta estos archivos en un entorno aislado para identificar actividades maliciosas y decide sobre su reputación. Los datos de estos archivos se envían a Kaspersky Security Network. Por lo tanto, si Cloud Sandbox detecta un archivo malicioso, Kaspersky Endpoint Security realizará la acción adecuada para eliminar la amenaza en todos los equipos donde se detecte el archivo.

Si el conmutador de alternancia **Cloud Sandbox** está activado, la tecnología Cloud Sandbox está habilitada.

Si el conmutador de alternancia **Cloud Sandbox** está desactivado, la tecnología Cloud Sandbox está deshabilitada.

Este conmutador de alternancia está desactivado de manera predeterminada.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana de configuración de desbloqueo del equipo

Desbloquear automáticamente el equipo aislado en

Esta casilla habilita o deshabilita el apagado automático de Aislamiento de la red después de un tiempo especificado.

Si esta casilla está seleccionada, puede especificar el retraso para deshabilitar automáticamente el Aislamiento de la red de un equipo.

Si esta casilla está desactivada, Kaspersky Endpoint Security deshabilita el Aislamiento de la red 8 horas después de que comience el aislamiento.

Esta casilla está seleccionada por defecto.

Horas

El intervalo después del cual el Aislamiento de la red se deshabilitará automáticamente.

Este campo solo se puede editar si la casilla **Desbloquear automáticamente el equipo aislado en** está seleccionada.

La ventana Exclusiones de aislamiento de la red

Exclusiones de aislamiento de la red

Esta lista contiene las conexiones de red que agregó como exclusiones de Aislamiento de la red.

Agregar

Al hacer clic en este botón, se abre una ventana donde puede especificar manualmente la configuración de la conexión de red que se agregará como una exclusión.

Agregar del perfil

Al hacer clic en este botón, se abre una ventana en la que 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 la red.

Este botón está disponible si se selecciona una conexión en la lista de exclusiones de Aislamiento de la red.

La ventana Propiedades de la regla

Nombre de regla

Nombre de una regla de exclusión de Aislamiento de la red.

Este es un parámetro opcional.

Sentido

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 **Personalizada**.

Intervalo o puerto local

Puerto local o rango del equipo para el que se configuran las exclusiones de Aislamiento de la red.

Intervalo o puerto remoto

Puerto remoto o rango del equipo para el que se configuran las exclusiones de Aislamiento de la red.

Dirección remota

Dirección de red del equipo para el que se configuran las exclusiones de Aislamiento de la red.

Aplicaciones

Esta casilla es para agregar una aplicación a la que se le permite iniciar una conexión de red agregada a las exclusiones de Aislamiento de la red en el equipo aislado.

Si esta casilla está seleccionada, puede agregar una aplicación de este tipo.

Si esta casilla está desactivada, cualquier aplicación en el equipo aislado puede iniciar una conexión de red agregada a las exclusiones de Aislamiento de la red.

Esta casilla está desactivada por defecto.

Agregar

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 agregada a las exclusiones de Aislamiento de la red.

Edición

Al hacer clic en este botón, se abre una ventana en la que puede editar una ruta a una aplicación agregada.

Este botón está disponible si se elige una aplicación de la lista.

Eliminar

Al hacer clic en este botón, se elimina una aplicación agregada.

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 a objeto**, puede seleccionar si desea especificar la ruta completa al objeto que se prohibirá. Si selecciona especificar la ruta, ingrese su valor en el campo correspondiente.

En la sección **Suma de control del objeto**, puede seleccionar si desea especificar la suma de control del objeto que se prohibirá. Si selecciona especificar la suma de control, seleccione su tipo e ingrese el valor en el campo correspondiente.

La ventana Endpoint Detection and Response (KATA)

Endpoint Detection and Response Expert (on-premise)

El conmutador de alternancia de **Endpoint Detection and Response Expert (on-premise)** habilita o deshabilita el componente Endpoint Detection and Response Expert (on-premise) que interactúa con la solución Kaspersky Anti Targeted Attack Platform. Esta solución detecta con rapidez amenazas avanzadas, como ataques dirigidos, amenazas persistentes avanzadas, ataques de día cero y más.

Si el conmutador de alternancia de **Endpoint Detection and Response Expert (on-premise)** está activado, el componente Endpoint Detection and Response Expert (on-premise) está habilitado.

Si el conmutador de alternancia de **Endpoint Detection and Response Expert (on-premise)** está desactivado, el componente Endpoint Detection and Response Expert (on-premise) está deshabilitado.

Este conmutador de alternancia está desactivado de manera predeterminada.

Endpoint Detection and Response Expert (versión 7.1 o anteriores)

Si se selecciona esta opción, el componente Endpoint Detection and Response Expert (on-premise) funciona en modo de compatibilidad con Endpoint Detection and Response Expert (versión 7.1 o anterior).

Endpoint Detection and Response Expert (versión 8.0 o posteriores)

Si se selecciona esta opción, el componente Endpoint Detection and Response Expert (on-premise) funciona en modo de compatibilidad con Endpoint Detection and Response Expert (versión 8.0 o posterior).

Heredar configuración de conexión de la directiva

Si se selecciona esta opción, los ajustes de conexión con los servidores de recopilación de telemetría, los servidores de recopilación de telemetría, los ajustes de transmisión de datos de los servidores de recopilación de telemetría, los límites en el número de eventos enviados a los servidores de recopilación de telemetría, los ajustes de conexión con los servidores de respuesta y los servidores de respuesta se heredan de la directiva principal y dejan de estar disponibles para su edición.

Esta opción está disponible si el modo **Endpoint Detection and Response Expert (versión 8.0 o posteriores)** está seleccionado.

Esta opción está seleccionada por defecto.

Usar configuración de conexión personalizada

Si se selecciona esta opción, los ajustes de conexión con los servidores de recopilación de telemetría, los servidores de recopilación de telemetría, los ajustes de transmisión de datos de los servidores de recopilación de telemetría, los límites en el número de eventos enviados a los servidores de recopilación de telemetría, los ajustes de conexión con los servidores de respuesta y los servidores de respuesta no se heredan de la directiva principal y permanecerán disponible para su edición.

Esta opción está disponible si el modo **Endpoint Detection and Response Expert (versión 8.0 o posteriores)** está seleccionado.

Dependiendo del modo seleccionado en las secciones **Conexión con los servidores de KATA** o **Conexión con los servidores de recopilación de telemetría**, puede establecer los ajustes de conexión con los servidores.

