kaspersky

Kaspersky Embedded Systems Security 3.3 para Windows

Contenido

Acerca de Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows protege equipos y otros sistemas integrados que ejecutan Microsoft® Windows® (en adelante, denominados también dispositivos protegidos) contra virus y otras amenazas del equipo. Los usuarios de Kaspersky Embedded Systems Security para Windows son administradores de red corporativos y especialistas a cargo de la protección antivirus de la red corporativa.

La aplicación no está diseñada para utilizarse en procesos tecnológicos que involucren sistemas de control automatizados. Para proteger los dispositivos en dichos sistemas, se recomienda utilizar la aplicación Kaspersky Industrial CyberSecurity for Nodes.

Puede instalar Kaspersky Embedded Systems Security para Windows en diversos sistemas integrados que ejecuten Windows, incluidos los siguientes tipos de dispositivos:

- Cajeros automáticos
- TPV (terminal de punto de venta).

Kaspersky Embedded Systems Security para Windows se puede administrar de las siguientes formas:

- Mediante la Consola de la aplicación instalada en el mismo dispositivo protegido donde está instalado Kaspersky Embedded Systems Security para Windows o en un dispositivo diferente
- Mediante comandos en la línea de comandos
- Mediante la Consola de administración de Kaspersky Security Center

La aplicación Kaspersky Security Center también se puede utilizar para la administración centralizada de varios dispositivos protegidos que ejecutan Kaspersky Embedded Systems Security para Windows.

Es posible revisar los contadores de rendimiento de Kaspersky Embedded Systems Security para Windows para la aplicación "Supervisor del sistema", además de los contadores y las capturas SNMP.

Componentes y funciones de Kaspersky Embedded Systems Security para Windows

La aplicación incluye los siguientes componentes:

- **Protección de archivos en tiempo real**. Kaspersky Embedded Systems Security para Windows analiza los objetos cuando obtiene acceso a ellos. Kaspersky Embedded Systems Security para Windows analiza los siguientes objetos:
  - Archivos.
  - Flujos de sistemas de archivos alternativos (flujos NTFS)
  - Registros de inicio maestro y sectores de inicio de los discos duros locales y los discos extraíbles
- **Análisis a pedido**. Kaspersky Embedded Systems Security para Windows ejecuta un solo análisis de la zona especificada en busca de virus y otras amenazas de seguridad informática. La aplicación analiza los archivos, la RAM y los objetos de ejecución automática del dispositivo protegido.
- **Control de inicio de aplicaciones**. Este componente atiende a los intentos del usuario de iniciar aplicaciones y regula el inicio de las aplicaciones en el dispositivo protegido.

- **Control de dispositivos**. El componente controla el registro y el uso de dispositivos externos a fin de proteger el dispositivo contra amenazas de seguridad informática que pueden surgir al intercambiar archivos con unidades flash conectadas mediante USB u otros tipos de dispositivos externos.

- **Administración de firewall**. Este componente permite administrar el Firewall de Windows; puede usarse para configurar los ajustes y las reglas del firewall del sistema operativo, así como para bloquear toda posibilidad de que el firewall se configure en forma externa.

- **Monitor de integridad de archivos**. Kaspersky Embedded Systems Security para Windows detecta cambios en los archivos dentro de las áreas de supervisión especificadas en la configuración de la tarea. Estos cambios pueden indicar una violación de la seguridad en el dispositivo protegido.

- **Inspección de registros**. Este componente supervisa la integridad del ambiente protegido sobre la base de los resultados de una inspección de los registros de eventos de Windows.

Las siguientes funciones se implementan en la aplicación:

- **Actualización de bases de datos** y **Actualización de módulos del programa**. Kaspersky Embedded Systems Security para Windows descarga las actualizaciones de las bases de datos y los módulos de la aplicación desde los servidores de actualizaciones FTP o HTTP de Kaspersky, el servidor de administración de Kaspersky Security Center u otros orígenes de actualizaciones.

- **Cuarentena**. Kaspersky Embedded Systems Security para Windows pone en cuarentena los objetos probablemente infectados al pasarlos de su ubicación original a la carpeta de *Cuarentena*. Por motivos de seguridad, los objetos en la carpeta Cuarentena se almacenan en forma cifrada.

- **Copia de seguridad**. Kaspersky Embedded Systems Security para Windows almacena copias cifradas de los objetos clasificados como *Infectados* en *Copia de seguridad* antes de desinfectarlos o eliminarlos.

- **Notificaciones de administrador y usuario**. Puede hacer que la aplicación notifique al administrador y a los usuarios que accedan al dispositivo protegido sobre los eventos vinculados al funcionamiento de Kaspersky Embedded Systems Security y al estado de la protección antivirus del dispositivo.

- **Cómo importar y exportar la configuración**. Puede exportar la configuración de Kaspersky Embedded Systems Security para Windows a un archivo de configuración XML e importar los parámetros a Kaspersky Embedded Systems Security para Windows desde el archivo de configuración. Puede guardar todos los ajustes de la aplicación o únicamente los ajustes de componentes individuales a un archivo de configuración.

- **Aplicar plantillas**. Puede configurar manualmente los ajustes de seguridad de un nodo en el árbol o en una lista de recursos del archivo del dispositivo protegido y guardar los valores de ajuste configurados como plantilla. Esta plantilla se puede utilizar entonces para especificar las opciones de seguridad de otros nodos en las tareas de análisis y protección de Kaspersky Embedded Systems Security para Windows.

- **Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security para Windows**. Puede configurar los derechos de administración de Kaspersky Embedded Systems Security para Windows y de los servicios de Windows que están registrados por la aplicación, para usuarios y grupos de usuarios.

- **Carga de eventos en el Registro de eventos de Windows**. Kaspersky Embedded Systems Security para Windows registra la información sobre la configuración de los componentes del software, el estado actual de las tareas, los eventos que ocurrieron durante su ejecución, los eventos asociados con la administración de Kaspersky Embedded Systems Security para Windows y la información necesaria para el diagnóstico de errores en Kaspersky Embedded Systems Security para Windows.

- **Zona de confianza**. Puede generar una lista de exclusiones de la protección o del alcance del análisis que Kaspersky Embedded Systems Security para Windows aplicará durante las tareas de Protección del equipo en tiempo real y a pedido.

- **Prevención de exploits**. La memoria de un proceso puede protegerse contra los exploits a través de un Agente de protección inyectado en el proceso.

Qué hay de nuevo

La nueva versión de Kaspersky Embedded Systems Security para Windows presenta las siguientes funcionalidades y mejoras nuevas:

- En la tarea Protección contra amenazas de red, se agregó protección contra ataques de suplantación de MAC.
- En la tarea Administración de firewall, puede seleccionar el modo de interacción con el Firewall de Windows: **Observar el estado de Windows Firewall** o **Controlar la operación de Windows Firewall**.
- Para la tarea Monitor de integridad de archivos, se agregó la capacidad de exportar reglas a un archivo externo y de importar las reglas contenidas en un archivo externo.
- Para la tarea Monitor de acceso al registro, se agregó la capacidad de exportar reglas a un archivo externo y de importar las reglas contenidas en un archivo externo.
- Las reglas de procesos de confianza ahora pueden aplicarse a la tarea Control de inicio de aplicaciones. Las tareas Monitor de acceso al registro y Monitor de integridad de archivos siempre aplican la configuración de la zona de confianza. Se quitaron los ajustes que regulaban la aplicabilidad de las reglas de procesos de confianza en las tareas Monitor de integridad de archivos y Monitor de acceso al registro. Los ajustes de aplicabilidad para las reglas de procesos de confianza ahora se encuentran en los ajustes de la zona de confianza.
- En la tarea Control de inicio de aplicaciones, se agregó una opción para filtrar por nombre de grupo de dispositivos al crear reglas basadas en eventos del registro de Kaspersky Security Center.
- En Kaspersky Security Center Web Console, en la configuración de reglas de la tarea Control de inicio de aplicaciones, ahora puede agregar reglas de autorización basadas en eventos del registro de Kaspersky Security Center.
- En el complemento para administrar la aplicación a través de Kaspersky Security Center, se amplió la lista de fuentes de información sobre usuarios en la configuración de reglas y tareas de las tareas Control de inicio de aplicaciones, Control de dispositivos, Monitor de integridad de archivos y Monitor de acceso al registro. Ahora, además de especificar usuarios de las listas de Active Directory, el administrador también puede seleccionar usuarios de las listas de cuentas de Kaspersky Security Center o ingresar nombres de usuario o grupos de usuarios manualmente.
- Desde ahora, los eventos de detección de amenazas ocurridos cuando la tarea Protección contra amenazas de red opera en modo "Informar únicamente sobre los ataques detectados" se publican con el nivel de importancia "Advertencia" en lugar de "Crítico".
- Se optimizó el número de eventos de las tareas Monitor de acceso al registro y Monitor de integridad de archivos. Los eventos duplicados no se enviarán a Kaspersky Security Center; quedarán asentados únicamente en los registros de las tareas.
- Compatibilidad con nuevos sistemas operativos: Windows 11 23H2 y Windows 11 23H2 IoT.
- La aplicación notifica al usuario cuando caduca el periodo de soporte para la versión instalada de la aplicación.
- El complemento para administrar la aplicación a través de Kaspersky Security Center ya no permite crear una directiva exportando las propiedades de la directiva desde un archivo KLP. Sin embargo, esto aún puede hacerse utilizando el Asistente de nueva directiva en la Consola de administración de Kaspersky Security Center.
- Se resolvieron problemas de las versiones anteriores; en esta versión, la aplicación incluye correcciones de versiones anteriores.

Fuentes de información acerca de Kaspersky Embedded Systems Security para Windows

Esta sección enumera las fuentes de información acerca de la aplicación.

Puede seleccionar la fuente de información más adecuada, según el nivel de importancia y la urgencia del problema.

Fuentes para la recuperación de información independiente

Puede usar las siguientes fuentes para buscar información acerca de Kaspersky Embedded Systems Security para Windows:

- Página de Kaspersky Embedded Systems Security para Windows en el sitio web de Kaspersky.
- Página de Kaspersky Embedded Systems Security para Windows en el sitio web de soporte técnico (base de conocimientos).
- Manuales.

Si no encontró una solución para su problema, comuníquese con el Servicio de soporte técnico de Kaspersky.

Se requiere una conexión a Internet para usar las fuentes de información en línea.

Página de Kaspersky Embedded Systems Security para Windows en el sitio web de Kaspersky

En la página de Kaspersky Embedded Systems Security para Windows, encontrará información general acerca de la aplicación, sus funciones y sus características.

La página de Kaspersky Embedded Systems Security para Windows contiene un vínculo a la tienda en línea. Allí podrá comprar la aplicación o renovar la licencia.

Página de Kaspersky Embedded Systems Security para Windows en la Base de conocimientos

La Base de conocimientos es una sección del sitio web del servicio de soporte técnico.

La página de Kaspersky Embedded Systems Security para Windows de la Base de conocimientos contiene artículos que brindan información útil, recomendaciones y respuestas a las preguntas más frecuentes sobre la adquisición, la instalación y el uso de la aplicación.

Los artículos de la base de conocimientos pueden ayudar a responder preguntas relacionadas no solo con Kaspersky Embedded Systems Security para Windows, sino también con otras aplicaciones de Kaspersky. Los artículos de la base de conocimientos también pueden incluir noticias de soporte técnico.

Documentación de Kaspersky Embedded Systems Security para Windows

La Guía del administrador de Kaspersky Embedded Systems Security para Windows contiene información sobre la instalación, la desinstalación, la configuración y el uso de la aplicación.

Debates sobre las aplicaciones de Kaspersky en el Foro

Puede debatir preguntas relacionadas con las aplicaciones de Kaspersky con otros usuarios y especialistas de Kaspersky en nuestro Foro.

En el Foro, puede consultar temas actuales, dejar comentarios y crear temas nuevos.

Kaspersky Embedded Systems Security para Windows

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Embedded Systems Security para Windows, además de brindar una lista de requisitos de hardware y software de Kaspersky Embedded Systems Security para Windows.

Kit de distribución

El kit de distribución incluye la aplicación de bienvenida que le permite realizar lo siguiente:

- Iniciar el asistente de instalación de Kaspersky Embedded Systems Security para Windows.
- Iniciar el asistente de instalación de la Consola de Kaspersky Embedded Systems Security para Windows.
- Iniciar el asistente de instalación, que instalará el Complemento de administración de Kaspersky Embedded Systems Security para Windows para administrar la aplicación mediante Kaspersky Security Center.
- Ir a la página de Kaspersky Embedded Systems Security para Windows en el sitio web de Kaspersky.
- Visitar el sitio web del Servicio de soporte técnico.
- Leer información sobre la versión actual de Kaspersky Embedded Systems Security para Windows.

Los archivos del kit de distribución se almacenan en carpetas diferentes según el uso deseado (ver la tabla a continuación).

Archivos del kit de distribución de Kaspersky Embedded Systems Security para Windows

Archivo	Objetivo
autorun.inf	Archivo de ejecución automática del asistente de instalación de Kaspersky Embedded Systems Security para Windows para instalar la aplicación desde una unidad extraíble.
release_notes.txt	El archivo contiene información sobre la versión.
migration.txt	El archivo describe la migración desde versiones anteriores de la aplicación.
setupui.exe	Archivo de inicio del programa de bienvenida (inicia setup.hta).
ess.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de la aplicación mediante Kaspersky Security Center.
\console\esstools.msi	Paquete de Windows Installer. Instala la Consola de la aplicación en un dispositivo administrado.
\console\setup.exe	Archivo que permite iniciar un asistente para instalar un conjunto de componentes de Herramientas de administración (incluida la Consola de Kaspersky Embedded Systems Security para Windows). El archivo de paquete de instalación esstools.msi se inicia con los parámetros de instalación definidos en el asistente.
\exec\bases.cab	Archivo de almacenamiento que contiene las bases de datos antivirus actuales al momento del lanzamiento de la aplicación.
\exec\config.ini	Archivo de configuración con los parámetros de instalación para la

	creación del paquete de instalación de Kaspersky Embedded Systems Security para Windows en Kaspersky Security Center.
\exec\ess.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de Kaspersky Embedded Systems Security para Windows mediante Kaspersky Security Center.
\exec\ess_x64.msi	Paquete de Windows Installer. Instala Kaspersky Embedded Systems Security para Windows en un dispositivo administrado que cuenta con un sistema operativo Microsoft Windows de 64 bits.
\exec\ess_x86.msi	Paquete de Windows Installer. Instala Kaspersky Embedded Systems Security para Windows en un dispositivo administrado que cuenta con un sistema operativo Microsoft Windows de 32 bits.
\exec\klcfginst.exe	Instalador de un Complemento de administración de la aplicación mediante Kaspersky Security Center.
\exec\license.txt	Archivo que contiene los términos del Contrato de licencia de usuario final y la Política de privacidad.
\exec\setup.exe	Archivo para instalar Kaspersky Embedded Systems Security para Windows en el dispositivo protegido por medio del asistente; este archivo ejecuta el archivo de paquete de instalación ess.msi con los parámetros de instalación definidos en el asistente.
\product_long_term\config.ini	Archivo de configuración con los parámetros de instalación para la creación del paquete de instalación de Kaspersky Embedded Systems Security para Windows en Kaspersky Security Center.
\product_long_term\ess_light.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de Kaspersky Embedded Systems Security para Windows mediante Kaspersky Security Center.
\product_long_term\ess_x86.msi	Paquete de Windows Installer. Instala la configuración **Proteger el equipo con la tecnología de denegación predeterminada** de Kaspersky Embedded Systems Security para Windows en un equipo protegido que cuenta con un sistema operativo de 32 bits.

	Los componentes que permiten las actualizaciones no están incluidos en la configuración Proteger el equipo con la tecnología de denegación predeterminada. Si se selecciona la configuración Proteger el equipo con la tecnología de denegación predeterminada, los siguientes componentes se incluyen de manera predeterminada: • Core • Prevención de exploits • Control de inicio de aplicaciones • Icono de la bandeja del sistema Cuando se instala la configuración "Proteger el equipo con la tecnología de denegación predeteterminada" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que protege el equipo a través del análisis de firmas y el uso de bases de datos antivirus, el conjunto de componentes de la aplicación se reduce automáticamente, pues se eliminan los siguientes componentes: • Protección de archivos en tiempo real • Análisis a pedido • los componentes que permiten actualizaciones Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.
\product_long_term\ess_x64.msi	Paquete de Windows Installer. Instala la configuración **Proteger el equipo con la tecnología de denegación predeterminada** de Kaspersky Embedded Systems Security para Windows en un equipo protegido que cuenta con un sistema operativo de 64 bits.