Configuración de conexión

Al hacer clic en este vínculo, se abre un cuadro de diálogo en el que puede configurar la conexión a los servidores.

Enviar solicitud de sincronización al servidor cada (min)

El intervalo entre las solicitudes de sincronización enviadas a un servidor KATA.

El valor predeterminado es 5 minutos.

Esta opción está disponible si el modo **Endpoint Detection and Response Expert (versión 8.0 o posteriores)** está seleccionado.

Agregar

Al hacer clic en este botón, se abre una ventana en la que puede configurar una conexión a un servidor.

Edición

Al hacer clic en este botón, se abre una ventana donde puede editar una conexión existente a un servidor.

Este botón está disponible si se selecciona un servidor en la lista de servidores.

Eliminar

Al hacer clic en este botón, se elimina de la lista el servidor seleccionado.

Este botón está disponible si se selecciona un servidor de la lista.

Dirección

Dirección IP de un servidor.

Puerto

Número de puerto de un servidor.

En la sección **Configuración de la transmisión de datos**, puede establecer los ajustes para enviar datos a los servidores.

Enviar telemetría a KATA

Esta casilla habilita/deshabilita el envío de eventos al servidor KATA.

Si se selecciona esta casilla, los eventos se envían al servidor KATA.

Si esta casilla está vacía, los eventos no se envían al servidor KATA.

Esta opción está disponible si el modo **Endpoint Detection and Response Expert (versión 7.1 o anteriores)** está seleccionado.

Esta casilla está desactivada de manera predeterminada.

Enviar telemetría a los servidores de recopilación de telemetría

Esta casilla habilita/deshabilita el envío de eventos al servidor de recopilación de telemetría.

Si se selecciona esta casilla, los eventos se envían al servidor de recopilación de telemetría.

Si esta casilla está vacía, los eventos no se envían al servidor de recopilación de telemetría.

Esta casilla está disponible si el modo **Endpoint Detection and Response Expert (versión 8.0 o posteriores)** está seleccionado.

Esta casilla está desactivada de manera predeterminada.

Retraso máximo de transmisión de evento (s)

El intervalo en el que Kaspersky Endpoint Security envía eventos a un servidor.

El valor por defecto es de 30 segundos.

En la sección **Limitación de solicitudes**, puede restringir el número de eventos transmitidos.

Habilitar limitación de solicitudes

Esta casilla habilita o deshabilita la restricción de la cantidad de eventos enviados por Kaspersky Endpoint Security a un servidor KATA.

Si la casilla está seleccionada, se restringe el número de eventos que envía la aplicación.

Si la casilla no está seleccionada, el número de eventos enviados por la aplicación no está restringido.

Esta casilla está seleccionada por defecto.

Cantidad máxima de eventos por hora

La cantidad máxima 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 en particular si la proporción de eventos de ese tipo con respecto al número total de eventos excede el umbral configurado.

El valor predeterminado es 15 %.

En la sección **Conexión con los servidores de respuesta**, puede configurar la conexión a los servidores de respuesta.

Configuración de conexión

Al hacer clic en este vínculo, se abre un cuadro de diálogo en el que puede configurar la conexión a los servidores.

Enviar solicitud de sincronización al servidor cada (min)

El intervalo entre las solicitudes de sincronización enviadas a un servidor KATA.

El valor predeterminado es 5 minutos.

Esta opción está disponible si el modo **Endpoint Detection and Response Expert (versión 8.0 o posteriores)** está seleccionado.

Agregar

Al hacer clic en este botón, se abre una ventana en la que puede configurar una conexión a un servidor.

Edición

Al hacer clic en este botón, se abre una ventana donde puede editar una conexión existente a un servidor.

Este botón está disponible si se selecciona un servidor en la lista de servidores.

Eliminar

Al hacer clic en este botón, se elimina de la lista el servidor seleccionado.

Este botón está disponible si se selecciona un servidor de la lista.

Dirección

Dirección IP de un servidor.

Puerto

Número de puerto de un servidor.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Servidor KATA

Dirección

Dirección IP de un servidor KATA.

Puerto

Número de puerto de un servidor KATA.

El valor por defecto es 443.

La ventana Configuración de la conexión del servidor

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 por defecto es de 10 segundos.

En la sección **Certificado TLS del servidor**, puede agregar o eliminar un certificado TLS y ver información sobre el certificado que agregó.

Agregar certificado TLS

Al hacer clic en este botón, se abre una ventana en la que puede seleccionar un certificado 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 TLS actual.

Este botón está disponible si se agregó un certificado TLS.

En la sección **Seguridad adicional de la conexión**, puede configurar la protección mejorada para la conexión entre Kaspersky Endpoint Security y un servidor KATA.

Usar autenticación bidireccional

Esta casilla habilita o deshabilita 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 la casilla está seleccionada, Kaspersky Endpoint Security usa la verificación bidireccional para conectarse a un servidor KATA.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no usa la verificación bidireccional para conectarse a un servidor KATA.

Esta casilla está desactivada por defecto.

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 con contraseña. No es posible agregar un contenedor de cifrado sin una contraseña.

Contraseña de criptocontenedor

La contraseña del contenedor de cifrado utilizado para la verificación bidireccional.

La sección “Actualización”

Actualizar módulos de la aplicación

Esta casilla habilita o deshabilita la actualización de los módulos de la aplicación. Las bases de datos de la aplicación siempre se actualizan.

Si la casilla está seleccionada, Kaspersky Endpoint Security actualiza los módulos de la aplicación.

Si esta casilla no está seleccionada, Kaspersky Endpoint Security no actualiza los módulos de la aplicación.

Esta casilla está seleccionada por defecto.

Orígenes de actualizaciones

Esta lista contiene las direcciones de los recursos desde los cuales Kaspersky Endpoint Security descarga e instala las actualizaciones de las bases de datos y los módulos de la aplicación. Puede especificar una carpeta local o de red, o un servidor FTP o HTTP como origen de actualizaciones.

Por defecto, la lista de orígenes de actualizaciones contiene servidores de actualizaciones 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 manera predeterminada.

Si administra Kaspersky Endpoint Security a través de Kaspersky Security Center Cloud Console, la lista de orígenes de actualizaciones también incluye puntos de distribución de manera predeterminada. Para obtener información detallada sobre los puntos de distribución, consulte la Ayuda de Kaspersky Security Center.

No puede eliminar los orígenes de actualizaciones predeterminados de la lista.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede especificar la ruta a una carpeta local o de red, o una dirección web que se agregará 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 la casilla de verificación junto al origen de actualizaciones está seleccionada.

Origen de actualizaciones

Esta columna contiene orígenes de actualizaciones para Kaspersky Endpoint Security.

Estado

Si el conmutador de alternancia en esta columna está activado, Kaspersky Endpoint Security utiliza el origen de actualizaciones correspondiente de la columna **Origen de actualizaciones** para recibir actualizaciones.

Si el conmutador de alternancia en esta columna está desactivado, Kaspersky Endpoint Security no utiliza el origen de actualizaciones correspondiente de la columna **Origen de actualizaciones** para recibir actualizaciones.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo "Agregar origen de actualizaciones"

Campo de entrada Introduzca una ruta a una carpeta local o de red, o una dirección web

Dirección del recurso desde el cual Kaspersky Endpoint Security copia las actualizaciones.

Puede especificar una ruta a una carpeta local o de red, o la dirección web o la dirección IP de un servidor FTP o HTTP como la dirección del recurso.

Puede especificar la dirección web de un servidor FTP en el formato siguiente: ftp://<nombre de usuario>:<contraseña>@<host>:<puerto>.

En la sección **Estado**, puede definir si Kaspersky Endpoint Security utiliza la dirección web especificada como origen de actualizaciones.

Deshabilitado

La dirección web se agrega a la lista de orígenes de actualizaciones, pero Kaspersky Endpoint Security no utiliza esta dirección web como origen de actualizaciones.

Habilitado

La dirección web se agrega a la lista de orígenes de actualizaciones y Kaspersky Endpoint Security utiliza esta dirección web como origen de actualizaciones.

La sección “Cifrado de datos”

Cifrado de disco FileVault

El conmutador de alternancia **Cifrado de disco FileVault** habilita o deshabilita la administración del cifrado de disco FileVault.

Si el conmutador de alternancia **Cifrado de disco FileVault** está activado, el cifrado de disco FileVault se puede aplicar a los equipos cliente desde Kaspersky Security Center.

Si el conmutador de alternancia **Cifrado de disco FileVault** está desactivado, el cifrado de disco FileVault no se puede aplicar a los equipos cliente desde Kaspersky Security Center.

Este conmutador de alternancia está desactivado de manera predeterminada.

Nota: Si el conmutador de alternancia **Cifrado de disco FileVault** está desactivado, los usuarios con derechos de administrador pueden cifrar y descifrar sus discos de inicio de su Mac desde Configuración 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 que 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 de alternancia **Cifrado de disco FileVault** está activado y la opción **Cifrar disco** está seleccionada, los usuarios con derechos de administrador no pueden descifrar el disco de inicio de su Mac desde Configuración del sistema.

Descifrar disco

Kaspersky Endpoint Security muestra una solicitud de credenciales de cuenta de equipo en los equipos cliente a los que 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 de alternancia **Cifrado de disco FileVault** está activado y la opción **Descifrar disco** está seleccionada, los usuarios con derechos de administrador no pueden cifrar el disco de inicio de su Mac desde Configuración del sistema.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Ajustes de telemetría

Agregar

Si hace clic en este botón, se abre una ventana donde puede agregar una regla a la Zona de confianza.

Edición

Al hacer clic en este botón, se abre una ventana en la que puede editar la regla seleccionada.

Eliminar

Al hacer clic en este botón, se elimina de la Zona de confianza la regla seleccionada.

Estado

El conmutador de alternancia en esta columna deshabilita/habilita la regla agregada a la Zona de confianza.

Si el conmutador está habilitado, la regla está activa.

Si el conmutador está deshabilitado, la regla está inactiva.

Nombre de regla

Esta columna contiene los nombres de las reglas agregadas a la Zona de confianza.

Descripción

Un comentario con información sobre la regla agregada a la Zona de confianza.

La ventana Agregar/editar regla de exclusión

Estado

Este conmutador de alternancia habilita/deshabilita la regla agregada a la Zona de confianza.

Si el conmutador está habilitado, la regla está activa.

Si el conmutador está deshabilitado, la regla está inactiva.

Nombre de regla

Nombre de la regla agregada a la Zona de confianza.

Descripción

Un comentario con información sobre la regla agregada a la Zona de confianza.

Indicadores de ataque (IOA)

Campo para ingresar los GUID de los indicadores de ataque.

La sección Configuración adicional

Protección

Al hacer clic en este vínculo, se abre la ventana **Protección**, donde puede administrar la configuración general de Kaspersky Endpoint Security instalado en los equipos de los usuarios y seleccionar los tipos de objetos que Kaspersky Endpoint Security detectará.

Informes y depósito de copias de seguridad

Al hacer clic en este vínculo, se abre la ventana **Informes y depósito de copias de seguridad**, donde puede administrar la configuración de informes y copias de seguridad.

Interacción con el usuario

Al hacer clic en este vínculo, se abre la ventana **Interacción con el usuario**, donde puede configurar las notificaciones que muestra Kaspersky Endpoint Security, el idioma de visualización de los eventos que se muestran en Kaspersky Security Center y configuraciones adicionales de Kaspersky Endpoint Security.

Red

Al hacer clic en este vínculo, se abre la ventana **Red**, donde puede administrar la configuración del servidor proxy, habilitar o deshabilitar el análisis de conexiones cifradas (HTTPS), seleccionar el almacenamiento de certificados para verificar el tráfico HTTPS cifrado en el navegador Mozilla Firefox y configurar los puertos supervisados.

Zona de confianza

Al hacer clic en este vínculo, se abre la ventana **Zona de confianza**, donde puede agregar exclusiones para la Protección contra amenazas de archivo o tareas de análisis y configurar aplicaciones de confianza.

La ventana Protección

En la sección **General**, puede habilitar o deshabilitar la protección de archivos en un equipo remoto y configurar el inicio automático de la aplicación cuando se enciende el equipo o se reinicia el sistema operativo.

Iniciar la aplicación con el inicio del equipo

Esta casilla habilita o deshabilita el inicio automático de Kaspersky Endpoint Security cuando se enciende un equipo remoto o después de reiniciar su sistema operativo.

Si la casilla está seleccionada, Kaspersky Endpoint Security se inicia automáticamente cuando se enciende el equipo remoto o se reinicia su sistema operativo.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no se inicia automáticamente cuando se enciende el equipo remoto o se reinicia su sistema operativo.