	Los componentes que permiten las actualizaciones no están incluidos en la configuración Proteger el equipo con la tecnología de denegación predeterminada. Si se selecciona la configuración Proteger el equipo con la tecnología de denegación predeterminada, los siguientes componentes se incluyen de manera predeterminada: • Core • Prevención de exploits • Control de inicio de aplicaciones • Icono de la bandeja del sistema Cuando se instala la configuración "Proteger el equipo con la tecnología de denegación predeteterminada" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que protege el equipo a través del análisis de firmas y el uso de bases de datos antivirus, el conjunto de componentes de la aplicación se reduce automáticamente, pues se eliminan los siguientes componentes: • Protección de archivos en tiempo real • Análisis a pedido • los componentes que permiten actualizaciones Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.
\product_long_term\klcfginst.exe	Instalador de un Complemento de administración de la aplicación mediante Kaspersky Security Center.
\product_long_term\license.txt	Archivo que contiene los términos del Contrato de licencia de usuario final y la Política de privacidad.
\product_long_term\setup.exe	Archivo para instalar Kaspersky Embedded Systems Security para Windows en el dispositivo protegido a través del asistente; este archivo ejecuta el archivo de paquete de instalación ess.msi con los parámetros de instalación definidos en el asistente.
\setup\images	Carpeta con archivos de inicio de la pantalla de bienvenida de la aplicación.
\setup\setup.hta	Archivo de inicio de la pantalla de bienvenida de la aplicación.
\setup\SETUP_STRINGS.JS	Archivo con los recursos de texto de la aplicación.

Requisitos de hardware y software

Antes de instalar Kaspersky Embedded Systems Security para Windows, debe desinstalar otras aplicaciones antivirus del dispositivo.

Requisitos de software para el dispositivo protegido

Puede instalar Kaspersky Embedded Systems Security para Windows en un dispositivo que ejecute un sistema operativo Microsoft Windows de 32 o 64 bits.

Se requiere Windows Installer 3.1 para instalar y utilizar la aplicación en un dispositivo protegido que ejecute Microsoft Windows XP.

Para instalar y usar Kaspersky Embedded Systems Security para Windows en dispositivos protegidos que tengan sistemas operativos integrados, se requiere el componente Administrador de filtros.

Para el correcto funcionamiento de Kaspersky Embedded Systems Security, se requiere compatibilidad con SHA-2 en Windows. Para obtener información detallada, consulte: https://support.kaspersky.com/15728.

Puede instalar Kaspersky Embedded Systems Security para Windows en un dispositivo que ejecute alguno de los siguientes sistemas operativos Microsoft Windows de 32 o 64 bits:

- Estaciones de trabajo:
  - Windows XP Pro SP2 (32 bits / 64 bits)
  - Windows XP Pro SP3 (32 bits)
  - Windows 7 Professional / Enterprise / Ultimate SP1 (32 bits / 64 bits)
  - Windows 8 Pro / Enterprise (32 bits / 64 bits)
  - Windows 8.1 Pro / Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1507 Home / Pro / Education / Enterprise (32 bits / 64 bits)
  - Windows 10 LTSC 2015 versión 1507 (32 bits / 64 bits)
  - Windows 10 RS1 versión 1607 Home / Pro / Education / Enterprise (32 bits / 64 bits)
  - Windows 10 LTSC 2016 versión 1607 (32 bits / 64 bits)
  - Windows 10 RS2 versión 1703 Home / Pro / Education / Enterprise (32 bits / 64 bits)
  - Windows 10 RS3 versión 1709 Home / Pro / Education / Enterprise (32 bits / 64 bits)

- Windows 10 RS4 versión 1803 Home / Pro / Education / Enterprise (32 bits / 64 bits)
- Windows 10 RS5 versión 1809 Home / Pro / Education / Enterprise (32 bits / 64 bits)
- Windows 10 LTSC 2019 versión 1809 (32 bits / 64 bits)
- Windows 10 19H2 versión 1909 Home / Pro / Education / Enterprise (32 bits / 64 bits)
- Windows 10 21H2 versión 21H2 Home / Pro / Education / Enterprise (32 bits / 64 bits)
- Windows 10 LTSC 2021 versión 21H2 (32 bits / 64 bits)
- Windows 10 22H2 versión 22H2 Home / Pro / Education / Enterprise (32 bits / 64 bits)
- Windows 11 21H2 versión 21H2 Home / Pro / Education / Enterprise (64 bits)
- Windows 11 22H2 versión 2H2 Home / Pro / Education / Enterprise (64 bits)
- Windows 11 23H2 versión 23H2 Home / Pro / Education / Enterprise (64 bits)

- Sistemas integrados:
  - Windows XP Embedded SP2 (WEPOS) (32 bits / 64 bits)
  - Windows XP Embedded SP3 (POS Ready 2009) (32 bits)
  - Windows 7 Embedded SP1 (POSReady 7) (32 bits / 64 bit)
  - Windows 8.0 Embedded Industry Pro (32 bits / 64 bits)
  - Windows 8.1 Embedded Industry Pro (32 bits / 64 bits)
  - Windows 10 versión 1507 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1607 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1703 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1709 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1803 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1809 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 1909 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 21H2 IoT Enterprise (32 bits / 64 bits)
  - Windows 10 versión 22H2 IoT Enterprise (32 bits / 64 bits)
  - Windows 11 versión 21H2 IoT Enterprise (64 bits)
  - Windows 11 versión 22H2 IoT Enterprise (64 bits)
  - Windows 11 versión 23H2 IoT Enterprise (64 bits)

Requisitos de hardware para el dispositivo protegido

Requisitos de hardware para el dispositivo protegido

Tipo de sistema operativo	Nombre del sistema operativo	Requisitos mínimos	Requisitos recomendados

Estaciones de trabajo	Windows XP x86 / x64	• Procesador: Procesador de un núcleo de 1,4 GHz Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 256 MB.
		  • Para instalar todos los componentes de la aplicación: 512 MB
		• Espacio libre en disco:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB.
		  • Para instalar todos los componentes de la aplicación: 2 GB
			• Procesador: procesador de cuatro núcleos de 2,4 GHz.
			• RAM: 2 GB
			• Espacio libre en disco:
			  • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB.
			  • Para instalar todos los componentes de la aplicación: 4 GB

	Windows 7 / 8 / 10 x86	• Procesador: procesador de un núcleo de 1,4 GHz Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 256 MB.
		  • Para instalar todos los componentes de la aplicación: 1 GB
		• Espacio libre en disco:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB.
		  • Para instalar todos los componentes de la aplicación: 2 GB
			• Procesador: procesador de cuatro núcleos de 2,4 GHz.
			• RAM: 2 GB
			• Espacio libre en disco:
			  • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB.
			  • Para instalar todos los componentes de la aplicación: 4 GB

	Windows 7 / 8 / 10 / 11 x64	• Procesador: Procesador de un núcleo de 1,4 GHz Pentium IV (x64).	• Procesador: procesador de cuatro núcleos de 2,4 GHz.

		• RAM:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 1 GB.
		  • Para instalar todos los componentes de la aplicación: 2 GB
		• Espacio libre en disco:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB.
		  • Para instalar todos los componentes de la aplicación: 2 GB
			• RAM:
			  • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB.
			  • Para instalar todos los componentes de la aplicación: 4 GB
			• Espacio libre en disco:
			  • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB.
			  • Para instalar todos los componentes de la aplicación: 4 GB

Sistemas integrados	Windows XP Embedded
	
	Windows Embedded POSReady 2009
		• Procesador: Procesador de un núcleo de 1,4 GHz Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 256 MB.
		  • Para instalar todos los componentes de la aplicación: 512 MB
		• Espacio libre en disco:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB.
		  • Para instalar todos los componentes de la aplicación: 2 GB
			• Procesador: procesador de cuatro núcleos de 2,4 GHz.
			• RAM: 2 GB
			• Espacio libre en disco:
			  • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB.
			  • Para instalar todos los componentes de la aplicación: 4 GB

	Windows 7 / 8 Embedded
	Windows 10 / 11 IoT
		• Procesador: Procesador de un núcleo de 1,4 GHz Pentium IV (x64).
		• RAM: 1 GB.
		• Espacio libre en disco:
		  • Para instalar solo el componente del Control de inicio de aplicaciones: 50 MB.
		  • Para instalar todos los componentes de la aplicación: 2 GB
			• Procesador: procesador de cuatro núcleos de 2,4 GHz.
			• RAM: 2 GB
			• Espacio libre en disco:
			  • Para instalar solo el componente del Control de inicio de aplicaciones: 2 GB.
			  • Para instalar todos los componentes de la aplicación: 4 GB

Limitar la funcionalidad en versiones obsoletas de Windows

- Al crear un paquete de instalación en Kaspersky Security Center versión 12 (o posterior), para instalar Kaspersky Endpoint Agent en dispositivos con Windows XP o Windows Server 2003, debe usarse el archivo ejecutable setup.exe del paquete de instalación creado en Kaspersky Security Center versión 10.5.
- Para administrar Kaspersky Endpoint Agent mediante Kaspersky Security Center:
  - En un equipo con Windows XP SP2 Professional (32 bits / 64 bits) o Windows Server 2003 o Windows Server 2003 R2, debe usar el Agente de red de Kaspersky Security Center (klnagent) versión 10.5.1781.
  - En un equipo con Windows XP SP3 Professional (32 bits) y Windows XP Embedded SP3 (32 bits), debe usar el Agente de red de Kaspersky Security Center (klnagent) versión 14.0.0.20023.

Requisitos funcionales y limitaciones

Esta sección describe los requisitos funcionales adicionales y las limitaciones existentes de los componentes de Kaspersky Embedded Systems Security para Windows.

Instalación y desinstalación

A continuación, se muestra la lista de limitaciones de instalación y desinstalación:

- Para el correcto funcionamiento de Kaspersky Embedded Systems Security, se requiere compatibilidad con SHA-2 en Windows.
- Cuando instala la aplicación, puede aparecer una advertencia en la pantalla si la ruta especificada a la carpeta de instalación de Kaspersky Embedded Systems Security contiene más de 150 caracteres. La advertencia no afecta el proceso de instalación: puede instalar y ejecutar Kaspersky Embedded Systems Security.
- Si desea instalar el componente de compatibilidad con el protocolo SNMP, asegúrese de reiniciar el servicio SNMP si este se está ejecutando.
- Si desea instalar y ejecutar Kaspersky Embedded Systems Security en un dispositivo que se ejecuta en un sistema operativo integrado, asegúrese de instalar el componente de administración de filtros.
- No puede instalar las Herramientas de administración de Kaspersky Embedded Systems Security a través de las directivas de grupo Active Directory® de Microsoft.
- Si excluye el nodo Protección antivirus de la lista de componentes de la aplicación instalados, este nodo desaparece de la lista de componentes disponibles una vez que se completa la instalación. Para instalar los componentes del nodo Protección antivirus, inicie el Asistente de instalación desde el paquete de instalación, ya que este contiene una lista completa de los componentes.
- Si la Consola de administración de Kaspersky Embedded Systems Security está instalada, es posible que el Asistente de instalación le solicite reiniciar el equipo. En este caso, no es obligatorio reiniciarlo. Basta con finalizar la sesión del usuario que instaló la Consola de administración y volver a iniciar sesión en el sistema.

- Si instala la aplicación en los dispositivos protegidos que se ejecutan en sistemas operativos más antiguos que no pueden recibir actualizaciones regulares, asegúrese de que los siguientes certificados raíz estén instalados:

  - DigiCert Assured ID Root CA
  - DigiCert_High_Assurance_EV_Root_CA
  - DigiCertAssuredIDRootCA

  Si los certificados raíz especificados no están instalados, la aplicación puede funcionar de forma incorrecta. Le recomendamos que instale los certificados lo antes posible.

Monitor de integridad de archivos

De manera predeterminada, el Monitor de integridad de archivos no supervisa los cambios en las carpetas del sistema o en los archivos de limpieza del sistema de archivos para que los informes de tareas no estén saturados con información sobre los cambios de archivos rutinarios que el sistema operativo realiza constantemente. No puede incluir tales carpetas en el área de supervisión.

Las siguientes carpetas y archivos están excluidas del área de supervisión:

- Archivos NTFS de limpieza y optimización con id de archivo de 0 a 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\

- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

La aplicación excluye carpetas de niveles superiores.

El componente no supervisa los cambios de archivo si se evita el sistema de archivos ReFS o NTFS (es decir, que los cambios se realicen a través de BIOS, LiveCD y otros).

Administración de firewall

A continuación, se muestra la lista de limitaciones para la Administración de Firewall:

- Debe especificar más de una dirección. De lo contrario, no es posible trabajar con IPv6.
- Las reglas de la directiva de Firewall predeterminadas admiten los escenarios básicos de interacción entre dispositivos protegidos y el Servidor de administración. Para hacer uso completo de las funciones de Kaspersky Security Center, debe configurar las reglas de puerto. Puede encontrar información sobre los números de puertos, los protocolos y sus funciones en la Base de conocimientos de Kaspersky Security Center.
- Una vez que se instala la aplicación y se configuran las reglas de la tarea, la aplicación supervisa los cambios en las reglas y en los grupos de reglas de Firewall de Windows cuando se inicia la tarea Administración de firewall. Para actualizar el estado y agregar las reglas requeridas, asegúrese de reiniciar la tarea Administración de firewall.
- Cuando se inicia la tarea Administración de Firewall, las reglas de denegación y las que supervisan el tráfico saliente se eliminan automáticamente de la configuración del firewall del sistema operativo.
- No se permite usar los caracteres "*" y "?" en la ruta de la aplicación ni en el nombre de la regla de firewall para la aplicación.

Otras limitaciones

Límites del **Análisis a pedido** y de la **Protección de archivos en tiempo real**:

- El análisis de dispositivos MTP conectados no está disponible.
- El análisis de archivos no está disponible si no se habilita el análisis de archivos SFX, si el análisis de archivos está habilitado en la configuración de protección de Kaspersky Embedded Systems Security, la aplicación analiza automáticamente los objetos tanto en archivos como en archivos SFX. El análisis de archivos SFX está disponible sin analizar los archivos.
- Si se habilitan simultáneamente la casilla **Análisis detallado de los procesos que se iniciarán (la ejecución del proceso se bloqueará hasta que finalice el análisis)** y **Uso de KSN**, no se podrá iniciar ningún proceso que reciba una dirección URL como argumento, incluso si se ha elegido el modo Solo estadísticas. Para evitar el bloqueo del proceso, elija una de las opciones:
  - Deshabilite **Uso de KSN**.

- Desactivar la casilla de verificación **Análisis detallado de los procesos que se iniciarán (la ejecución del proceso se bloqueará hasta que finalice el análisis)**

Opción recomendada: Deshabilitar la casilla de verificación Análisis detallado de los procesos que se iniciarán

Licencia:

- No puede activar la aplicación con una clave mediante el asistente de instalación si la clave se creó con el comando SUBST o si la ruta de acceso al archivo de clave es una ruta de acceso de red.

- Si planea usar un servidor proxy de Kaspersky Security Center para activar el producto en un dispositivo cliente, deshabilite la optimización para VDI en ese dispositivo cuando instale el Agente de red de Kaspersky Security Center.

Actualizaciones:

- De manera predeterminada, el icono de la aplicación está oculto después de instalar las actualizaciones de los módulos críticos de Kaspersky Embedded Systems Security.

- KLRAMDISK no se admite en dispositivos protegidos que se ejecutan con los sistemas operativos Windows XP y Windows Server® 2003.

Interfaz:

- En la Consola de la aplicación, el filtrado en la Cuarentena, Copia de seguridad, Registro de auditoría del sistema o Registro de tareas distingue entre mayúsculas y minúsculas.

- Al configurar un área de análisis o de protección en la Consola de la aplicación, sólo puede utilizar una máscara y sólo al final de la ruta de acceso. Los siguientes son ejemplos de máscaras correctas: "C:\Temp\Temp*", o "C:\Temp\Temp???.doc" y "C:\Temp\Temp*.doc". Esta limitación no afecta la configuración de la Zona de confianza.

Seguridad:

- Si se encuentra activada la característica Control de la cuenta de usuario del sistema operativo, una cuenta de usuario debe formar parte del grupo de Administradores KAVWSEE para abrir la Consola de la aplicación con un doble clic en el icono de la aplicación ubicado en el área de notificación de la bandeja. De lo contrario, será necesario iniciar sesión como usuario que cuenta con permiso para abrir la Interfaz de diagnóstico compacto o el complemento de Microsoft Management Console.

- Si el Control de la cuenta de usuario está habilitado, no puede desinstalar la aplicación a través de la ventana Programas y características de Microsoft Windows.

Integración con Kaspersky Security Center:

- Cuando se reciben paquetes de actualización, el Servidor de administración verifica las actualizaciones de la base de datos antes de enviar las actualizaciones a los dispositivos protegidos en la red. El Servidor de administración no verifica las actualizaciones de módulos del programa.

- Asegúrese de que las casillas requeridas estén seleccionadas en la configuración de Interacción con Servidor de administración al momento de utilizar los componentes que transmiten datos dinámicos a Kaspersky Security Center mediante las listas de la red (Cuarentena, Copia de seguridad).

Prevención de exploits:

- Prevención de exploits no está disponible si las bibliotecas apphelp.dll no están cargadas en la configuración del entorno actual.

- El componente Prevención de exploits es incompatible con la utilidad EMET de Microsoft en dispositivos protegidos que ejecutan el sistema operativo Microsoft Windows 10. Kaspersky Embedded Systems Security para Windows bloquea EMET si el componente Prevención de exploits se instala en un dispositivo protegido que tenga instalada la utilidad EMET.

- El componente Prevención de exploits no es compatible con el motor de bases de datos SQL Server® 2012. Si instala Kaspersky Embedded Systems Security en el equipo con MS SQL Server 2012 instalado, debe agregar la biblioteca sqlos.dll del servidor de bases de datos a la lista de exclusiones en la tarea Prevención de exploits.

Instalación y desinstalación de la aplicación

Esta sección proporciona instrucciones paso a paso para instalar y eliminar Kaspersky Embedded Systems Security para Windows.

Acerca de la actualización para Kaspersky Embedded Systems Security para Windows

Se encuentra disponible una actualización a la versión 3.3 de Kaspersky Embedded Systems Security para Windows para las versiones 2.1 y posteriores de la aplicación. Para actualizar la aplicación, debe instalarse la versión nueva sobre la versión instalada. No es necesario reiniciar el equipo tras la operación.

De manera predeterminada, la aplicación crea una nueva carpeta de instalación con el nombre de la nueva versión de la aplicación, tomando como base la ruta a la carpeta de instalación de la versión existente. Puede especificar manualmente una nueva ruta para la carpeta de instalación de la aplicación.

Al actualizar Kaspersky Embedded Systems Security para Windows a la versión 3.3, la versión instalada anteriormente se elimina automáticamente.

Si su versión de Kaspersky Embedded Systems Security para Windows es anterior a la 2.1, antes de instalar la nueva versión, desinstale la versión instalada.

Si la copia de Kaspersky Embedded Systems Security para Windows versión 2.1 (o posterior) que desea actualizar está protegida con contraseña, deberá proporcionar dicha contraseña al instalador.

Cuando actualice la aplicación, la licencia que esté utilizando se aplicará automáticamente a la versión 3.3 de Kaspersky Embedded Systems Security para Windows. Podrá seguir usando los componentes y las tareas de la nueva aplicación sin restricciones. El plazo de la licencia no se modificará.

Si actualiza la aplicación y la licencia está caducada, la nueva versión de la aplicación se ejecutará en modo de funcionalidad limitada después de la instalación (con ello, por ejemplo, no podrá actualizar las bases de datos de la aplicación).

Migrar los valores de configuración de la versión actualizada de la aplicación

Los siguientes ajustes de configuración no se modifican cuando se actualiza la aplicación:

- configuración de la aplicación y de las tareas
- registros de tareas y registros de auditoría del sistema
- contenido de Cuarentena y Copia de seguridad
- cuentas con las que se inician las tareas
- permisos de acceso de usuarios para administrar la aplicación
- configuración de notificaciones sobre el funcionamiento de las tareas
- El servicio de KAVFS continúa la ejecución con el atributo PPL si este se le asignó en la versión anterior de la aplicación.

Los siguientes ajustes se restablecen o toman los valores predeterminados de la nueva versión cuando se actualiza la aplicación:

- todos los contadores, incluidos los estados de la base de datos antivirus
- datos sobre las actualizaciones instaladas para los módulos de la aplicación y las bases de datos antivirus
- estados de las tareas
- ajustes de la aplicación y de las tareas configurados a través del Registro
- ajustes de la aplicación y de las tareas que se hayan modificado al instalar correcciones críticas.

Migración de la lista de sesiones de red bloqueadas

La lista de sesiones de red bloqueadas de los equipos cliente no se migra cuando se actualiza la aplicación.

Los ajustes para desbloquear automáticamente el acceso a los recursos de archivos en red bloqueados no se modifican cuando se actualiza la aplicación.

Migración de la configuración y de las reglas de Control de inicio de aplicaciones

Cuando se actualiza la aplicación, las reglas de Control de inicio de aplicaciones se migran sin cambios.

A la hora de migrar a la versión nueva, recomendamos detener la tarea Control de inicio de aplicaciones si se está ejecutando en el modo a Activo o cambiar el modo de la tarea a *Solo estadísticas*.

Completada la actualización, recomendamos controlar que las reglas de Control de inicio de aplicaciones se hayan migrado y funcionen correctamente en modo *Solo estadísticas*.

Migración de los valores de configuración y las reglas de Administración de firewall

Cuando se actualiza la aplicación, las reglas de la tarea Administración de firewall se migran sin cambios.

Si el componente Administración de firewall no estaba instalado en la versión anterior de la aplicación, cuando se complete la actualización, la tarea Administración de Firewall se ejecutará en modo Observar el estado de Windows Firewall.

Si el componente Administración de firewall sí estaba instalado en la versión anterior de la aplicación, la tarea Administración de firewall se ejecutará en modo Controlar la operación de Windows Firewall cuando se complete la actualización.

Actualización de la aplicación con cambios en la configuración

Cuando se instala desde la carpeta /exec la configuración "Proteger el equipo con bases antivirus" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que no depende del análisis de firmas y el uso de bases de datos antivirus para proteger el equipo ("Proteger el equipo con la tecnología de denegación predeterminada"), el conjunto de componentes de la aplicación se amplía y se complementa automáticamente con los siguientes componentes:

- Protección de archivos en tiempo real

- Análisis a pedido
- Protección contra amenazas de red

El archivo de almacenamiento que contiene las bases de datos antivirus se descomprime de forma automática.

Si no desea utilizar estos componentes y tareas para proteger el dispositivo, reinicie la instalación del producto desde la carpeta /product_long_term.

Cuando se instala desde la carpeta /product_long_term la configuración "Proteger el equipo con la tecnología de denegación predeterminada" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que protege el equipo a través del análisis de firmas y el uso de bases de datos antivirus ("Proteger el equipo con bases antivirus"), el conjunto de componentes de la aplicación se reduce automáticamente, pues se eliminan los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido
- los componentes que permiten actualizaciones

Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.

Declaración de Kaspersky Security Network y Declaración de Kaspersky Managed Protection

Una vez que la aplicación se actualice a la versión 3.3, la tarea Uso de KSN se detendrá. Para continuar usando la infraestructura en la nube de KSN y el servicio KMP tras la actualización, deberá leer y aceptar los términos de la Declaración de Kaspersky Security Network y de la Declaración de Kaspersky Managed Protection.

Acerca de la actualización para las Herramientas de administración de Kaspersky Embedded Systems Security para Windows

Todas las versiones de la Consola de aplicación se pueden actualizar a la versión 3.3 de Kaspersky Embedded Systems Security Console para Windows.

Además:

- Los valores de configuración de la Consola de la aplicación no se modifican.
- Todas las versiones anteriores de Kaspersky Embedded Systems Security para Windows se pueden administrar con la versión 3.3 de la Consola de la aplicación.
- Kaspersky Embedded Systems Security para Windows versión 3.3 se puede administrar con cualquier versión más antigua de la Consola de la aplicación.

Las siguientes versiones del Complemento de administración se pueden actualizar a la versión 3.3:

- 2.1.0.xxx
- 2.3.0.xxx
- 3.0.0.xxx

- 3.1.0.xxx
- 3.2.0.xxx

Además:

- Los valores de configuración del Complemento de administración de las versiones mencionadas más arriba no se modifican al actualizar a la versión 3.3.
- Las siguientes versiones de Kaspersky Embedded Systems Security para Windows pueden ser administradas por el Complemento de administración versión 3.3: 2.1.0.441, 2.3.0.754, 3.0.0.102, 3.1.0.461 y 3.2.0.200.
- Kaspersky Embedded Systems Security para Windows versión 3.3 se puede administrar mediante el Complemento de administración de cualquiera de las versiones mencionadas arriba.

Durante la actualización, se instala una nueva versión del Complemento de administración o de la Consola de la aplicación sobre la versión instalada anteriormente. No es necesario reiniciar el equipo tras esta operación.

Códigos de los componentes del software Kaspersky Embedded Systems Security para Windows para el servicio Windows Installer

Los archivos \product_long_term\ess_x86.msi y \product_long_term\ess_x64.msi están diseñados para instalar la configuración **Proteger el equipo con la tecnología de denegación predeterminada** de Kaspersky Embedded Systems Security para Windows, y los archivos \product\ess_x86.msi y \product\ess_x64.msi están diseñados para instalar la configuración **Proteger el equipo con bases antivirus** de Kaspersky Embedded Systems Security para Windows.

Cuando se selecciona la configuración "Proteger el equipo con bases antivirus", de manera predeterminada, se incluyen todos los componentes de Kaspersky Embedded Systems Security para Windows, excepto los componentes Administración de firewall y Contadores de rendimiento.

Cuando se instala la configuración "Proteger el equipo con bases antivirus" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que no depende del análisis de firmas y el uso de bases de datos antivirus para proteger el equipo, el conjunto de componentes de la aplicación se amplía y se complementa automáticamente con los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido
- Protección contra amenazas de red

Los componentes que permiten las actualizaciones no están incluidos en la configuración Proteger el equipo con la tecnología de denegación predeterminada.

Si se selecciona la configuración Proteger el equipo con la tecnología de denegación predeterminada, los siguientes componentes se incluyen de manera predeterminada:

- Core
- Prevención de exploits
- Control de inicio de aplicaciones
- Icono de la bandeja del sistema

Cuando se instala la configuración "Proteger el equipo con la tecnología de denegación predeteterminada" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que protege el equipo a través del análisis de firmas y el uso de bases de datos antivirus, el conjunto de componentes de la aplicación se reduce automáticamente, pues se eliminan los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido
- los componentes que permiten actualizaciones

Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.

Los archivos \console\esstools_x86.msi y \console\esstools_x64.msi instalan todos los componentes de software que forman parte de las Herramientas de administración.

Las siguientes secciones presentan los códigos de los componentes de Kaspersky Embedded Systems Security para Windows para el servicio Windows Installer. Estos códigos pueden utilizarse para definir una lista de los componentes que se instalan durante la instalación de Kaspersky Embedded Systems Security para Windows desde la línea de comandos.

Componentes de software de Kaspersky Embedded Systems Security para Windows

La siguiente tabla contiene códigos y descripciones de los componentes del software de Kaspersky Embedded Systems Security.

Descripción de los componentes del software de Kaspersky Embedded Systems Security

Componente	Identificador	Funciones del componente
Funcionalidad básica	Core	Este componente contiene el conjunto de funciones básicas de la aplicación y asegura su funcionamiento.

		Si se especifican otros componentes de Kaspersky Embedded Systems Security al instalar Kaspersky Embedded Systems Security desde la línea de comandos, pero no se especifica el componente Core, este se instala automáticamente.
Control de inicio de aplicaciones	AppCtrl	Este componente supervisa los intentos del usuario de iniciar aplicaciones y permite o deniega el inicio de aplicaciones de acuerdo con las reglas especificadas de Control de inicio de aplicaciones. Se implementa en la tarea Control de inicio de aplicaciones.
Control de dispositivos	DevCtrl	Este componente rastrea los intentos de conectar dispositivos externos a un dispositivo protegido y permite o deniega el uso de estos de acuerdo con las reglas especificadas de Control de dispositivos. El componente se implementa en la tarea Control de dispositivos.
Protección antivirus	AVProtection	Este componente brinda protección antivirus.
Protección contra amenazas de red	IDS	Este componente analiza el tráfico de red entrante en busca de actividad típica de los ataques de red. Al detectar un intento de ataque de red que apunta a su equipo, Kaspersky Embedded Systems Security para Windows bloquea la actividad de red del equipo atacante.
Análisis a pedido	Ods	Este componente instala los archivos del sistema de Kaspersky Embedded Systems Security para Windows y lleva a cabo las tareas de análisis a pedido (análisis a pedido de los objetos en el dispositivo protegido).
Protección de archivos en tiempo real	Oas	Este componente realiza análisis de virus en archivos en el dispositivo protegido cuando se accede a estos archivos. Implementa la tarea Protección de archivos en tiempo real.
Uso de Kaspersky Security Network	Ksn	Este componente proporciona protección basada en tecnologías en la nube de Kaspersky. Implementa la tarea Uso de KSN (enviar solicitudes y recibir conclusiones del servicio de Kaspersky Security Network).
Monitor de integridad de archivos	Fim	Este componente registra las operaciones realizadas en archivos en el área de supervisión especificado. El componente implementa la tarea Monitor de integridad de archivos.

Monitor de acceso a registros	RegMonitor	Este componente permite supervisar las acciones que se realizaron con las ramas y claves del registro especificadas en las áreas de supervisión definidas en la configuración de la tarea. El componente implementa el Monitor de acceso a registros.
Prevención de exploits	AntiExploit	Este componente permite administrar la configuración para proteger la memoria que utilizan los procesos en la memoria de un dispositivo.
Administración de firewall	Firewall	Este componente permite administrar el firewall de Windows a través de la interfaz gráfica de usuario de Kaspersky Embedded Systems Security. El componente implementa la tarea Administración de Firewall.
Módulo de integración con el Agente de red de Kaspersky Security Center	AKIntegración	Este componente brinda una conexión entre Kaspersky Embedded Systems Security para Windows y el Agente de red de Kaspersky Security Center. Puede instalar este componente en el dispositivo protegido si planea administrar la aplicación a través de Kaspersky Security Center.
Inspección de registros	LogInspector	Este componente supervisa la integridad del ambiente protegido sobre la base de los resultados de una inspección de los registros de eventos de Windows.
Conjunto de contadores de rendimiento del "supervisor del sistema"	PerfMonCounters	Este componente instala un conjunto de contadores de rendimiento del supervisor del sistema. Estos contadores permiten medir el rendimiento de Kaspersky Embedded Systems Security para Windows y localizar los posibles cuellos de botella que puedan surgir cuando Kaspersky Embedded Systems Security para Windows se utiliza junto con otros programas.
Contadores y capturas SNMP	SnmpSupport	Este componente publica contadores y capturas de Kaspersky Embedded Systems Security a través del Protocolo simple de administración de redes (SNMP) en Microsoft Windows. El componente puede instalarse en el dispositivo protegido solo si el servicio SNMP de Microsoft también está instalado en ese dispositivo.
Icono de Kaspersky Embedded Systems Security en el área de notificación	TrayApp	Este componente muestra el icono de Kaspersky Embedded Systems Security en el área de notificación de la bandeja de tareas del dispositivo protegido. El icono de Kaspersky Embedded Systems Security

		muestra el estado de protección del dispositivo y puede usarse para abrir la Consola de Kaspersky Embedded Systems Security en Microsoft Management Console (si está instalado) y la ventana **Acerca de la aplicación**.

Componentes de software “Herramientas de administración”

La siguiente tabla contiene código y la descripción del componente de software de las "Herramientas de administración".

Descripción del componente de software "Herramientas de administración"

Componente	Código	Funciones del componente
Componente de Kaspersky Embedded Systems Security para Windows	MmcSnapin	Este componente instala el complemento Microsoft Management Console para administrar la aplicación mediante la Consola de Kaspersky Embedded Systems Security para Windows. Si se especifican otros componentes durante la instalación de las "Herramientas de administración" desde la línea de comandos y no se indica el componente MmcSnapin, este se instala automáticamente.

Cambios en el sistema después de la instalación de Kaspersky Embedded Systems Security para Windows

Si Kaspersky Embedded Systems Security para Windows y el conjunto de "Herramientas de administración" (incluida la Consola de la aplicación) se instalan juntos, el servicio Windows Installer realiza las siguientes modificaciones en el dispositivo protegido:

- Se crean las carpetas de Kaspersky Embedded Systems Security para Windows en el dispositivo protegido y en el dispositivo protegido en el que se instala la Consola de la aplicación.
- Se registran los servicios de Kaspersky Embedded Systems Security para Windows.
- Se crea un grupo de usuarios de Kaspersky Embedded Systems Security para Windows.
- Las claves de Kaspersky Embedded Systems Security para Windows se graban en el registro del sistema.
- Se crea la tarea de detección de actualizaciones del SO de Kaspersky Embedded Systems que se muestra en el Programador de tareas de Windows.

Estos cambios se describen a continuación.