Esta casilla está seleccionada por defecto.

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.

Habilitar protección

Esta casilla habilita o deshabilita la protección de un equipo remoto con Kaspersky Endpoint Security instalado.

Si la casilla está seleccionada, se habilita la protección del equipo remoto.

Si la casilla no está seleccionada, se deshabilita la protección del equipo remoto.

Esta casilla está seleccionada por defecto.

En la sección **Tipos de objetos a detectar**, puede seleccionar los tipos de objetos que Kaspersky Endpoint Security detectará.

Virus, gusanos, programas troyanos, utilidades maliciosas, adware y marcadores automáticos

Esta casilla habilita o deshabilita la detección de los siguientes tipos de programas:

- Todos los tipos de malware.
- Aplicaciones que muestran publicidades (por ejemplo, anuncios) en el equipo o remplazan los resultados de búsqueda del navegador con sitios web de publicidad.
- Aplicaciones que subrepticiamente establecen conexiones telefónicas a través del módem de un equipo.

La casilla está seleccionada de forma predeterminada y no se puede desmarcar.

Software legítimo que intrusos pueden utilizar para dañar el equipo del usuario o los datos personales

Esta casilla habilita o deshabilita la detección de aplicaciones que no son maliciosas ni peligrosas, pero que en ciertas circunstancias pueden usarse para hacer daño al equipo de un usuario.

Si la casilla está seleccionada, Kaspersky Endpoint Security detecta software legítimo que los intrusos pueden utilizar para dañar el equipo o los datos personales de un usuario.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no detecta software legítimo que los intrusos pueden utilizar para dañar el equipo o los datos personales de un usuario.

Esta casilla está desactivada por defecto.

La sección **Avanzado** le permite habilitar el modo de ahorro de energía.

Omitir las tareas programadas cuando el equipo está funcionando con batería

Esta casilla habilita o deshabilita el inicio de tareas de análisis programado en equipos que funcionan con batería.

Si la casilla está seleccionada, Kaspersky Endpoint Security no inicia las tareas de análisis programado en los equipos que funcionan con batería.

Si la casilla no está seleccionada, Kaspersky Endpoint Security inicia las tareas de análisis programado en los equipos que funcionan con batería.

Esta casilla está seleccionada por defecto.

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 de datos correspondiente.

Habilitar esta opción puede afectar negativamente al rendimiento de Kaspersky Endpoint Security.

Por defecto, esta opción está desactivada.

Límite máximo (en porcentajes)

Valor máximo permitido de uso de CPU por 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.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Informes y depósito de copias de seguridad

En la sección **Informes**, puede configurar los ajustes para generar y almacenar informes sobre eventos que ocurren mientras Kaspersky Endpoint Security se está ejecutando.

Eliminar los informes después de días

Esta casilla habilita o deshabilita la eliminación de informes después del período especificado.

Si la casilla está seleccionada, Kaspersky Endpoint Security elimina los informes después del período especificado. De forma predeterminada, Kaspersky Endpoint Security almacena los informes durante 30 días.

Si la casilla no está seleccionada, Kaspersky Endpoint Security almacena los informes de forma indefinida.

Esta casilla está seleccionada por defecto.

Registrar eventos que no sean críticos

Esta casilla habilita o deshabilita el registro de eventos no críticos (como los eventos informativos) en el informe. Los eventos no críticos no afectan la seguridad.

Si la casilla está seleccionada, Kaspersky Endpoint Security registra eventos informativos en el informe.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no registra eventos informativos en el informe.

Esta casilla está desactivada por defecto.

Conservar solo los eventos recientes

Esta casilla habilita o deshabilita conservar solo información sobre eventos importantes de la ejecución anterior de la tarea.

Si la casilla está seleccionada, cada vez que se inicia una tarea, Kaspersky Endpoint Security elimina la información sobre eventos no críticos de la ejecución anterior de la tarea, pero conserva información importante (por ejemplo, sobre el malware detectado) en el informe.

Si la casilla no está seleccionada, Kaspersky Endpoint Security conserva toda la información de la ejecución anterior de la tarea.

Esta casilla está desactivada por defecto.

En la sección **Depósito de copias de seguridad**, puede especificar cuánto tiempo se pueden almacenar los objetos en el depósito de copias de seguridad.

Eliminar los objetos después de días

Esta casilla habilita o deshabilita la eliminación de objetos del depósito de copias de seguridad después del período especificado.

Si la casilla está seleccionada, Kaspersky Endpoint Security elimina los objetos del depósito de copias de seguridad después del período especificado. El período de almacenamiento predeterminado es de 30 días.

Si la casilla no está seleccionada, Kaspersky Endpoint Security almacena los objetos en el depósito de copias de seguridad de forma indefinida.

Esta casilla está seleccionada por defecto.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Interacción con el usuario

En la sección **Interfaz de la aplicación**, puede configurar si el ícono de la aplicación se muestra en la barra de menús en un equipo remoto, y si un usuario puede abrir la ventana principal de Kaspersky Endpoint Security y utilizar la interfaz de la aplicación.

Mostrar ícono de la aplicación en la barra de menús

Esta casilla habilita o deshabilita la visualización del ícono de la aplicación en la barra de menús de un equipo remoto.

Si la casilla está seleccionada, el ícono de la aplicación se muestra en la barra de menús.

Si la casilla no está seleccionada, el ícono de la aplicación no se muestra en la barra de menús.

Esta casilla está seleccionada por defecto.

Permitir que el usuario abra la aplicación

Esta casilla habilita o deshabilita la capacidad del usuario de abrir la ventana principal de Kaspersky Endpoint Security y utilizar la interfaz de la aplicación en un equipo remoto.

Si la casilla está seleccionada, el usuario puede abrir la ventana principal de Kaspersky Endpoint Security y utilizar la interfaz de la aplicación en un equipo remoto.

Si la casilla no está seleccionada, Kaspersky Endpoint Security evita que el usuario abra la ventana principal de la aplicación y oculta la interfaz de la aplicación en un equipo remoto.

Esta casilla está seleccionada por defecto.

En la sección **Notificaciones**, puede habilitar las notificaciones sobre eventos de Kaspersky Endpoint Security y elegir el tipo de notificación preferido.