Carpetas de Kaspersky Embedded Systems Security para Windows en un dispositivo protegido

Cuando se instala Kaspersky Embedded Systems Security para Windows, se crean las siguientes carpetas en un dispositivo protegido:

- La carpeta de instalación predeterminada de Kaspersky Embedded Systems Security para Windows que contiene los archivos ejecutables de Kaspersky Embedded Systems Security para Windows depende del conjunto de bits del sistema operativo. Por lo tanto, las carpetas de instalación predeterminadas son las siguientes:
  - En la versión de 32 bits de Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- Archivos MIB (Management Information Base) que contienen una descripción de los contadores y los enlaces publicados por Kaspersky Embedded Systems Security para Windows a través del protocolo SNMP:
  - %Kaspersky Embedded Systems Security%\mibs
- Las versiones de 64 bits de los archivos ejecutables de Kaspersky Embedded Systems Security para Windows (esta carpeta se creará únicamente durante la instalación de Kaspersky Embedded Systems Security para Windows para la versión de 64 bits de Microsoft Windows):
  - %Kaspersky Embedded Systems Security%\x64
- Archivos de servicio de Kaspersky Embedded Systems Security para Windows:
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Dskm

  Para Windows XP, la ruta de acceso a la carpeta de Kaspersky Lab es %ALLUSERSPROFILE%\Application Data
- Archivos con configuración para orígenes de actualizaciones:

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update
- Actualizaciones de bases de datos y módulos del programa descargados mediante la tarea Copia de actualizaciones (la carpeta se crea la primera vez que se descargan actualizaciones con la tarea Copia de actualizaciones).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Update\Distribution
- Registros de tareas y registro de auditoría del sistema.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports
- Conjunto de bases de datos actualmente en uso.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Current
- Copias de seguridad de bases de datos; se sobrescriben cada vez que se actualizan las bases de datos.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Backup
- Archivos temporales creados durante la ejecución de tareas de actualización.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Bases\Temp

- Objetos en cuarentena (carpeta predeterminada).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Quarantine

- Objetos en copia de seguridad (carpeta predeterminada).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Backup

- Objetos restaurados de la copia de seguridad y la cuarentena (carpeta predeterminada para los objetos restaurados).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored

Carpeta creada durante la instalación de la Consola de la aplicación

Las carpetas de instalación predeterminadas de la Consola de la aplicación que contienen los archivos de las "Herramientas de administración" dependen del conjunto de bits del sistema operativo. Por lo tanto, las carpetas de instalación predeterminadas son las siguientes:

- Para la versión de 32 bits de Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

- Para la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

Servicios de Kaspersky Embedded Systems Security para Windows

Los siguientes servicios de Kaspersky Embedded Systems Security para Windows se inician con la cuenta de sistema local (SYSTEM):

- Servicio de Kaspersky Security (KAVFS): servicio esencial de Kaspersky Embedded Systems Security para Windows que administra las tareas y el flujo de trabajo de Kaspersky Embedded Systems Security para Windows.

- Servicio de Kaspersky Security Management (KAVFSGT): este servicio está previsto para la administración de la aplicación Kaspersky Embedded Systems Security para Windows a través de la Consola de la aplicación.

- Servicio de Kaspersky Security Exploit Prevention (KAVFSSLP): este servicio actúa como intermediario; en ese rol, comunica los ajustes de seguridad a los agentes de seguridad externos y recibe datos sobre los eventos de seguridad.

Grupo de Kaspersky Embedded Systems Security para Windows

"Administradores de ESS" es un grupo que se crea en el dispositivo protegido. Sus usuarios tienen acceso absoluto al servicio de Kaspersky Security Management y a todas las funciones de Kaspersky Embedded Systems Security para Windows.

Claves de registro del sistema

Cuando se instala Kaspersky Embedded Systems Security para Windows, se crean las siguientes claves de registro del sistema:

- Propiedades de Kaspersky Embedded Systems Security para Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]

- Configuración del registro de eventos de Kaspersky Embedded Systems Security para Windows (Registro de eventos de Kaspersky): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]

- Propiedades del servicio de administración de Kaspersky Embedded Systems Security para Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]

- Configuración del contador de rendimiento:

  - Para la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]

  - Para la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]

- Configuración del componente de compatibilidad con el protocolo SNMP:

  - Para la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\SnmpAgent]

  - Para la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\SnmpAgent]

- Configuración del archivo de volcado:

  - Para la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\CrashDump]

  - Para la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\CrashDump]

- Configuración del archivo de rastreo:

  - Para la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.2\Trace]

  - Para la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.2\Trace]

- Configuración para tareas y funciones de la aplicación: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3\Environment]

Tarea del sistema Kaspersky Embedded Systems Security OS Upgrade Detect

Durante la instalación de Kaspersky Embedded Systems Security, el servicio de Windows Installer crea una tarea de detección de actualizaciones del SO: Kaspersky Embedded Systems Security OS Upgrade Detect. La tarea se inicia en forma inmediata una vez creada y vuelve a iniciarse cada vez que se inicia el sistema operativo. La tarea analiza la versión de los controladores utilizados por la aplicación: si la versión del sistema operativo se ha actualizado, la aplicación actualiza los controladores a la versión que corresponda para el sistema operativo.

Esta tarea no afecta a la aplicación y se puede eliminar. Recomendamos tener presente el escenario de actualización del sistema operativo.

Procesos de Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows inicia los procesos que se describen en la siguiente tabla.

Procesos de Kaspersky Embedded Systems Security para Windows

Nombre del archivo	Objetivo
kavfswp.exe	Flujo de trabajo de Kaspersky Embedded Systems Security para Windows
kavtray.exe	Proceso para el icono de la bandeja del sistema
kavfsmui.exe	Proceso para el componente de interfaz de diagnóstico compacto
kavshell.exe	Proceso de la utilidad de línea de comandos
kavfsrcn.exe	Proceso de administración remota de Kaspersky Embedded Systems Security para Windows
kavfs.exe	Proceso del servicio de Kaspersky Security
kavfsgt.exe	Proceso del servicio de Kaspersky Security Management
kavfswh.exe	Proceso del servicio de Kaspersky Security Exploit Prevention

Configuraciones de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer

Esta sección contiene descripciones de las configuraciones para instalar y desinstalar Kaspersky Embedded Systems Security para Windows, sus valores predeterminados, claves para modificar la configuración de instalación y sus posibles valores. Estas claves pueden utilizarse junto con claves estándar para el comando `msiexec` del servicio Windows Installer durante la instalación de Kaspersky Embedded Systems Security para Windows desde la línea de comandos.

Configuración de instalación y opciones de la línea de comandos en Windows Installer

- Aceptación de los términos del Contrato de licencia de usuario final: debe aceptar los términos para instalar Kaspersky Embedded Systems Security para Windows.

  Los valores posibles para la opción de la línea de comandos `EULA=<valor>` son los siguientes:

  - `0`: rechaza los términos del Contrato de licencia de usuario final (valor predeterminado).
  - `1`: acepta los términos del Contrato de licencia de usuario final.

- Aceptación de los términos de la Política de privacidad: debe aceptar los términos para instalar Kaspersky Embedded Systems Security para Windows.

  Los valores posibles para la opción de la línea de comandos `PRIVACYPOLICY=<valor>` son los siguientes:

  - `0`: rechaza los términos de la Política de privacidad (valor predeterminado).
  - `1`: acepta los términos de la Política de privacidad.

- Permita la instalación de Kaspersky Embedded Systems Security para Windows si la actualización KB4528760 no está instalada. Para obtener información detallada sobre la actualización KB4528760, visite el sitio web de Microsoft.

  Los valores posibles para la opción de la línea de comandos `SKIPCVEWINDOWS10=<valor>` son los siguientes:

  - `0`: cancelar la instalación de Kaspersky Embedded Systems Security para Windows si la actualización KB4528760 no está instalada (valor predeterminado).
  - `1`: permitir la instalación de Kaspersky Embedded Systems Security para Windows si la actualización KB4528760 no está instalada.

  La actualización KB4528760 corrige la vulnerabilidad de seguridad CVE-2020-0601. Para obtener información detallada sobre la vulnerabilidad de seguridad CVE-2020-0601, visite el sitio web de Microsoft.

- Instalar Kaspersky Embedded Systems Security para Windows y conservar la configuración de la versión anterior durante la actualización.

  Los valores posibles para la opción de la línea de comandos RESTOREDEFSETTINGS=<valor> son los siguientes:

  - `0`: durante la actualización, se transferirán a la nueva versión todos los datos de la versión anterior (valor predeterminado).
  - `1`: durante la actualización, se migrará a la nueva versión únicamente el archivo que contiene los datos de activación y las claves privadas ([unidad]:\ProgramData\Kaspersky Lab\<producto>\<versión>\Data\product.dat). Se eliminarán todos los demás datos de la versión anterior, incluidos los ajustes, las bases de datos antivirus, los informes, los objetos en cuarentena y los objetos de copia de seguridad.

- Instalar Kaspersky Embedded Systems Security para Windows y conservar los informes de la versiones anteriores durante la actualización.

  Los valores posibles para la opción de la línea de comandos KEEP_REPORTS=<valor> son los siguientes:

  - `0`: durante la actualización, se migrarán a la nueva versión todos los datos de la versión anterior, excepto los informes ([unidad]:\ProgramData\Kaspersky Lab\<producto>\<versión>\Reports). Los informes se eliminarán.
  - `1`: durante la actualización, se migrarán a la nueva versión todos los datos de la versión anterior, incluidos los ajustes, las bases de datos antivirus, los informes, los objetos en cuarentena y los objetos de copia de seguridad (valor predeterminado).

- Instalación de Kaspersky Embedded Systems Security para Windows con un análisis preliminar de los procesos activos y los sectores de inicio de los discos locales

  Los valores posibles para la opción de la línea de comandos `PRESCAN=<valor>` son los siguientes:

  - `0`: no realice un análisis preliminar de los procesos activos y de los sectores de arranque de los discos locales durante la instalación (valor predeterminado).
  - `1`: realice un análisis preliminar de los procesos activos y de los sectores de arranque de los discos locales durante la instalación.

- Carpeta de destino en la que se guardan los archivos de Kaspersky Embedded Systems Security para Windows durante la instalación. Puede especificar otra carpeta.

  Los valores predeterminados para la opción de la línea de comandos `INSTALLDIR=<ruta completa a la carpeta>` son los siguientes:

- Kaspersky Embedded Systems Security para Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
- Herramientas de administración: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
- En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%

- Iniciar la tarea Protección de archivos en tiempo real inmediatamente después de que se inicie Kaspersky Embedded Systems Security para Windows.

  Los valores posibles para la opción de la línea de comandos `RUNRTP=< valor >` son los siguientes:

  - `1`: iniciar (valor predeterminado).
  - `0`: no iniciar.

- Modo de ejecución la tarea Protección de archivos en tiempo real.

  Los valores posibles para la opción de la línea de comandos `RUNRTP=< valor >` son los siguientes:

  - `1`: recomendado (valor predeterminado).
  - `0`: solo notificar.

- Los objetos excluidos del área de protección según las recomendaciones de Microsoft Corporation. En la tarea Protección de archivos en tiempo real, excluya del área de la protección a los objetos del dispositivo que Microsoft Corporation recomiende excluir. Es posible que algunas aplicaciones instaladas en el dispositivo protegido se vuelvan inestables si una aplicación antivirus intercepta o modifica los archivos utilizados. Por ejemplo, Microsoft Corporation incluye algunas aplicaciones del controlador de dominio en la lista de tales objetos.

  Los valores posibles para la opción de la línea de comandos `ADDMSEXCLUSION=<valor>` son los siguientes:

  - `1`: excluir (valor predeterminado).
  - `0`: no excluir.

- Los objetos excluidos del área de protección según las recomendaciones de Kaspersky. En la tarea Protección de archivos en tiempo real, excluya del área de la protección a los objetos del dispositivo que Kaspersky recomiende excluir.

  Los valores posibles para la opción de la línea de comandos `ADDKLEXCLUSION=<valor>` son los siguientes:

  - `1`: excluir (valor predeterminado).
  - `0`: no excluir.

- Permite la conexión remota con la Consola de la aplicación. De manera predeterminada, no se permite la conexión remota a la Consola de la aplicación instalada en el dispositivo protegido. Durante la instalación, puede permitir la conexión. Kaspersky Embedded Systems Security para Windows crea reglas de autorización para el proceso kavfsgt.exe mediante la utilización del protocolo de TCP para todos los puertos.

  Los valores posibles para la opción de la línea de comandos `ALLOWREMOTECON=<valor>` son los siguientes:

  - `1`: permitir.
  - `0`: denegar (valor predeterminado).

- Ruta de acceso al archivo de clave (`LICENSEKEYPATH`). De forma predeterminada, Windows Installer busca el archivo con la extensión .key en la carpeta \exec del kit de distribución. Si la carpeta \exec contiene más de un archivo de clave, Windows Installer selecciona el archivo de clave con la fecha de caducidad más lejana en el futuro. Puede guardar un archivo de clave de antemano en la carpeta \exec o puede indicar otra ruta de acceso al archivo a través de la opción **Agregar clave**. Para agregar una clave después de la instalación de Kaspersky Embedded Systems Security para Windows, utilice la herramienta administrativa que prefiera (por ejemplo, la Consola de la aplicación). Si no agrega una clave durante la instalación de la aplicación, Kaspersky Embedded Systems Security para Windows no funcionará.

- Ruta al archivo de configuración. Kaspersky Embedded Systems Security para Windows importa la configuración a partir del archivo de configuración especificado creado en la aplicación. Kaspersky Embedded Systems Security para Windows no importa contraseñas del archivo de configuración (por ejemplo, contraseñas de cuenta para iniciar tareas ni contraseñas para establecer conexión con un servidor proxy). Una vez que se hayan importado las configuraciones, deberá introducir todas las contraseñas de forma manual. Si no ha especificado ningún archivo de configuración, la aplicación empleará los valores predeterminados tras la instalación.

  No se especifica el valor predeterminado para `CONFIGPATH=<nombre del archivo de configuración>`.

- Modo de la tarea **Análisis al inicio del sistema operativo** (SCANSTARTUP_BLOCKING). Si instala Kaspersky Embedded Systems Security para Windows en el modo de instalación sin la clave SCANSTARTUP_BLOCKING, la tarea **Análisis al inicio del sistema operativo** tendrá asignados los siguientes parámetros en el ajuste **Área del análisis**:

  - **Acción que se realizará con los objetos infectados y otros objetos: Solo notificar**
  - **Acción que se realizará con los objetos probablemente infectados: Solo notificar**

  Si instala Kaspersky Embedded Systems Security para Windows en el modo de instalación con la clave SCANSTARTUP_BLOCKING, la tarea **Análisis al inicio del sistema operativo** tendrá asignados los siguientes parámetros en el ajuste **Área del análisis**:

  - **Acción que se realizará con los objetos infectados y otros objetos: Realizar la acción recomendada**
  - **Acción que se realizará con los objetos probablemente infectados: Realizar la acción recomendada**

  La tarea **Análisis al inicio del sistema operativo** se crea automáticamente. De manera predeterminada, se aplica el modo **Solo notificar**. En este caso, cuando concluya el despliegue de Kaspersky Embedded Systems Security en los dispositivos, podrá habilitar la tarea **Análisis al inicio del sistema operativo** si no se descubrieron problemas con los servicios del sistema al realizarse los análisis. Si la aplicación detecta servicios críticos del sistema como objetos infectados o probablemente infectados, el modo **Solo notificar** le da tiempo para averiguar el motivo y resolver el problema. Si la aplicación aplica el modo **Realizar la acción recomendada**, se realizará la acción **Desinfectar. Eliminar si falla la desinfección**. Desinfectar o eliminar archivos del sistema puede provocar problemas críticos en el inicio del sistema operativo.

- La habilitación de las conexiones de red para la opción de la Consola de la aplicación se utiliza para instalar la Consola de Kaspersky Embedded Systems Security para Windows en otro dispositivo. Puede administrar de forma remota la protección del dispositivo desde otro dispositivo con la Consola de Kaspersky Embedded Systems Security para Windows instalada. El puerto 135 (TCP) se abre en el Firewall de Microsoft Windows, se permiten las conexiones de red del archivo ejecutable kavfsrcn.exe para la administración remota de Kaspersky Embedded Systems Security para Windows y se concede acceso a aplicaciones DCOM. Cuando finalice la instalación, agregue los usuarios al grupo de Administradores de ESS para permitirles administrar la aplicación de forma remota y autorice las conexiones de red para el servicio de Kaspersky Security Management (kavfsgt.exe file) en el dispositivo protegido. Puede leer más sobre la configuración adicional cuando la Consola de Kaspersky Embedded Systems Security para Windows se instala en otro dispositivo.

  Los valores posibles para la opción de la línea de comandos `ADDWFEXCLUSION=<valor>` son los siguientes:

  - 1: permitir.

- `0`: denegar (valor predeterminado).

- Deshabilitación de la verificación de software incompatible. Utilice esta configuración para habilitar o deshabilitar la verificación de software incompatible durante la instalación en segundo plano de la aplicación en el dispositivo protegido. Independientemente del valor de esta configuración, durante la instalación de Kaspersky Embedded Systems Security, la aplicación siempre advierte sobre otras versiones de la aplicación instaladas en el dispositivo protegido.