Notificaciones

El conmutador de alternancia **Notificaciones** habilita o deshabilita las notificaciones sobre los eventos de Kaspersky Endpoint Security.

Si el conmutador de alternancia **Notificaciones** está activado, Kaspersky Endpoint Security muestra notificaciones sobre eventos que ocurren mientras se ejecutan los componentes de Kaspersky Endpoint Security.

Si el conmutador de alternancia **Notificaciones** está desactivado, Kaspersky Endpoint Security no muestra notificaciones sobre eventos que ocurren mientras se ejecutan los componentes de Kaspersky Endpoint Security.

Este conmutador de alternancia está activado de forma predeterminada.

Notificaciones del usuario

Al hacer clic en este vínculo, se abre una ventana donde puede seleccionar los tipos de notificaciones que se utilizarán para todos los tipos de eventos.

En la sección **Permitir que el usuario salga de la aplicación**, puede configurar si un usuario puede cerrar Kaspersky Endpoint Security en un equipo remoto.

Mostrar Salir en el menú contextual del ícono de la aplicación

Esta casilla habilita o deshabilita la disponibilidad del elemento **Salir** en el menú contextual del ícono de la aplicación que se muestra en la barra de menús.

Si la casilla está seleccionada, el elemento **Salir** se muestra en el menú contextual del ícono de la aplicación. El usuario de un equipo remoto puede salir de Kaspersky Endpoint Security en el equipo.

Si la casilla no está seleccionada, el elemento **Salir** no está disponible en el menú contextual del ícono de la aplicación. El usuario de un equipo remoto no puede salir de Kaspersky Endpoint Security en el equipo.

Esta casilla está seleccionada por defecto.

En la sección **Eventos en Kaspersky Security Center**, puede seleccionar el idioma de visualización para los eventos de Kaspersky Endpoint Security en la aplicación.

Idioma de visualización

En esta lista desplegable, puede seleccionar el idioma de visualización para los eventos de Kaspersky Endpoint Security en la aplicación.

En la sección **Restricciones**, puede permitir la administración 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 habilita o deshabilita la administración local de las actualizaciones de Kaspersky Endpoint Security en un equipo remoto.

Si la casilla está seleccionada, se habilita la administración local de las actualizaciones de Kaspersky Endpoint Security en un equipo remoto.

Si la casilla no está seleccionada, las actualizaciones de Kaspersky Endpoint Security en un equipo remoto solo se pueden administrar mediante el complemento de administración de Kaspersky Endpoint Security en Kaspersky Security Center.

Esta casilla está seleccionada por defecto.

Permitir que el usuario administre las claves de forma local

Esta casilla habilita o deshabilita la administración local de las claves de Kaspersky Endpoint Security en un equipo remoto.

Si la casilla está seleccionada, se habilita la administración local de las claves de Kaspersky Endpoint Security en un equipo remoto.

Si la casilla no está seleccionada, las claves de Kaspersky Endpoint Security en un equipo remoto solo se pueden administrar mediante el complemento de administración de Kaspersky Endpoint Security en Kaspersky Security Center.

Esta casilla está seleccionada por defecto.

En la sección **rotección con contraseña**, puede establecer y configurar la contraseña para limitar las acciones no deseadas en los dispositivos del usuario.

rotección con contraseña

El conmutador de **rotección con contraseña** habilita o deshabilita la protección con contraseña de acciones no deseadas en los dispositivos de los usuarios.

Si el conmutador de **rotección con contraseña** está activado, puede establecer y configurar una contraseña para limitar las acciones de usuario en sus dispositivos.

Si el conmutador de **rotección con contraseña** está desactivado, un usuario puede realizar una acción no deseada sin ingresar una contraseña.

Este conmutador de alternancia está desactivado de manera predeterminada.

Si activa este conmutador, 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.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Notificaciones del usuario

Eventos

Esta columna enumera los eventos que pueden ocurrir mientras se ejecuta Kaspersky Endpoint Security:

- **Eventos críticos**. Eventos de crucial importancia en términos de seguridad.
- **Falla funcional**. Eventos que hacen que el sistema falle.
- **Eventos importantes**. Eventos a los que el usuario debe prestar atención.
- **Eventos informativos**. Eventos de naturaleza informativa.

Notificaciones

Una notificación es un mensaje emergente que notifica al usuario sobre un evento.

La casilla en la columna **Notificaciones** habilita o deshabilita las notificaciones emergentes acerca de eventos de una categoría en particular.

Sonido

Un sonido de notificación asociado a un evento.

La casilla en la columna **Sonido** habilita o deshabilita las notificaciones de sonido para eventos de una categoría en particular.

La ventana “Zona de confianza”: la sección “Archivos y carpetas”

Agregar

Si hace 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 elimina el archivo o carpeta seleccionado de la lista de exclusiones.

Este botón está disponible si la casilla de verificación junto al archivo o carpeta está seleccionada.

Archivo o carpeta

Esta columna contiene archivos o carpetas agregados a la Zona de confianza.

Estado

El conmutador de alternancia de esta columna deshabilita o habilita el análisis de la carpeta o del archivo agregados a la Zona de confianza.

Si el conmutador de alternancia está activado, Kaspersky Endpoint Security no analiza el archivo o carpeta correspondiente.

Si el conmutador de alternancia está desactivado, Kaspersky Endpoint Security analiza el archivo o carpeta correspondiente.

Comentario

Información sobre el archivo o la carpeta agregados a la Zona de confianza.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar exclusión”

Ingrese un nombre de archivo, nombre de carpeta o campo de entrada de máscara

Ruta a un archivo o carpeta, o una máscara de archivo o carpeta que se excluirá del alcance de la protección.

Incluir subcarpetas

Esta casilla habilita o deshabilita el análisis de las subcarpetas de la carpeta especificada en el campo **Introduzca un nombre de archivo, de carpeta o máscara**.

Si la casilla está seleccionada, Kaspersky Endpoint Security no analiza las subcarpetas de la carpeta especificada durante los análisis de malware.

Si la casilla no está seleccionada, Kaspersky Endpoint Security solo excluye los archivos que se encuentran directamente en la carpeta especificada en **Introduzca un nombre de archivo, de carpeta o máscara** durante los análisis de malware. Se analizan las subcarpetas de la carpeta especificada.

Esta casilla está seleccionada por defecto.

En la sección **Componentes**, puede seleccionar componentes que no analizarán el archivo o la carpeta especificados.