  Los valores posibles para la opción de la línea de comandos `SKIPINCOMPATIBLESW=<valor>` son los siguientes:

  - `0`: se realiza la verificación de software incompatible (valor predeterminado).
  - `1`: no se realiza la verificación de software incompatible.

Configuración de desinstalación y opciones de la línea de comandos en Windows Installer

- Restauración de objetos en cuarentena.

  Los valores posibles para la opción de la línea de comandos `RESTOREQTN=<valor>` son los siguientes:

  - `0`: eliminar el contenido puesto en cuarentena (valor predeterminado).
  - `1`: restaurar el contenido puesto en cuarentena en la carpeta especificada por el parámetro RESTOREPATH en la subcarpeta \Quarantine.

- Restauración del contenido de la copia de seguridad.

  Los valores posibles para la opción de la línea de comandos `RESTOREBCK=<valor>` son los siguientes:

  - `0`: eliminar el contenido de la copia de seguridad (valor predeterminado).
  - `1`: restaurar el contenido de la copia de seguridad en la carpeta especificada por el parámetro RESTOREPATH en la subcarpeta \Backup.

- Ingrese la contraseña actual para confirmar la desinstalación (si la protección con contraseña está habilitada).

  No se especifica el valor predeterminado para `UNLOCK_PASSWORD=<contraseña especificada>`.

- Carpeta de objetos restaurados. Los objetos restaurados se almacenan en la carpeta especificada.

  El valor predeterminado para la opción de la línea de comandos `RESTOREPATH=<ruta completa a la carpeta>` es %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Restored.

Registros de instalación y desinstalación de Kaspersky Embedded Systems Security para Windows

Si Kaspersky Embedded Systems Security para Windows se instala o desinstala con la ayuda del asistente de instalación (o desinstalación), el servicio Windows Installer crea un registro de instalación (o instalación). Se guardará un archivo de registro llamado ess_v3.2_install_<uid>.log (donde <uid> es un identificador único de registro formado por ocho caracteres) en la carpeta %temp% del usuario cuya cuenta se haya utilizado para iniciar el archivo setup.exe.

Si utiliza la opción **Modificar o eliminar** disponible en el menú **Inicio** para la Consola de la aplicación o Kaspersky Embedded Systems Security para Windows, se creará automáticamente un archivo de registro llamado ess_v3.3_install_<uid> en la carpeta %temp%.

Si Kaspersky Embedded Systems Security para Windows se instala o desinstala desde la línea de comandos, el archivo de registro de instalación no se crea de manera predeterminada.

Para instalar Kaspersky Embedded Systems Security para Windows y crear un archivo de registro en el disco C:\:

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Planificación de la instalación

Esta sección describe el conjunto de herramientas de administración de Kaspersky Embedded Systems Security para Windows y aspectos especiales de la instalación y desinstalación de Kaspersky Embedded Systems Security para Windows con el asistente, desde la línea de comandos, mediante Kaspersky Security Center y mediante directivas de grupos de Active Directory.

Antes de iniciar la instalación Kaspersky Embedded Systems Security para Windows, planee las etapas principales de la instalación.

1. Defina qué herramientas de administración utilizará para configurar y administrar Kaspersky Embedded Systems Security para Windows.
2. Seleccione los componentes de la aplicación necesarios para la instalación.
3. Elija el método de instalación.

Selección de herramientas de administración

Defina las herramientas de administración que utilizará para configurar Kaspersky Embedded Systems Security para Windows y para administrar la aplicación. Kaspersky Embedded Systems Security para Windows se puede administrar desde la Consola de la aplicación, la utilidad de línea de comandos y la Consola de administración de Kaspersky Security Center.

Consola de Kaspersky Embedded Systems Security para Windows

La Consola de Kaspersky Embedded Systems Security para Windows es un complemento independiente agregado a Microsoft Management Console. Kaspersky Embedded Systems Security para Windows puede administrarse mediante la Consola de la aplicación instalada en el dispositivo protegido o en cualquier otro dispositivo de la red corporativa.

Es posible agregar varios complementos de Kaspersky Embedded Systems Security para Windows a una Microsoft Management Console abierta en el modo de creación, a fin de usarla para administrar la protección de varios dispositivos con Kaspersky Embedded Systems Security para Windows instalado.

La Consola de la aplicación se incluye en el conjunto de componentes de la aplicación "Herramientas de administración".

Utilidad de línea de comandos

Puede administrar Kaspersky Embedded Systems Security para Windows desde la línea de comandos del dispositivo protegido.

La utilidad de línea de comandos está incluida en el grupo de componentes de la aplicación Kaspersky Embedded Systems Security para Windows.

Kaspersky Security Center

Si su empresa utiliza Kaspersky Security Center para administrar de forma centralizada la protección antivirus de los dispositivos, puede gestionar Kaspersky Embedded Systems Security para Windows a través de la Consola de administración de Kaspersky Security Center.

Deben instalarse los siguientes componentes:

- **Módulo de integración con el Agente de red de Kaspersky Security Center**. Este componente está incluido en el grupo de componentes de la aplicación Kaspersky Embedded Systems Security para Windows. Permite la comunicación entre Kaspersky Embedded Systems Security para Windows y el Agente de red. Instale el módulo de integración con el Agente de red de Kaspersky Security Center en el dispositivo protegido.

- **Agente de red de Kaspersky Security Center**. Instale este componente en todos los dispositivos protegidos. Este componente admite la interacción entre la instancia de Kaspersky Embedded Systems Security para Windows instalada en el dispositivo protegido y la Consola de administración de Kaspersky Security Center. El archivo de instalación del Agente de red se encuentra en la carpeta del kit de distribución de Kaspersky Security Center.

- **Complemento de administración de Kaspersky Embedded Systems Security 3.3 para Windows**. Además, puede instalar el Complemento de administración para gestionar Kaspersky Embedded Systems Security para Windows a través de la Consola de administración en el dispositivo protegido donde se instaló el servidor de administración de Kaspersky Security Center. Esto proporciona la interfaz para la administración de la aplicación mediante Kaspersky Security Center. El archivo de instalación del Complemento de administración, \exec\klcfginst.exe, está incluido en el kit de distribución de Kaspersky Embedded Systems Security para Windows.

Selección del tipo de instalación

Después de especificar los componentes de software para la instalación de Kaspersky Embedded Systems Security para Windows, deberá seleccionar el método de instalación de la aplicación.

Seleccione el método de instalación en función de la arquitectura de la red y de las siguientes condiciones:

- Si necesita configuraciones de instalación de Kaspersky Embedded Systems Security para Windows especiales o la configuración de instalación recomendada.

- Si la configuración de instalación será la misma para todos los dispositivos protegidos o específica para cada dispositivo protegido.

Se puede instalar Kaspersky Embedded Systems Security para Windows de forma interactiva con el asistente de instalación o en modo silencioso sin la intervención del usuario, y se puede invocar mediante la ejecución del archivo del paquete de instalación con las opciones de instalación desde la línea de comandos. Puede instalar Kaspersky Embedded Systems Security para Windows de forma remota y centralizada mediante las políticas de grupo de Active Directory o ejecutando la tarea de instalación remota de Kaspersky Security Center.

Puede instalar y configurar Kaspersky Embedded Systems Security para Windows en un solo dispositivo protegido y guardar sus valores de configuración en un archivo de configuración; en el futuro puede usar el archivo creado para instalar Kaspersky Embedded Systems Security para Windows en otros dispositivos protegidos. Tenga en cuenta que esta capacidad no existe cuando la aplicación se instala mediante las directivas del grupo de Active Directory.

Inicio del asistente de instalación

El asistente de instalación puede instalar los siguientes elementos:

- Los componentes de Kaspersky Embedded Systems Security para Windows en un dispositivo protegido, desde el archivo \exec\setup.exe incluido en el kit de distribución.
- La Consola de Kaspersky Embedded Systems Security para Windows desde el archivo \console\setup.exe del kit de distribución en el dispositivo protegido u otro host LAN.

Ejecución del archivo del paquete de instalación desde la línea de comandos con la configuración de instalación requerida

Si el archivo del paquete de instalación se inicia sin opciones de línea de comandos, Kaspersky Embedded Systems Security para Windows se instalará con la configuración predeterminada. Las opciones de Kaspersky Embedded Systems Security para Windows pueden utilizarse para modificar la configuración de instalación.

La Consola de la aplicación puede instalarse en el dispositivo protegido y/o en la estación de trabajo del administrador.

También puede utilizar comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security para Windows y la Consola de la aplicación.

Instalación centralizada mediante Kaspersky Security Center

Si su red utiliza Kaspersky Security Center para administrar la protección antivirus de los dispositivos en red, Kaspersky Embedded Systems Security para Windows puede instalarse en varios dispositivos ejecutando la tarea de instalación remota.

Los dispositivos protegidos en los que quiera instalar Kaspersky Embedded Systems Security para Windows mediante Kaspersky Security Center pueden encontrarse en el mismo dominio que Kaspersky Security Center, en otro dominio o no pertenecer a ninguno.

Instalación centralizada a partir de directivas de grupo de Active Directory

Las políticas de grupo de Active Directory pueden utilizarse para instalar Kaspersky Embedded Systems Security para Windows en un dispositivo protegido. La Consola de la aplicación puede instalarse en el dispositivo protegido o en la estación de trabajo del administrador.

Kaspersky Embedded Systems Security para Windows puede instalarse utilizando la configuración de instalación recomendada.

Los dispositivos protegidos en los cuales se instala Kaspersky Embedded Systems Security para Windows mediante directivas de grupo de Active Directory deben estar ubicados en el mismo dominio y en la misma unidad organizacional. La instalación se lleva a cabo al iniciar el dispositivo protegido, antes de iniciar sesión en Microsoft Windows.

Instalación y desinstalación de la aplicación mediante un asistente

Esta sección describe la instalación y la desinstalación de Kaspersky Embedded Systems Security para Windows y de la Consola de la aplicación por medio del asistente de instalación, y contiene información sobre la configuración adicional de Kaspersky Embedded Systems Security para Windows y acciones a realizar después de la instalación.

Instalación mediante el asistente de instalación

Las siguientes secciones contienen información sobre la instalación de Kaspersky Embedded Systems Security para Windows y la Consola de la aplicación.

Para instalar y utilizar Kaspersky Embedded Systems Security para Windows:

1. Instale Kaspersky Embedded Systems Security para Windows en el dispositivo protegido.
2. Instale la Consola de la aplicación en los dispositivos desde los que administrará Kaspersky Embedded Systems Security para Windows.
3. Si instaló la Consola de la aplicación en un dispositivo de la red que no es el dispositivo protegido, realice las acciones de configuración necesarias para permitir que los usuarios de la Consola de la aplicación administren Kaspersky Embedded Systems Security para Windows de forma remota.
4. Realice acciones después de la instalación de Kaspersky Embedded Systems Security para Windows.

Instalación de Kaspersky Embedded Systems Security para Windows

Antes de instalar Kaspersky Embedded Systems Security para Windows, realice lo siguiente:

1. Asegúrese de que no haya otros programas antivirus instalados en el dispositivo protegido.
2. Asegúrese de que la cuenta con la que planee ejecutar el asistente de instalación pertenezca al grupo de administradores del dispositivo protegido.

Después de completar las acciones descritas anteriormente, continúe con el procedimiento de instalación. Siga las indicaciones del asistente de instalación, especifique la configuración para la instalación de Kaspersky Embedded Systems Security para Windows. Puede detener el proceso de instalación de Kaspersky Embedded Systems Security para Windows en cualquier paso del asistente de instalación. Para ello, haga clic en el botón **Cancelar** que se encuentra en la ventana del asistente de instalación.

Puede leer más sobre la configuración de instalación (desinstalación).

Para instalar Kaspersky Embedded Systems Security para Windows mediante el asistente de instalación:

1. Ejecute el archivo setupui.exe en el dispositivo protegido.
2. En la ventana que se abre, en la sección **Instalación**, haga clic en el vínculo **Proteger el equipo con la tecnología de denegación predeterminada** o **Proteger el equipo con bases antivirus**.

Cuando se selecciona la configuración "Proteger el equipo con bases antivirus", de manera predeterminada, se incluyen todos los componentes de Kaspersky Embedded Systems Security para Windows, excepto los componentes Administración de firewall y Contadores de rendimiento.

Cuando se instala la configuración "Proteger el equipo con bases antivirus" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que no depende del análisis de firmas y el uso de bases de datos antivirus para proteger el equipo, el conjunto de componentes de la aplicación se amplía y se complementa automáticamente con los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido
- Protección contra amenazas de red

Los componentes que permiten las actualizaciones no están incluidos en la configuración Proteger el equipo con la tecnología de denegación predeterminada.

Si se selecciona la configuración Proteger el equipo con la tecnología de denegación predeterminada, los siguientes componentes se incluyen de manera predeterminada:

- Core
- Prevención de exploits
- Control de inicio de aplicaciones
- Icono de la bandeja del sistema

Cuando se instala la configuración "Proteger el equipo con la tecnología de denegación predeteterminada" de Kaspersky Embedded Systems Security para Windows sobre una versión de la aplicación que protege el equipo a través del análisis de firmas y el uso de bases de datos antivirus, el conjunto de componentes de la aplicación se reduce automáticamente, pues se eliminan los siguientes componentes:

- Protección de archivos en tiempo real
- Análisis a pedido
- los componentes que permiten actualizaciones

Esta configuración se recomienda para proteger dispositivos con recursos limitados. En este caso, puede activar la aplicación a largo plazo y el componente Control de inicio de aplicaciones proporciona protección al equipo.

3. En la pantalla bienvenida del Asistente de instalación de Kaspersky Embedded Systems Security para Windows, haga clic en el botón **Siguiente**.

   Se abre la ventana **Contrato de licencia de usuario final y Política de privacidad**.

4. Revise los términos del Contrato de licencia y la Política de privacidad.

5. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las casillas de verificación **Confirmo que he leído, entendido y que acepto en su totalidad los términos y condiciones de este Contrato de licencia de usuario final** y **Soy consciente y acepto que mis datos sean tratados y transmitidos (incluso a otros países) tal y como se describe en la Política de**

privacidad. Confirmo que he leído y entendido en su totalidad la Política de privacidad para continuar con la instalación.

Si no acepta el Contrato de licencia de usuario final y/o la Política de privacidad, la instalación se cancelará.

6. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Instalación personalizada**.

7. Seleccione los componentes que quiera instalar.

   El componente Compatibilidad con Protocolo SNMP de Kaspersky Embedded Systems Security para Windows solo aparece en la lista de componentes que se sugiere instalar si el servicio Microsoft Windows SNMP está instalado en el dispositivo protegido.

8. Para cancelar todos los cambios, haga clic en el botón **Instalación personalizada** en la ventana **Restablecer**. Haga clic en el botón **Siguiente**.

9. En la ventana **Seleccione una carpeta de destino**:

   - Si es necesario, especifique una carpeta en la cual se copiarán los archivos de Kaspersky Embedded Systems Security para Windows.
   - Si fuera necesario, revise la información sobre el espacio disponible en las unidades locales, haciendo clic en el botón **Disco**.

   Haga clic en el botón **Siguiente**.

10. En la ventana **Configuración avanzada de instalación**, configure las siguientes opciones de instalación:

    - **Habilitar Protección de archivos en tiempo real después de instalar la aplicación (recomendado)**
    - **Agregar archivos recomendados por Microsoft a la lista de exclusiones**
    - **Agregar archivos recomendados por Kaspersky a la lista de exclusiones**

      Haga clic en el botón **Siguiente**.

11. En la ventana **Importar opciones de configuración del archivo de configuración**:

    a. Especifique el archivo de configuración para importar Kaspersky Embedded Systems Security para Windows de un archivo de configuración existente creado en cualquier versión anterior de la aplicación.

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

12. En la ventana **Activación de la aplicación**, realice una de las siguientes acciones:

    - Si desea activar la aplicación, especifique un archivo de clave de Kaspersky Embedded Systems Security para Windows.
    - Si desea activar la aplicación más adelante, haga clic en el botón **Siguiente**.
    - Si se guardó previamente un archivo de clave en la carpeta \exec del kit de distribución, el nombre del archivo aparecerá en el campo **Clave**.

Para agregar una clave usando un archivo de clave guardado en otra carpeta, especifique el archivo.

Una vez que se agrega el archivo de clave, la información sobre la licencia se mostrará en la ventana. Kaspersky Embedded Systems Security para Windows muestra la fecha de caducidad calculada de la licencia. El periodo de la licencia entra en vigor en el momento en que se agrega una clave y caduca antes de la fecha de caducidad del archivo de clave.

Haga clic en el botón **Siguiente** para ingresar el archivo de clave en la aplicación.

13. En la ventana **Listo para instalar**, haga clic en el botón **Instalar**. El asistente comenzará con la instalación de los componentes de Kaspersky Embedded Systems Security para Windows.

14. Una vez que termine la instalación, se abrirá la ventana **Instalación finalizada**.

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

Se cierra el asistente de instalación. Una vez finalizada la instalación, ya podrá utilizar Kaspersky Embedded Systems Security para Windows si ha agregado la clave de activación.