Cualquiera

Ni el componente Analizar ni el componente Protección contra archivos peligrosos analizarán el archivo o la carpeta especificados.

Desde lista

Esta opción le permite seleccionar componentes.

Protección contra amenazas de archivo

Si esta casilla de verificación está seleccionada, el componente de Protección contra archivos peligrosos no analizará el archivo o la carpeta especificados.

La casilla está disponible si la opción **Desde lista** está seleccionada.

Análisis

Si esta casilla de verificación está seleccionada, el componente Analizar no analizará el archivo o carpeta especificado.

La casilla está disponible si la opción **Desde lista** está seleccionada.

Campo de entrada Comentario

Información sobre el archivo o la carpeta agregados a la Zona de confianza.

En la sección **Estado**, puede seleccionar si la exclusión está activa o no.

Deshabilitado

Kaspersky Endpoint Security analiza el archivo o la carpeta correspondiente.

Habilitado

Kaspersky Endpoint Security no analiza el archivo o la carpeta correspondiente.

La ventana “Zona de confianza”: la sección “Aplicaciones de confianza”

Lista de aplicaciones de confianza

Una lista de aplicaciones de confianza cuya actividad de red no se supervisará a través de Kaspersky Endpoint Security.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede introducir una ruta a la aplicación cuya actividad de red no se supervisará a través de Kaspersky Endpoint Security.

Eliminar

Al hacer clic en este botón, se elimina de la lista la aplicación de confianza seleccionada.

Este botón está disponible si la casilla de verificación junto a la aplicación de confianza está seleccionada.

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 de alternancia que indica el estado de la supervisión de la actividad de red de la aplicación.

Si el estado es **Habilitado**, Kaspersky Endpoint Security no supervisa la actividad de red de la aplicación correspondiente.

Si el estado es **Deshabilitado**, 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 se agrega manualmente.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

El cuadro de diálogo “Agregar aplicación”

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 habilita o deshabilita la supervisión de las operaciones con archivos de una aplicación en un equipo cliente.

Si la casilla está seleccionada, Kaspersky Endpoint Security no supervisa la actividad de archivos de la aplicación.

Si la casilla no está seleccionada, Kaspersky Endpoint Security supervisa la actividad de archivos de la aplicación.

Esta casilla está seleccionada por defecto.

No supervisar la actividad de red

Esta casilla habilita o deshabilita la supervisión del tráfico de Internet entrante y saliente en un equipo cliente.

Si la casilla está seleccionada, Kaspersky Endpoint Security no supervisa la actividad de red de la aplicación.

Si la casilla no está seleccionada, Kaspersky Endpoint Security supervisa la actividad de red de la aplicación.

Esta casilla está seleccionada por defecto.

La ventana Red

En la sección **Configuración de servidor proxy**, puede configurar el uso de un servidor proxy y las opciones que se utilizarán en la conexión a un servidor proxy.

No usar un servidor proxy

Si se selecciona esta opción, Kaspersky Endpoint Security no utiliza un servidor proxy para conectarse a los orígenes de actualizaciones para las bases de datos y los módulos de la aplicación.

Usar la configuración de servidor proxy del sistema

Si se selecciona esta opción, Kaspersky Endpoint Security se conecta a los orígenes de actualizaciones de las bases de datos y los módulos de la aplicación con la configuración de servidor proxy establecida en su sistema operativo.

Esta opción está seleccionada por defecto.

Usar la configuración de servidor proxy especificada

Si se selecciona esta opción, Kaspersky Endpoint Security se conecta a los orígenes de actualizaciones de las bases de datos y los módulos de la aplicación con la configuración de servidor proxy que haya especificado.

Dirección

Dirección IP o nombre simbólico de un servidor proxy.

Este campo está disponible si la opción **Usar la configuración de servidor proxy especificada** está seleccionada.

Puerto

Número de puerto del servidor proxy.

El número de puerto predeterminado es 8080.

Este campo está disponible si la opción **Usar la configuración de servidor proxy especificada** está seleccionada.

Usar autenticación

Esta casilla habilita o deshabilita el uso de la autenticación al conectarse a un servidor proxy.

Si la casilla está seleccionada, Kaspersky Endpoint Security requiere las credenciales del usuario para conectarse a un servidor proxy.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no requiere las credenciales del usuario para conectarse a un servidor proxy.

Esta casilla está seleccionada por defecto.

Esta casilla está disponible si la opción **Usar la configuración de servidor proxy especificada** está seleccionada.

Nombre de usuario

Nombre de usuario para conectarse al servidor proxy.

Este campo está disponible si la opción **Usar la configuración de servidor proxy especificada** y la casilla **Usar autenticación** están seleccionadas.

Contraseña

Contraseña para el nombre de usuario especificado.

Este campo está disponible si la opción **Usar la configuración de servidor proxy especificada** y la casilla **Usar autenticación** están seleccionadas.

Mostrar

Al hacer clic en este botón, se muestran los caracteres de la contraseña que ingresó en el campo **Contraseña**.

Omitir el servidor proxy para las direcciones locales

Esta casilla habilita o deshabilita el uso de un servidor proxy al actualizar las bases de datos y los módulos de la aplicación desde una carpeta local o de red.

Si la casilla está seleccionada, Kaspersky Endpoint Security no utiliza un servidor proxy al actualizar las bases de datos y los módulos de la aplicación desde una carpeta local o de red.

Si la casilla no está seleccionada, Kaspersky Endpoint Security utiliza un servidor proxy al actualizar las bases de datos y los módulos de la aplicación desde una carpeta local o de red.

Esta casilla está seleccionada por defecto.

Esta casilla está disponible si la opción **Usar la configuración de servidor proxy especificada** está seleccionada.

En la sección **Verificar conexiones seguras**, puede definir si Kaspersky Endpoint Security analiza las conexiones seguras (HTTPS).

Verificación de conexiones seguras (HTTPS)

El conmutador de alternancia **Verificación de conexiones seguras (HTTPS)** habilita o deshabilita el análisis de conexiones seguras establecidas a través del protocolo HTTPS y la visualización de notificaciones cuando el Control Web bloquea el acceso del usuario a recursos web peligrosos.

Si el conmutador de alternancia **Verificación de conexiones seguras (HTTPS)** está activado, Kaspersky Endpoint Security hace lo siguiente:

- La Protección contra amenazas web analiza la información que el equipo envía y recibe a través del protocolo HTTPS en Safari, Google Chrome y Firefox.
- La aplicación muestra notificaciones cuando el usuario accede a recursos web bloqueados por el Control Web en el equipo remoto.