Instalación de la Consola de Kaspersky Embedded Systems Security para Windows

Siga las instrucciones del asistente de instalación para configurar las opciones de instalación para la instalación de la Consola de la aplicación. Puede detener el proceso de instalación de Virus en cualquier paso del asistente de instalación. Para ello, haga clic en el botón **Cancelar** que se encuentra en la ventana del asistente de instalación.

Para instalar la Consola de la aplicación:

1. Asegúrese de que la cuenta que utiliza para ejecutar el asistente de instalación pertenezca al grupo de administradores del dispositivo.

2. Ejecute el archivo setupui.exe en el dispositivo protegido.

   Se abre la ventana de bienvenida.

3. Haga clic en el vínculo **Instalar la Consola de Kaspersky Embedded Systems Security para Windows**.

   Se abre la ventana de bienvenida del asistente de instalación.

4. Haga clic en el botón **Siguiente**.

5. En la ventana que se abre, revise los términos del Contrato de licencia de usuario final y la Política de privacidad, y seleccione las casillas de verificación debajo del texto **Confirmo que he leído, entendido y que acepto en su totalidad los términos y condiciones de este Contrato de licencia de usuario final** para continuar con la instalación.

6. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración avanzada de instalación**.

7. En la ventana **Configuración avanzada de instalación**:

   - Si tiene pensado utilizar la Consola de la aplicación para administrar una instancia de Kaspersky Embedded Systems Security para Windows instalada en un dispositivo remoto, marque la casilla de verificación **Permitir el acceso remoto**.

- Para abrir la **Instalación personalizada** y seleccionar componentes:

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

  Se abre la ventana **Instalación personalizada**.

  b. Seleccione los componentes de las "Herramientas de administración" en la lista.

  De forma predeterminada, se instalan todos los componentes.

  c. Haga clic en el botón **Siguiente**.

Puede encontrar más información sobre los componentes de Kaspersky Embedded Systems Security para Windows.

8. En la ventana **Seleccione una carpeta de destino**:

   a. Si lo necesita, puede indicar otra carpeta en la que se guardarán los archivos de instalación.

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

9. En la ventana **Listo para instalar**, haga clic en el botón **Instalar**.

   El asistente comenzará a instalar los componentes seleccionados.

10. Haga clic en el botón **Finalizar**.

Se cierra el asistente de instalación. La Consola de la aplicación se instalará en el dispositivo protegido.

Si instaló las Herramientas de administración en un dispositivo de la red que no sea el protegido, configure los ajustes avanzados.

Configuración avanzada después de la instalación de la Consola de la aplicación en otro dispositivo

Si la Consola de la aplicación se instaló en cualquier dispositivo de la red que no sea el dispositivo protegido, realice las siguientes acciones para que los usuarios pueden administrar Kaspersky Embedded Systems Security para Windows de forma remota:

- Agregar usuarios de Kaspersky Embedded Systems Security para Windows al grupo de administración de ESS en el dispositivo protegido.
- Habilite las conexiones de red para el servicio de Kaspersky Security Management (kavfsgt.exe) si el dispositivo protegido usa el firewall de Windows o de un tercero.
- Si no se seleccionó la casilla **Permitir el acceso remoto** durante la instalación de la Consola de la aplicación en un dispositivo que ejecuta Microsoft Windows, permita manualmente conexiones de red para la Consola de la aplicación mediante el firewall del dispositivo.

La Consola de la aplicación en el dispositivo remoto utiliza el protocolo DCOM para recibir información sobre eventos de Kaspersky Embedded Systems Security para Windows (objetos analizados, tareas finalizadas, etc.) del servicio de Kaspersky Security Management en el dispositivo protegido. Debe permitir conexiones de red para la Consola de la aplicación en la configuración de Firewall de Windows para establecer conexiones entre la Consola de la aplicación y el servicio de Kaspersky Security Management.

En el dispositivo remoto, donde está instalada la Consola de la aplicación, haga lo siguiente:

- Asegúrese de que esté permitido el acceso remoto anónimo a las aplicaciones COM (pero no el inicio y la activación remotos de las aplicaciones COM).
- En el Firewall de Windows, abra el puerto TCP 135 y permita las conexiones de red para kavfsrcn.exe, el archivo ejecutable del proceso de administración remota de Kaspersky Embedded Systems Security para Windows.

  El dispositivo en el que está instalada la Consola de la aplicación utiliza el puerto TCP 135 para acceder al dispositivo protegido y recibir una respuesta.
- Configure una regla saliente para el Firewall de Windows para permitir la conexión.

  A diferencia de los servicios de TCP/IP y UDP/IP tradicionales, donde un único protocolo tiene un puerto fijo, DCOM asigna dinámicamente puertos para los objetos COM remotos. Si existe un firewall entre el cliente (donde está instalada la Consola de la aplicación) y el terminal DCOM (el dispositivo protegido), debe abrirse un intervalo grande de puertos.

Los mismos pasos deben aplicarse para configurar cualquier otro firewall de software o hardware.

Si la Consola de la aplicación está abierta mientras usted configura la conexión entre el dispositivo protegido y el dispositivo en el cual está instalada la Consola de la aplicación:

1. Cierre la consola de la aplicación.
2. Espere hasta que finalice el proceso de administración remota kavfsrcn.exe de Kaspersky Embedded Systems Security para Windows.
3. Reinicie la consola de la aplicación.

   Se aplicará la nueva configuración de conexión.

Permiso de acceso remoto anónimo a las aplicaciones COM

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Para permitir el acceso remoto anónimo a las aplicaciones COM:

1. En el dispositivo remoto donde se encuentra instalada la Consola de Kaspersky Embedded Systems Security para Windows, abra la consola de Servicios de componentes.
2. Seleccione **Iniciar** → **Ejecutar**.
3. Escriba el comando `dcomcnfg`.
4. Haga clic en el botón **Aceptar**.
5. Amplíe el nodo **Equipos** en la consola de **Servicios de componentes** en su dispositivo protegido.
6. Abra el menú contextual en el nodo **Mi equipo**.
7. Seleccione **Propiedades**.

8. En la pestaña **Seguridad COM** de la ventana **Propiedades**, haga clic en el botón **Editar límites** ubicado en el grupo de opciones de configuración **Permisos de acceso**.

9. Asegúrese de que la casilla de verificación **Permitir el acceso remoto** esté activada para el usuario con INICIO DE SESIÓN ANÓNIMO en la ventana **Permitir el acceso remoto**.

10. Haga clic en el botón **Aceptar**.

Permiso de conexión de red para el proceso de administración remota de Kaspersky Embedded Systems Security para Windows

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Para abrir el puerto TCP 135 en el firewall de Windows y permitir conexiones de red para el proceso de administración remota de Kaspersky Embedded Systems Security para Windows:

1. Cierre la Consola de Kaspersky Embedded Systems Security para Windows en el dispositivo remoto.

2. Realice una de las siguientes opciones:

   - En Microsoft Windows XP SP2 o una versión posterior:

     a. Seleccione **Inicio** > **Firewall de Windows**.

     b. En la ventana **Firewall de Windows** (o Configuración de Firewall de Windows), haga clic en el botón **Agregar puerto** en la pestaña **Exclusiones**.

     c. En el campo **Nombre**, especifique el nombre del puerto RPC (TCP/135) o introduzca otro nombre, por ejemplo, DCOM de Kaspersky Embedded Systems Security para Windows, y especifique el número de puerto (135) en el campo **Nombre de puerto**.

     d. Seleccione el protocolo **TCP**.

     e. Haga clic en el botón **Aceptar**.

     f. Presione el botón **Agregar** en la pestaña **Exclusiones**.

   - En Microsoft Windows 7 o una versión posterior:

     a. Seleccione **Inicio** > **Panel de control** > **Firewall de Windows**.

     b. En la ventana **Firewall de Windows**, seleccione **Permitir un programa o una característica a través de Firewall de Windows**.

     c. En la ventana **Permitir que programas se comuniquen a través de Firewall de Windows**, haga clic en el botón **Permitir otro programa**.

3. Especifique el archivo kavfsrcn.exe en la ventana **Agregar programa**. Está ubicado en la carpeta de destino especificada durante la instalación de la Consola de Kaspersky Embedded Systems Security para Windows mediante Microsoft Management Console.

4. Haga clic en el botón **Aceptar**.

5. Haga clic en el botón **Aceptar** en la ventana Firewall de Windows (**Configuración de Firewall de Windows**).

Agregado de la regla saliente para el Firewall de Windows

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Para agregar la regla saliente para el Firewall de Windows:

1. Seleccione **Inicio** > **Panel de control** > **Firewall de Windows**.
2. En la ventana **Firewall de Windows**, haga clic en el vínculo **Configuración avanzada**.

   Se abre la ventana **Firewall de Windows con seguridad avanzada**.
3. Seleccione el nodo secundario **Reglas salientes**.
4. Haga clic en la opción **Nueva regla** en el panel **Acciones**.
5. En la ventana **Asistente para nueva regla de salida** que se abre, seleccione la opción **Puerto** y haga clic en **Siguiente**.
6. Seleccione el protocolo **TCP**.
7. En el campo **Puertos remotos específicos**, especifique el siguiente intervalo de puertos para permitir conexiones salientes: 1024-65535.
8. En la ventana **Acción**, seleccione la opción **Permitir la conexión**.
9. Guarde la nueva regla y cierre la ventana **Firewall de Windows con seguridad avanzada**.

Ahora el firewall de Windows permitirá conexiones de red entre la Consola de la aplicación y el servicio de Kaspersky Security Management.

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows inicia la protección y las tareas de análisis inmediatamente después de la instalación si ha activado la aplicación. Si se selecciona **Habilitar Protección de archivos en tiempo real después de instalar la aplicación (recomendado)** (opción predeterminada) durante la instalación de Kaspersky Embedded Systems Security para Windows, la aplicación analizará los objetos del sistema de archivos del dispositivo cuando acceda a ellos. Kaspersky Embedded Systems Security para Windows ejecutará la tarea Análisis de áreas críticas todos los viernes a las 8:00 p. m.

Le recomendamos realizar los siguientes pasos después de instalar Kaspersky Embedded Systems Security:

- Inicie la tarea de actualización de bases de datos de la aplicación. Después de la instalación, Kaspersky Embedded Systems Security para Windows analizará los objetos con la base de datos incluida en el kit de distribución de la aplicación.

Recomendamos actualizar las bases de datos de Kaspersky Embedded Systems Security para Windows inmediatamente, ya que pueden estar desactualizadas.

La aplicación actualizará la base de datos a cada hora, de acuerdo con la programación predeterminada de la tarea.

- Realice un Análisis de áreas críticas del dispositivo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el dispositivo antes de la instalación de Kaspersky Embedded Systems Security para Windows.
- Configure las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security para Windows.

Inicio y configuración de la tarea de Actualización de bases de datos de Kaspersky Embedded Systems Security para Windows

Para actualizar la base de datos de la aplicación después de la instalación:

1. En la configuración de la tarea Actualización de bases de datos, configure una conexión con el origen de actualizaciones a través de los servidores de actualizaciones FTP o HTTP de Kaspersky.
2. Inicie la tarea Actualización de bases de datos.

El Protocolo de autodescubrimiento de Proxy Web (WPAD) no se puede configurar en su red para detectar la configuración del servidor proxy automáticamente en la red de área local. En eso, su red puede requerir la autenticación al acceder al servidor proxy.

Para especificar la configuración del servidor proxy opcional y la configuración de autenticación para acceder al servidor proxy:

1. Abra el menú contextual en el nodo **Kaspersky Embedded Systems Security para Windows**.
2. Seleccione **Propiedades**.

   Se muestra la ventana **Configuración de la aplicación**.
3. Seleccione la pestaña **Configuración de conexión**.
4. En la sección **Configuración del servidor proxy**, seleccione la casilla **Usar el servidor proxy especificado**.
5. Ingrese la dirección del servidor proxy en el campo **Dirección** e ingrese el número de puerto para el servidor proxy en el campo **Puerto**.
6. En la sección **Configuración de autenticación del servidor proxy**, seleccione el método de autenticación necesario en la lista desplegable:

   - **Usar autenticación NTLM** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security para Windows utilizará la cuenta especificada en la configuración de la tarea para acceder al servidor proxy. De forma predeterminada, la tarea se inicia con la cuenta **Sistema local** (**SYSTEM**).

- **Usar autenticación NTLM con nombre de usuario y contraseña** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security para Windows utilizará la cuenta especificada para acceder al servidor proxy. Introduzca un nombre de usuario y contraseña o seleccione un usuario de la lista.

- **Aplicar nombre de usuario y contraseña** para seleccionar la autenticación básica. Introduzca un nombre de usuario y contraseña o seleccione un usuario de la lista.

7. Haga clic en el botón **Aceptar** en la ventana **Configuración de la aplicación**.

Para configurar la conexión con los servidores de actualizaciones de Kaspersky, en la tarea Actualización de bases de datos:

1. Inicie la Consola de la aplicación de una de las siguientes maneras:

   - Abrir la Consola de la aplicación en el dispositivo protegido. Para ello, seleccione **Inicio** > **Todos los programas** > **Kaspersky Embedded Systems Security para Windows** > **Herramientas de administración** > **Consola de Kaspersky Embedded Systems Security 3.3 para Windows**.

   - Si la Consola de la aplicación se inició en cualquier dispositivo que no sea el protegido, conéctela al dispositivo:

     a. Abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows** en el árbol de la Consola de la aplicación.

     b. Seleccione el elemento **Conectarse a otro equipo**.

     c. En el cuadro de diálogo **Seleccionar dispositivo protegido**, seleccione **Otro dispositivo** y, en el campo de texto, indique el nombre de red del dispositivo protegido.

     Si la cuenta que usaba para iniciar sesión en Microsoft Windows no tiene permisos de acceso para el servicio de Kaspersky Security Management, indique una cuenta que tenga estos permisos.

   Se abre la ventana Consola de la aplicación.

2. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.

3. Seleccione el nodo secundario **Actualización de bases de datos**.

4. Haga clic en el vínculo **Propiedades** del panel de resultados.

5. En la ventana **Configuración de tareas** que se abre, abra la pestaña **Configuración de conexión**.

6. Seleccione **Usar la configuración del servidor proxy para conectarse a los servidores de actualizaciones de Kaspersky**.

7. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guardará la configuración para establecer conexión con el origen de actualizaciones en la tarea Actualización de bases de datos.

Para ejecutar la tarea de Actualización de bases de datos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.

2. En el menú contextual del nodo secundario **Actualización de bases de datos**, seleccione el elemento **Iniciar**.

   Iniciará la tarea Actualización de bases de datos.

   Una vez que la tarea haya finalizado correctamente, podrá ver la fecha de lanzamiento de las últimas actualizaciones de bases de datos instaladas en el panel de resultados del nodo **Kaspersky Embedded Systems Security para Windows**.

Análisis de áreas críticas

Después de actualizar las bases de datos de Kaspersky Embedded Systems Security para Windows, analice el dispositivo protegido en busca de malware con la tarea Análisis de áreas críticas.

Para ejecutar la tarea Análisis de áreas críticas.

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.

2. En el menú contextual del nodo secundario **Análisis de áreas críticas**, seleccione el comando **Iniciar**.

Cuando inicie la tarea, el panel de resultados mostrará el estado de tarea **En ejecución**.

Para ver el registro de tareas,

En el panel de resultados del nodo **Análisis de áreas críticas**, haga clic en el vínculo **Abrir el registro de tareas**.

Modificación del conjunto de componentes y reparación de Kaspersky Embedded Systems Security para Windows

Puede agregar o quitar los componentes de Kaspersky Embedded Systems Security para Windows. Debe detener la tarea de Protección de archivos en tiempo real antes de poder eliminar el componente de Protección de archivos en tiempo real. En otros casos, no es necesario detener la protección de archivos en tiempo real ni el servicio de Kaspersky Security.

Si la administración de la aplicación está protegida con contraseña, Kaspersky Embedded Systems Security para Windows solicita la contraseña cuando intenta quitar componentes o modificar el conjunto de componentes en el asistente de instalación.

Para modificar el conjunto de componentes de Kaspersky Embedded Systems Security para Windows:

1. En el menú **Iniciar**, seleccione **Todos los programas** > **Kaspersky Embedded Systems Security para Windows** > **Modificar o eliminar Kaspersky Embedded Systems Security para Windows**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.

2. Seleccione **Modificar conjunto de componentes**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Instalación personalizada**.