Si el conmutador de alternancia **Verificación de conexiones seguras (HTTPS)** está desactivado, Kaspersky Endpoint Security hace lo siguiente:

- La Protección contra amenazas web no analiza los datos que el equipo envía y recibe a través del protocolo HTTPS.
- La aplicación no muestra notificaciones cuando el usuario accede a recursos web bloqueados por el Control Web en el equipo remoto.

Este conmutador de alternancia está activado de forma predeterminada.

En la sección **Seleccionar 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 por defecto.

Configuración de la tienda de certificados del navegador Mozilla Firefox

Si se selecciona esta opción, Kaspersky Endpoint Security usa el certificado del almacén de certificados del navegador.

En este caso, debe agregar manualmente el certificado de Kaspersky Endpoint Security al almacén de certificados del navegador Mozilla Firefox. Para obtener más información, consulte Cómo agregar el certificado de Kaspersky 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 emitir notificación.

En la sección **Puertos supervisados**, puede configurar qué puertos supervisa Kaspersky Endpoint Security.

Puertos seleccionados

Al hacer clic en este vínculo, se abre una ventana donde puede configurar una lista de puertos que Kaspersky Endpoint Security supervisa.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana “Administrar certificados raíz de confianza”

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede agregar los certificados que se considerarán de confianza.

Eliminar

Al hacer clic en este botón, se elimina de la lista el certificado seleccionado.

Lista de certificados de confianza

La columna muestra los nombres de los certificados raíz de confianza.

La lista está vacía de manera predeterminada.

Imponer

Cuando el conmutador de alternancia **Imponer** está activado, Kaspersky Endpoint Security prohíbe cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

Cuando el conmutador de alternancia **Imponer** está desactivado, Kaspersky Endpoint Security permite cambiar los valores de la configuración de tareas, la configuración de la aplicación, las directivas de subgrupos y los servidores de administración secundarios en un equipo local.

La ventana Puertos supervisados

Lista de puertos supervisados

Una lista de puertos para los cuales puede configurar la supervisión de datos transmitidos.

De forma predeterminada, la lista de puertos contiene puertos que los servicios más comunes utilizan con frecuencia.

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo donde puede agregar un puerto que desee supervisar a través de Kaspersky Endpoint Security.

Eliminar

Al hacer clic en este botón, se elimina de la lista el puerto seleccionado.

Este botón está disponible si la casilla de verificación junto al puerto está seleccionada.

Puerto

Esta columna contiene los números de puertos.

Estado

Esta columna contiene un conmutador de alternancia que indica el estado de supervisión de los datos transmitidos a través del puerto.

Si el estado es **Supervisado**, Kaspersky Endpoint Security analiza el tráfico transmitido a través del puerto correspondiente.

Si el estado es **No supervisado**, Kaspersky Endpoint Security no analiza el tráfico transmitido a través del puerto correspondiente.

Descripción

Esta columna contiene una descripción del puerto.

El cuadro de diálogo “Agregar puerto”

Campo de entrada Puerto

El número del puerto para el cual desea que Kaspersky Endpoint Security analice los datos transmitidos.

Campo de entrada Descripción

Información adicional sobre el puerto, por ejemplo, el tipo de puerto.

La ventana “Información de licencia”

En la ventana **Información de licencia**, puede ver información sobre una licencia, incluida su fecha de caducidad, la cantidad de equipos en los que puede usar Kaspersky Endpoint Security con esta licencia y el tipo de licencia.

Agregar como clave de reserva

Esta casilla habilita o deshabilita la adición de un archivo de claves o código de activación específico como clave de reserva.

Si la casilla está seleccionada, Kaspersky Endpoint Security agrega el archivo de claves o el código de activación especificado como clave de reserva.

Si la casilla no está seleccionada, Kaspersky Endpoint Security agrega el archivo de claves o el código de activación especificado como la clave activa.

Esta casilla está desactivada por defecto.

La ventana “Análisis”

Alcance del análisis

Al hacer clic en este vínculo, se abre una ventana en la que puede crear el alcance del análisis.

En la sección **Si se detecta un objeto malicioso**, puede seleccionar la acción que realiza Kaspersky Endpoint Security al detectar un objeto infectado.

Solicitar al usuario que realice una acción después del análisis

Kaspersky Endpoint Security no procesa objetos hasta que se completa el análisis. En ese momento, Kaspersky Endpoint Security muestra una notificación con información sobre cada objeto infectado y le pide al usuario que seleccione qué acción tomar. Las opciones disponibles dependen del tipo de objeto.

Esta opción está seleccionada por defecto.

Solicitar al usuario que realice una acción de inmediato

Kaspersky Endpoint Security muestra una notificación con información sobre cada objeto infectado que la aplicación detecta y solicita al usuario que seleccione una acción. Las opciones disponibles dependen del tipo de objeto.

No solicitar una acción

Kaspersky Endpoint Security registra información sobre los objetos detectados en el informe sin procesarlos.

Desinfectar automáticamente

Esta casilla habilita o deshabilita la desinfección de objetos infectados que Kaspersky Endpoint Security detecta sin solicitar confirmación al usuario.

Si la casilla está seleccionada, Kaspersky Endpoint Security desinfecta automáticamente los objetos infectados.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los objetos infectados.

Esta casilla está disponible si se selecciona la opción **No solicitar una acción**.

Esta casilla está seleccionada por defecto.

Desinfectar, eliminar si la desinfección falla

Esta casilla habilita o deshabilita la eliminación de objetos infectados o probablemente infectados después de que falla un intento de desinfectarlos.

Si la casilla está seleccionada, Kaspersky Endpoint Security elimina automáticamente los objetos infectados que no pudieron desinfectarse.

Si la casilla no está seleccionada, Kaspersky Endpoint Security no elimina los objetos infectados que no pudieron desinfectarse.

Esta casilla se muestra si la opción **No solicitar una acción** está seleccionada y la casilla **Desinfectar automáticamente** está seleccionada.

Esta casilla está seleccionada por defecto.

En la sección **Tipos de archivo**, puede seleccionar el formato de los archivos que Kaspersky Endpoint Security analizará.

Analizar todos los archivos

Kaspersky Endpoint Security analiza todos los objetos del sistema de archivos que se ejecutan, abren o guardan.

Analizar las aplicaciones y los documentos por contenido

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados en función del formato del archivo.

Kaspersky define la lista de formatos de archivo, la cual forma parte de las bases de datos de Kaspersky Endpoint Security.

Analizar las aplicaciones y los documentos por extensión

Kaspersky Endpoint Security analiza solo los objetos que pueden estar infectados en función de la extensión del archivo.

Kaspersky define la lista de extensiones de archivo, la cual 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 los archivos nuevos y modificados

Esta casilla habilita o deshabilita el análisis de solo los archivos que Kaspersky Endpoint Security reconoce como nuevos o modificados desde el último análisis.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza solo los archivos que reconoce como nuevos o modificados desde el último análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza todos los archivos.

Omitir análisis de volumen del sistema de solo lectura

La casilla habilita o deshabilita el análisis del volumen de sistema de solo lectura de Kaspersky Endpoint Security.

Si la casilla está seleccionada, Kaspersky Endpoint Security no analiza el volumen de sistema de solo lectura. Esto reduce significativamente el tiempo de análisis.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza el volumen de sistema de solo lectura.

Esta casilla está seleccionada por defecto.

Saltear los archivos de más de MB

Esta casilla habilita o deshabilita la exclusión del análisis de los archivos mayores que el tamaño especificado.

Si la casilla está seleccionada, Kaspersky Endpoint Security omite los archivos mayores que el tamaño especificado.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza los archivos sin importar su tamaño.

Esta casilla está desactivada por defecto.

De forma predeterminada, el tamaño es 100 MB.

Saltear si el análisis toma más de s

Esta casilla habilita o deshabilita el límite de duración de los análisis de archivos. Kaspersky Endpoint Security omite un archivo si su análisis excede el límite de tiempo especificado.

Si la casilla está seleccionada, Kaspersky Endpoint Security omite un archivo si su análisis excede el límite de tiempo especificado.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza los archivos sin importar cuánto tiempo pueda tomar el análisis.

El valor por defecto es de 30 segundos.

En la sección **Archivos compuestos**, puede seleccionar los tipos de archivos compuestos que analiza Kaspersky Endpoint Security.

Analizar archivos comprimidos

Esta casilla habilita o deshabilita el análisis de los archivos comprimidos.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los archivos comprimidos.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los archivos comprimidos durante el análisis.

Todos

Kaspersky Endpoint Security analiza todos los archivos.

Esta opción está disponible si la casilla **Analizar archivos comprimidos** está seleccionada.

Solo los nuevos

Kaspersky Endpoint Security analiza solo los archivos nuevos.

Esta opción está disponible si la casilla **Analizar archivos comprimidos** está seleccionada.

Analizar los archivos comprimidos protegidos con contraseña

Esta casilla habilita o deshabilita el análisis de archivos comprimidos protegidos con contraseña.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los archivos comprimidos protegidos con contraseña.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los archivos comprimidos protegidos con contraseña durante el análisis.

Analizar objetos OLE incrustados

Esta casilla habilita o deshabilita el análisis de objetos incrustados en archivos, como hojas de cálculo Excel, macros o archivos adjuntos de correo electrónico.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los objetos OLE incrustados.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los objetos OLE incrustados durante el análisis.

Todos

Kaspersky Endpoint Security analiza todos los objetos OLE.

Esta opción está disponible si la casilla **Analizar objetos OLE incrustados** está seleccionada.

Solo los nuevos

Kaspersky Endpoint Security analiza solo objetos OLE incrustados nuevos.

Esta opción está disponible si la casilla **Analizar objetos OLE incrustados** está seleccionada.

Analizar los archivos de formato de correo electrónico

Use esta casilla para habilitar/deshabilitar el análisis de archivos en formatos de correo electrónico y bases de datos de correo electrónico.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza los archivos en formatos de correo electrónico y bases de datos de correo electrónico.

Si la casilla no está seleccionada, Kaspersky Endpoint Security omite los archivos en formatos de correo electrónico y bases de datos de correo electrónico durante los análisis.

Ventana Alcance del análisis

Agregar

Al hacer clic en este botón, se abre un cuadro de diálogo en el que puede especificar un archivo, una carpeta o una máscara de archivo/carpeta para agregar al alcance del análisis.

Eliminar

Si hace clic en el botón, se quita un objeto del alcance del análisis.

Este botón está disponible si la casilla de verificación junto al objeto está seleccionada.

No puede eliminar los objetos predeterminados incluidos en el alcance del análisis.

Alcance del análisis

Esta columna contiene los objetos analizados durante un análisis de malware.

Estado

El conmutador de alternancia de esta columna habilita o deshabilita el análisis de los objetos agregados al alcance del análisis.

Si el conmutador de alternancia está activado, Kaspersky Endpoint Security analiza el objeto correspondiente.

Si el conmutador de alternancia 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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

El cuadro de diálogo "Agregar alcance del análisis"

Introduzca un nombre de archivo, de carpeta o máscara

Ruta a un archivo, carpeta o máscara de archivo/carpeta.

El objeto es una carpeta

Esta casilla habilita o deshabilita el análisis de un objeto como una carpeta.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza el objeto que ha especificado en el campo **Introduzca un nombre de archivo, de carpeta o máscara** como una carpeta.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza el objeto que ha especificado en el campo **Introduzca un nombre de archivo, de carpeta o máscara** como un archivo.

Esta casilla está seleccionada por defecto.

Incluir subcarpetas

Esta casilla habilita o deshabilita el análisis de las subcarpetas de la carpeta especificada en el campo **Introduzca un nombre de archivo, de carpeta o máscara**.

Si la casilla está seleccionada, Kaspersky Endpoint Security analiza las subcarpetas durante los análisis de malware.

Si la casilla no está seleccionada, Kaspersky Endpoint Security analiza solo los archivos que se encuentran directamente en la carpeta especificada en **Introduzca un nombre de archivo, de carpeta o máscara** durante los análisis de malware.

Esta casilla está seleccionada por defecto.

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 del alcance del análisis. De lo contrario, la tarea de análisis puede finalizar con el error *Archivo infectado no eliminado*.

Ventana Parámetros del archivo

Se admiten los siguientes tipos de hashes de archivos:

- **MD5**

  Un hash de este tipo debe constar de 32 caracteres e incluir 0-9, a-f, A-F.

- **SHA256**

  Un hash de este tipo debe constar de 64 caracteres e incluir 0-9, a-f, A-F.