3. En la ventana de **Instalación personalizada**, en la lista de componentes disponibles, seleccione los componentes que desea agregar o quitar de Kaspersky Embedded Systems Security para Windows. Para ello, realice las siguientes acciones:

- Para cambiar el conjunto de componentes, haga clic en el botón situado junto al nombre del componente seleccionado. Luego, en el menú contextual, seleccione:
  - **El componente se instalará en el disco duro local** si desea instalar un componente.
  - **El componente y sus subcomponentes se instalarán en el disco duro local** si desea instalar un grupo de componentes.
- Para eliminar los componentes instalados previamente, haga clic en el botón situado junto al nombre del componente seleccionado. A continuación, en el menú contextual, seleccione **El componente no estará disponible**.

Haga clic en el botón **Siguiente**.

4. En la ventana **Listo para instalar**, confirme los cambios en el conjunto de componentes haciendo clic en el botón **Instalar**.
5. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la instalación.

El conjunto de componentes de Kaspersky Embedded Systems Security para Windows se modificará según la configuración especificada.

Si el funcionamiento de Kaspersky Embedded Systems Security presenta problemas (Kaspersky Embedded Systems Security deja de funcionar, las tareas dejan de funcionar o no se inician), puede reparar Kaspersky Embedded Systems Security. Puede realizar una reparación y guardar la configuración actual de Kaspersky Embedded Systems Security para Windows, o puede seleccionar una opción para restablecer toda la configuración de Kaspersky Embedded Systems Security para Windows a sus valores predeterminados.

Para reparar Kaspersky Embedded Systems Security para Windows después de que la aplicación o una tarea deje de funcionar:

1. En el menú **Iniciar**, seleccione **Todos los programas**.
2. Seleccione **Kaspersky Embedded Systems Security para Windows**.
3. Seleccione **Modificar o eliminar Kaspersky Embedded Systems Security para Windows**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.
4. Seleccione **Reparar componentes instalados**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Reparar componentes instalados**.
5. En la ventana **Reparar componentes instalados**, seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación** si desea restablecer las opciones de la aplicación y restaurar Kaspersky Embedded Systems Security para Windows con su configuración predeterminada. Haga clic en el botón **Siguiente**.
6. En la ventana **Listo para reparar**, confirme la operación de reparación haciendo clic en el botón **Instalar**.
7. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la operación de reparación.

Kaspersky Embedded Systems Security para Windows se reparará utilizando la configuración especificada.

Desinstalación mediante el asistente de instalación

Esta sección contiene instrucciones sobre cómo desinstalar Kaspersky Embedded Systems Security para Windows y la Consola de la aplicación de un dispositivo protegido con el Asistente de instalación/desinstalación.

Desinstalación de Kaspersky Embedded Systems Security para Windows

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security para Windows. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Kaspersky Embedded Systems Security para Windows puede desinstalarse del dispositivo protegido con el asistente de instalación/desinstalación.

Después de desinstalar Kaspersky Embedded Systems Security para Windows de un dispositivo protegido, es posible que deba reiniciarlo. El reinicio se puede posponer.

Las opciones de desinstalación, reparación e instalación de la aplicación mediante el panel de control de Windows no están disponibles si el sistema operativo usa la función de UAC (Control de la cuenta de usuario) o el acceso a la aplicación está protegido por contraseña.

Si la administración de la aplicación está protegida con contraseña, Kaspersky Embedded Systems Security para Windows solicita la contraseña cuando intenta quitar componentes o modificar el conjunto de componentes en el asistente de instalación.

Para desinstalar Kaspersky Embedded Systems Security para Windows.

1. En el menú **Iniciar**, seleccione **Todos los programas**.
2. Seleccione **Kaspersky Embedded Systems Security para Windows**.
3. Seleccione **Modificar o eliminar Kaspersky Embedded Systems Security para Windows**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.
4. Seleccione **Eliminar componentes de software**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración avanzada de desinstalación de la aplicación**.
5. Si es necesario, en la ventana **Configuración avanzada de desinstalación de la aplicación**:

   a. Seleccione la casilla de verificación **Exportar objetos de Cuarentena** para exportar los objetos en cuarentena de Kaspersky Embedded Systems Security para Windows. De forma predeterminada, la casilla no está activada.

   b. Seleccione la casilla de verificación **Exportar objetos de Copia de seguridad** para exportar los objetos de la Copia de seguridad de Kaspersky Embedded Systems Security para Windows. De forma predeterminada, la casilla no está activada.

c. Haga clic en el botón **Guardar en** y seleccione la carpeta a la cual desea exportar los objetos. De forma predeterminada, los objetos se exportarán a %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

Haga clic en el botón **Siguiente**.

6. En la ventana **Listo para desinstalar**, confirme la desinstalación haciendo clic en el botón **Desinstalar**.
7. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la desinstalación.

Kaspersky Embedded Systems Security para Windows se desinstalará del dispositivo protegido.

Desinstalación de la Consola de Kaspersky Embedded Systems Security para Windows

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Puede desinstalar la Consola de la aplicación del dispositivo protegido con el asistente de instalación/desinstalación.

Después de desinstalar la Consola de la aplicación, no es necesario reiniciar el dispositivo protegido.

Para desinstalar la Consola de la aplicación:

1. En el menú **Iniciar**, seleccione **Todos los programas**.
2. Seleccione **Kaspersky Embedded Systems Security para Windows**.
3. Seleccione **Modificar o eliminar Kaspersky Embedded Systems Security para Windows**.

   Se abrirá la ventana **Reparar o eliminar la instalación** del asistente.
4. Seleccione **Eliminar componentes de software** y haga clic en el botón **Siguiente**.
5. Se abre la ventana **Listo para desinstalar**. Haga clic en el botón **Desinstalar**.

   Se abre la ventana **Desinstalación finalizada**.
6. Haga clic en el botón **Aceptar**.

Una vez que termine la desinstalación, la ventana del asistente de instalación se cerrará.

Instalación y desinstalación de la aplicación desde la línea de comandos

Esta sección indica cómo instalar y desinstalar Kaspersky Embedded Systems Security para Windows desde la línea de comandos y contiene ejemplos de comandos para realizar dichas acciones, así como ejemplos de comandos para agregar y quitar componentes de Kaspersky Embedded Systems Security para Windows desde la línea de comandos.

Acerca de la instalación y desinstalación de Kaspersky Embedded Systems Security para Windows desde la línea de comandos

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security para Windows. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Para instalar o desinstalar Kaspersky Embedded Systems Security para Windows y agregar o eliminar sus componentes, puede ejecutar los archivos de paquete de instalación \exec\ess_x86.msi o \exec\ess_x64.msi desde la línea de comandos, tras especificar los parámetros de instalación con las respectivas opciones en la línea de comandos.

El conjunto de "Herramientas de administración" puede instalarse en el dispositivo protegido o en otro dispositivo de la red y hacer que trabaje con la Consola de la aplicación de forma local o remota. Para ello, utilice el paquete de instalación \console\esstools.msi.

Lleve a cabo la instalación usando una cuenta incluida en el grupo de administradores del dispositivo protegido en el que se instalará la aplicación.

Si ejecuta los archivos \exec\ess_x86.msi o \exec\ess_x64.msi en el dispositivo protegido sin especificar ninguna opción adicional en la línea de comandos, Kaspersky Embedded Systems Security para Windows se instalará con los parámetros de instalación predeterminados.

Puede asignar el conjunto de componentes que se instalará con la opción de la línea de comandos ADDLOCAL y enumerando los códigos de los componentes o conjuntos de componentes seleccionados.

Comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security para Windows

Esta sección presenta ejemplos de comandos utilizados para instalar Kaspersky Embedded Systems Security para Windows.

En dispositivos protegidos con Microsoft Windows de 32 bits, ejecute los archivos con el sufijo x86 del kit de distribución. En dispositivos protegidos con Microsoft Windows de 64 bits, ejecute los archivos con el sufijo x64 del kit de distribución.

La información detallada sobre el uso de comandos estándares de Windows Installer y opciones de la línea de comandos se proporciona en la documentación suministrada por Microsoft.

Ejemplos de la instalación de Kaspersky Embedded Systems Security para Windows desde el archivo setup.exe

Para instalar Kaspersky Embedded Systems Security para Windows con la configuración de instalación recomendada sin intervención del usuario, ejecute el siguiente comando:

```
\exec\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1
```

Puede instalar Kaspersky Embedded Systems Security para Windows con la siguiente configuración:

- Instalar solo los componentes Protección de archivos en tiempo real y Análisis a pedido.
- No ejecutar la función de Protección de archivos en tiempo real al iniciar Kaspersky Embedded Systems Security para Windows.
- No excluir archivos que Microsoft Corporation recomienda excluir del área de análisis.

Para instalar componentes como Control de dispositivos, ejecute el siguiente comando:

```
\exec\setup.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

Si necesita instalar Kaspersky Embedded Systems Security para Windows en un equipo con dispositivos de red o dispositivos SCSI que ocasionan un bloqueo del sistema tras la instalación de Kaspersky Embedded Systems Security para Windows, puede usar las siguientes opciones adicionales con este comando:

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

Habilita (1) o deshabilita (0) la interceptación de conexiones de adaptadores de red.

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

Habilita (1) o deshabilita (0) la interceptación de conexiones de adaptadores SCSI.

Lista de comandos que se utilizan en la instalación: ejecutar un archivo .msi

Para instalar Kaspersky Embedded Systems Security para Windows con la configuración de instalación recomendada sin intervención del usuario, ejecute el siguiente comando:

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

Para instalar Kaspersky Embedded Systems Security para Windows con los parámetros de instalación recomendados y mostrar la interfaz de instalación, ejecute el siguiente comando:

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

Para instalar Kaspersky Embedded Systems Security para Windows con los parámetros de instalación recomendados y habilitar la rotación de archivos de seguimiento cuando el número de archivos de seguimiento alcance el número máximo especificado, ejecute el siguiente comando:

```
msiexec /i ess.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

El parámetro `TRACE_FOLDER` es obligatorio.

El parámetro `TRACE_MAX_ROLL_COUNT` está sujeto a las siguientes reglas:

- Si especifica este parámetro, se habilitará la rotación de archivos de seguimiento cuando el número de archivos de seguimiento alcance el número máximo definido en el parámetro. Intervalo de valores posible para el parámetro: de 1 a 999.
- Si se indica 0 como número máximo de archivos de seguimiento, la rotación de archivos de seguimiento quedará deshabilitada.
- Si se indica un valor para el parámetro, pero dicho valor no es válido o no pertenece al intervalo de valores posibles (de 1 a 999), se habilitará la rotación de archivos de seguimiento con el número máximo predeterminado (5 archivos de seguimiento).

- Si no se especifica este parámetro, ocurrirá lo siguiente:
  - Si la rotación de archivos de seguimiento ya se encuentra configurada en el dispositivo, la configuración no se modificará. La aplicación ignorará los parámetros ingresados.
  - Si la rotación de archivos de seguimiento no está configurada en el dispositivo, se habilitará la opción de rotación con el número máximo predeterminado (5 archivos de seguimiento).

Para instalar y activar Kaspersky Embedded Systems Security para Windows utilizando el archivo de clave C:\0000000A.key:

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

Para instalar Kaspersky Embedded Systems Security para Windows con un análisis preliminar de los procesos activos y los sectores de inicio de los discos locales, ejecute el siguiente comando:

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

Para instalar Kaspersky Embedded Systems Security para Windows en la carpeta de instalación C:\ESS, ejecute el siguiente comando:

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

Para instalar Kaspersky Embedded Systems Security para Windows y guardar un archivo de registro de instalación con el nombre ess.log en la carpeta donde se encuentra el archivo msi de Kaspersky Embedded Systems Security para Windows, ejecute el siguiente comando:

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

Para instalar la Consola de Kaspersky Embedded Systems Security para Windows, ejecute el siguiente comando:

```
msiexec /i esstools.msi /qn EULA=1
```

Para instalar y activar Kaspersky Embedded Systems Security para Windows utilizando el archivo de clave C:\0000000A.key y configurar Kaspersky Embedded Systems Security para Windows según los ajustes del archivo de configuración C:\settings.xml, ejecute el siguiente comando:

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1
PRIVACYPOLICY=1
```

Para instalar un parche de la aplicación cuando Kaspersky Embedded Systems Security para Windows está protegido con contraseña, ejecute el siguiente comando:

```
msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
```

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows inicia la protección y las tareas de análisis inmediatamente después de la instalación si ha activado la aplicación. Si selecciona la opción **Habilitar Protección de archivos en tiempo real después de instalar la aplicación (recomendado)** durante la instalación de Kaspersky Embedded Systems Security, la aplicación analizará los objetos del sistema de archivos del dispositivo cuando acceda a ellos. Kaspersky Embedded Systems Security para Windows ejecutará la tarea Análisis de áreas críticas todos los viernes a las 8:00 p. m.

Le recomendamos realizar los siguientes pasos después de instalar Kaspersky Embedded Systems Security:

- Inicie la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security para Windows. Después de la instalación, Kaspersky Embedded Systems Security para Windows analizará los objetos con la base de datos incluida en el kit de distribución. Le recomendamos que actualice la base de datos de Kaspersky Embedded Systems Security de inmediato. Para ello, debe ejecutar la tarea de Actualización de bases de datos. La base de datos se actualizará cada hora de acuerdo con la programación predeterminada.

  Por ejemplo, puede iniciar la tarea Actualización de bases de datos con el siguiente comando:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
  /PROXYPWD:123456
  ```

  En este caso, las actualizaciones de bases de datos de Kaspersky Embedded Systems Security para Windows se descargan desde los servidores de actualizaciones de Kaspersky. La conexión a un origen de actualizaciones se establece a través de un servidor proxy (dirección del servidor proxy: proxy.company.com, puerto: 8080) y utiliza la autenticación NTLM incorporada de Windows para acceder al servidor con una cuenta (nombre de usuario: inetuser; contraseña: 123456).

- Realice un Análisis de áreas críticas del dispositivo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el dispositivo antes de la instalación de Kaspersky Embedded Systems Security para Windows.

Para iniciar la tarea de Análisis de áreas críticas a través de la línea de comandos:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Este comando guarda el registro de tareas en el archivo scancritical.log disponible en la carpeta actual.

- Configure las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security para Windows.

Cómo agregar o eliminar componentes. Comandos de ejemplo

El componente Control de inicio de aplicaciones se instala automáticamente.

Para instalar el componente Análisis a pedido, ejecute el siguiente comando:

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

o

```
\exec\setup.exe /s /p ADDLOCAL=Oas,Ods
```

Después de agregar los componentes a la lista, Kaspersky Embedded Systems Security reinstala los componentes existentes e instala los componentes especificados.

Para eliminar los componentes instalados, ejecute el siguiente comando:

```
msiexec /i ess.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Para instalar nuevos componentes, ejecute el siguiente comando:

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

Una vez que haya enumerado los componentes que desee instalar y eliminar, Kaspersky Embedded Systems Security para Windows instalará y eliminará los componentes correspondientes.

Desinstalación de Kaspersky Embedded Systems Security para Windows. Comandos de ejemplo

Para desinstalar Kaspersky Embedded Systems Security para Windows desde el dispositivo protegido, ejecute el siguiente comando:

- Para sistemas operativos de 32 bits:
  ```
  msiexec /x ess_x86.msi /qn
  ```
- Para sistemas operativos de 64 bits:
  ```
  msiexec /x ess_x64.msi /qn
  ```

o

- Para sistemas operativos de 32 bits:
  ```
  msiexec /x {263DB314-C453-4539-A5C1-845B542FFDCA} /qn
  ```
- Para sistemas operativos de 64 bits:
  ```
  msiexec /x {429EF48A-879D-428A-BA60-22761417FD8E} /qn
  ```

Para desinstalar la Consola de Kaspersky Embedded Systems Security para Windows, ejecute el siguiente comando:

```
msiexec /x esstools.msi /qn
```

o

```
msiexec /x {4A79347C-BAE9-4A94-BF5D-16CDA5085084} /qn
```

Para desinstalar Kaspersky Embedded Systems Security para Windows de un dispositivo donde esté habilitada la protección con contraseña, ejecute el siguiente comando:

- Para sistemas operativos de 32 bits:
  ```
  msiexec /x {263DB314-C453-4539-A5C1-845B542FFDCA} UNLOCK_PASSWORD=*** /qn
  ```
- Para sistemas operativos de 64 bits:
  ```
  msiexec /x {429EF48A-879D-428A-BA60-22761417FD8E} UNLOCK_PASSWORD=*** /qn
  ```

Códigos de devolución

La siguiente tabla contiene una lista de códigos de devolución de la línea de comandos.

Códigos de devolución

Código	Descripción
1324	El nombre de la carpeta de destino contiene caracteres no válidos.
25001	Derechos insuficientes de instalar Kaspersky Embedded Systems Security para Windows. Para instalar la aplicación, inicie el asistente de instalación con derechos del administrador local.
25003	Kaspersky Embedded Systems Security para Windows no puede instalarse en dispositivos que ejecutan esta versión de Microsoft Windows. Inicie el asistente de instalación para versiones de 64 bits de Microsoft Windows.
25004	Se ha detectado un software incompatible. Para continuar con la instalación, desinstale el siguiente software: <lista de software incompatible>.
25010	La ruta indicada no se puede usar para guardar objetos puestos en cuarentena.
25011	El nombre de la carpeta para guardar objetos en cuarentena contiene caracteres no válidos.
26251	No es posible descargar DLL de contadores de rendimiento.
26252	No es posible descargar DLL de contadores de rendimiento.
27300	El controlador no se puede instalar.
27301	El controlador no se puede desinstalar.
27302	El componente de la red no se puede instalar. Se alcanzó la cantidad máxima admitida de dispositivos filtrados.
27303	Bases de datos antivirus no encontradas.

Instalación y desinstalación de la aplicación mediante Kaspersky Security Center

En esta sección, encontrará información sobre la instalación de Kaspersky Embedded Systems Security para Windows a través de Kaspersky Security Center, una descripción del procedimiento para instalar y desinstalar Kaspersky Embedded Systems Security para Windows a través de Kaspersky Security Center y una descripción de las acciones que se deben realizar cuando concluye la instalación de Kaspersky Embedded Systems Security para Windows.

Información general sobre la instalación mediante Kaspersky Security Center

Puede instalar Kaspersky Embedded Systems Security para Windows a través de Kaspersky Security Center ejecutando la tarea de instalación remota.

Una vez finalizada la tarea de instalación remota, Kaspersky Embedded Systems Security para Windows se instalará con la misma configuración en múltiples dispositivos protegidos.

Todos los dispositivos protegidos pueden combinarse en un solo grupo de administración y se puede crear una tarea de grupo que instale Kaspersky Embedded Systems Security para Windows en los dispositivos protegidos del grupo.

Puede crear una tarea que instale Kaspersky Embedded Systems Security para Windows de forma remota en un grupo de dispositivos protegidos que no pertenecen al mismo grupo de administración. Al crear esta tarea, debe generar una lista de los dispositivos protegidos individuales en los que se debe instalar Kaspersky Embedded Systems Security para Windows.

La información detallada acerca de la tarea de instalación remota está disponible en la *Ayuda de Kaspersky Security Center*.

Derechos para instalar o desinstalar Kaspersky Embedded Systems Security para Windows

La cuenta especificada en la tarea de instalación o desinstalación remota debe pertenecer al grupo de administradores en cada uno de los dispositivos protegidos en todos los casos, excepto en los descritos a continuación:

- Si el Agente de red de Kaspersky Security Center ya está instalado en los dispositivos protegidos en los que se instalará Kaspersky Embedded Systems Security para Windows (independientemente del dominio en que estén los dispositivos protegidos o si pertenecen a alguno).

  Si el Agente de red todavía no está instalado en los dispositivos protegidos, se puede instalar junto con Kaspersky Embedded Systems Security para Windows mediante una tarea de instalación remota. Antes de instalar el Agente de red, asegúrese de que la cuenta que indique en la tarea esté incluida en el grupo de administradores de cada uno de los dispositivos protegidos.

- Todos los dispositivos protegidos en los que desea instalar Kaspersky Embedded Systems Security para Windows pertenecen al mismo dominio que el Servidor de administración, y el Servidor de administración se ha registrado como cuenta de **Administrador de dominio** (si esta cuenta dispone de derechos de administrador local en los dispositivos protegidos incluidos en el dominio).

De manera predeterminada, al usar el método **Instalación forzada**, la tarea de instalación remota se inicia desde la cuenta que ejecuta el servidor de administración.

Al trabajar con tareas de grupo o con tareas para grupos de dispositivos protegidos bajo el modo de instalación/desinstalación forzada, la cuenta debe disponer de los siguientes derechos en el dispositivo protegido:

- Derecho de ejecutar aplicaciones remotamente.
- Derechos sobre el recurso compartido **Admin$**.
- Derecho de **Iniciar sesión como servicio**.

Instalación de Kaspersky Embedded Systems Security para Windows a través de Kaspersky Security Center

La información detallada sobre la generación de un paquete de instalación y la creación de una tarea de instalación remota está disponible en la Guía de implementación de Kaspersky Security Center.

Si tiene pensado administrar Kaspersky Embedded Systems Security para Windows desde Kaspersky Security Center en el futuro, asegúrese de que se cumplan las siguientes condiciones:

- El dispositivo protegido en el que está instalado el Servidor de administración de Kaspersky Security Center también tiene instalado el Complemento de administración (archivo \exec\klcfginst.exe del kit de distribución de Kaspersky Embedded Systems Security para Windows).

- El Agente de red de Kaspersky Security Center está instalado en los dispositivos protegidos. Si el Agente de red de Kaspersky Security Center no está instalado en los dispositivos protegidos, puede instalarlo junto con Kaspersky Embedded Systems Security para Windows mediante una tarea de ejecución remota.

Los dispositivos también pueden combinarse en un grupo de administración para luego administrar la configuración de protección a través de las directivas y tareas de grupo de Kaspersky Security Center.

Para instalar Kaspersky Embedded Systems Security para Windows con la tarea de instalación remota:

1. Inicie la Consola de administración de Kaspersky Security Center.
2. En Kaspersky Security Center, expanda el nodo **Avanzado**.
3. Expanda el nodo secundario **Instalación remota**.
4. En el panel de resultados del nodo secundario **Paquetes de instalación**, haga clic en el botón **Crear paquete de instalación**.
5. Seleccione el tipo de paquete de instalación en **Crear paquete de instalación para una aplicación de Kaspersky**.
6. Ingrese el nombre del nuevo paquete de instalación.
7. Especifique el archivo ess.kud del kit de distribución de Kaspersky Embedded Systems Security para Windows como el archivo del paquete de instalación.

   Se abre la ventana **Contrato de licencia de usuario final y Política de privacidad**.
8. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las casillas de verificación **Confirmo que he leído, entendido y que acepto en su totalidad los términos y condiciones de este Contrato de licencia de usuario final** y **Soy consciente y acepto que mis datos sean tratados y transmitidos (incluso a otros países) tal y como se describe en la Política de privacidad. Confirmo que he leído y entendido en su totalidad la Política de privacidad** para continuar con la instalación.

   Debe aceptar el Contrato de licencia y la Política de privacidad para continuar.
9. Para cambiar el conjunto de componentes de Kaspersky Embedded Systems Security para Windows que se instalarán y las opciones de instalación predeterminadas en el paquete de instalación:

   a. En Kaspersky Security Center, expanda el nodo **Instalación remota**.

   b. En el panel de resultados del nodo secundario **Paquetes de instalación**, abra el menú contextual del paquete de instalación Kaspersky Embedded Systems Security para Windows creado y seleccione **Propiedades**.

   c. En la ventana **Propiedades:<nombre del paquete de instalación>**, abra la sección **Configuración**.

   En el grupo de opciones de configuración **Componentes para instalar**, seleccione las casillas situadas junto a los nombres de los componentes de Kaspersky Embedded Systems Security para Windows que quiera instalar.

d. Para indicar una carpeta de destino que no sea la predeterminada, especifique el nombre y la ruta de la carpeta en el campo **Carpeta de destino**.

La ruta de acceso a la carpeta de destino puede contener variables de entorno del sistema. La carpeta se creará si no existe en el dispositivo protegido.

e. En el grupo **Configuración avanzada de instalación**, configure los siguientes parámetros:

- Analizar el dispositivo protegido en busca de virus antes de la instalación
- **Habilitar la protección en tiempo real después de la instalación**
- **Agregar archivos recomendados por Microsoft a la lista de exclusiones**
- **Agregar archivos recomendados por Kaspersky a la lista de exclusiones**
- **Habilitar el inicio demorado del servicio de Kaspersky Security en el inicio del sistema operativo**

f. En la ventana de diálogo **Propiedades: <nombre del paquete de instalación>**, haga clic en **Aceptar**.

10. En el nodo **Paquetes de instalación**, cree una tarea para instalar Kaspersky Embedded Systems Security para Windows de forma remota en los dispositivos protegidos seleccionados (grupo de administración). Configure los parámetros de la tarea.

Para saber más sobre la creación y configuración de tareas de instalación remotas, consulte la *Ayuda de Kaspersky Security Center*.

11. Ejecute la tarea de instalación remota de Kaspersky Embedded Systems Security para Windows.

Kaspersky Embedded Systems Security para Windows se instalará en los dispositivos protegidos especificados en la tarea.

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security para Windows

Después de instalar Kaspersky Embedded Systems Security para Windows, recomendamos que actualice las bases de datos de Kaspersky Embedded Systems Security para Windows en los dispositivos y realice un Análisis de áreas críticas de los dispositivos en caso de que estos no hayan tenido instaladas aplicaciones antivirus con protección en tiempo real habilitada antes de la instalación de Kaspersky Embedded Systems Security para Windows.

Si los dispositivos protegidos en los que se instaló Kaspersky Embedded Systems Security para Windows forman parte del mismo grupo de administración en Kaspersky Security Center, puede llevar a cabo estas tareas de la siguiente manera:

1. Cree tareas de Actualización de bases de datos para los grupos de dispositivos protegidos en los que se instaló Kaspersky Embedded Systems Security para Windows. Establezca el servidor de administración de Kaspersky Security Center como origen de actualizaciones.

2. Cree una tarea de grupo de Análisis a pedido con el estado del Análisis de áreas críticas. Kaspersky Security Center evalúa el estado de seguridad de cada uno de los dispositivos protegidos del grupo de acuerdo con los resultados de esta tarea, no en función de los resultados de la tarea Análisis de áreas críticas.

3. Cree una nueva directiva para el grupo de dispositivos protegidos. En las propiedades de la directiva, en la sección **Configuración de la aplicación**, desactive el inicio programado de las tareas locales de análisis a

pedido del sistema y actualización de bases de datos en los dispositivos protegidos del grupo de administración en la configuración de la subsección **Ejecutar tareas locales del sistema**.

También puede configurar las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security para Windows.

Instalación de la Consola de la aplicación mediante Kaspersky Security Center

La información detallada sobre la creación de un paquete de instalación y la tarea de instalación remota está disponible en la Guía de implementación de Kaspersky Security Center.

Para instalar la Consola de la aplicación mediante una tarea de instalación:

1. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Avanzado**.
2. Expanda el nodo secundario **Instalación remota**.
3. En el panel de resultados del nodo secundario Paquetes de instalación, haga clic en el botón **Crear paquete de instalación**. Al crear el nuevo paquete de instalación:
   a. En la ventana **Asistente de paquete nuevo**, seleccione **Crear un paquete de instalación para el archivo ejecutable especificado** como un tipo de paquete.
   b. Ingrese el nombre del nuevo paquete de instalación.
   c. Seleccione el archivo \console\setup.exe de la carpeta del kit de distribución de Kaspersky Embedded Systems Security para Windows y seleccione la casilla de verificación **Copiar carpeta entera al paquete de instalación**.
   d. Utilice la opción de línea de comandos ADDLOCAL en el campo **Configuración de inicio del archivo ejecutable (opcional)** para instalar la Consola de la aplicación. La Consola de la aplicación se instala en la carpeta de instalación predeterminada. Asegúrese de especificar el parámetro "EULA=1". De lo contrario, es imposible instalar componentes.
      ```
      /s /p "ADDLOCAL=MmcSnapin EULA=1"
      ```
      Opcionalmente, en el campo **Configuración de inicio del archivo ejecutable (opcional)**, puede usar la opción de línea de comandos ADDLOCAL para modificar el conjunto de componentes que se instalarán y la opción de línea de comandos INSTALLDIR para especificar una carpeta de destino distinta de la predeterminada. Por ejemplo, para realizar una instalación independiente de la Consola de la aplicación en la carpeta C:\KasperskyConsole, use la siguiente opción de línea de comandos:
      ```
      /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
      ```
4. En el nodo secundario **Paquetes de instalación**, cree una tarea para instalar la Consola de la aplicación de forma remota en los dispositivos protegidos seleccionados (grupo de administración). Configure los parámetros de la tarea.

   Para saber más sobre la creación y configuración de tareas de instalación remotas, consulte la ayuda de Kaspersky Security Center.

5. Ejecute la tarea de instalación remota.

La Consola de la aplicación se instalará en los dispositivos protegidos especificados en la tarea.

Desinstalación de Kaspersky Embedded Systems Security para Windows a través de Kaspersky Security Center

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security para Windows. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Si la administración de Kaspersky Embedded Systems Security para Windows en dispositivos de la red está protegida por contraseña, escriba la contraseña al crear una tarea para la desinstalación de varias aplicaciones. Si la protección por contraseña no está administrada centralmente por la directiva de Kaspersky Security Center, Kaspersky Embedded Systems Security para Windows se desinstalará correctamente de los dispositivos en los cuales la contraseña introducida se corresponda con el valor establecido. Kaspersky Embedded Systems Security para Windows no se desinstalará de los otros dispositivos protegidos.

Para desinstalar Kaspersky Embedded Systems Security para Windows.

1. En la Consola de administración de Kaspersky Security Center, cree e inicie una tarea de desinstalación de la aplicación.

2. En la tarea, seleccione el método de desinstalación (similar a la selección del método de instalación; consulte la sección anterior) y especifique la cuenta que el Servidor de administración usará para acceder a los dispositivos protegidos. Kaspersky Embedded Systems Security para Windows solo puede desinstalarse con la configuración de desinstalación predeterminada.

Instalación y desinstalación a través de directivas de grupo de Active Directory

En esta sección, se describe cómo instalar y desinstalar Kaspersky Embedded Systems Security para Windows a través de las directivas de grupo de Active Directory y se brinda información sobre las acciones que se deben realizar después de instalar Kaspersky Embedded Systems Security para Windows mediante directivas de grupo.

Instalación de Kaspersky Embedded Systems Security para Windows mediante directivas de grupo de Active Directory

Puede instalar Kaspersky Embedded Systems Security para Windows en varios dispositivos protegidos a través de la directiva de grupo de Active Directory. Puede instalar la Consola de la aplicación del mismo modo.

Los dispositivos protegidos donde desea instalar Kaspersky Embedded Systems Security para Windows o la Consola de la aplicación deben pertenecer al mismo dominio y a una sola unidad organizacional.

Los sistemas operativos de los dispositivos protegidos en los que desea instalar Kaspersky Embedded Systems Security para Windows con la directiva deben tener la misma cantidad de bits (32 bits o 64 bits).

Usted debe disponer de derechos de administrador de dominio.

Para instalar Kaspersky Embedded Systems Security para Windows, use el paquete de instalación de ess_x86.msi o ess_x64.msi. Para instalar la Consola de la aplicación, use el paquete de instalación de esstools.msi.

Se ofrece información detallada sobre el uso de las directivas de grupo de Active Directory en la documentación provista por Microsoft.

Para instalar Kaspersky Embedded Systems Security para Windows (o la Consola de la aplicación):

1. En la carpeta compartida del controlador de dominio, guarde el archivo msi que corresponda a la cantidad de bits (32 bits o 64 bits) de la versión instalada del sistema operativo Microsoft Windows.
2. Guarde el archivo de clave en la misma carpeta pública en el controlador de dominio.
3. En la misma carpeta compartida en el controlador de dominio, cree un archivo install_props.json que contenga las líneas que se indican a continuación. Esto significa que acepta los términos del Contrato de licencia de usuario final y de la Política de privacidad.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. En el controlador de dominio, cree una nueva directiva para el grupo al que pertenezcan los dispositivos protegidos.
5. Utilice el **Editor de objetos de directiva de grupo** para crear un nuevo paquete de instalación en el nodo **Configuración del equipo**. Escriba la ruta del archivo msi de Kaspersky Embedded Systems Security para Windows (o la Consola de la aplicación) en el formato UNC (convención de nomenclatura universal).
6. Seleccione **Instalar siempre con privilegios elevados** en el servicio Windows Installer, tanto en el nodo **Configuración del equipo** como en el nodo **Configuración del usuario** del grupo seleccionado.
7. Aplique los cambios utilizando el comando `gpupdate / force`.

Kaspersky Embedded Systems Security para Windows se instalará en los dispositivos protegidos del grupo después de que se hayan reiniciado.

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security para Windows

Después de instalar Kaspersky Embedded Systems Security para Windows en los dispositivos protegidos, se recomienda actualizar inmediatamente las bases de datos de la aplicación y ejecutar un Análisis de áreas críticas. Puede realizar estas acciones desde la Consola de la aplicación.

También puede configurar las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security para Windows.

Desinstalación de Kaspersky Embedded Systems Security para Windows mediante políticas de grupo de Active Directory

Los archivos de volcado y rastreo no se eliminan al desinstalar Kaspersky Embedded Systems Security para Windows. Puede eliminar manualmente los archivos de volcado y rastreo de la carpeta especificada durante la configuración de la escritura de los archivos de volcado y rastreo.

Si utilizó una directiva del grupo de Active Directory para instalar Kaspersky Embedded Systems Security para Windows (o la Consola de la aplicación) en el grupo de dispositivos protegidos, puede utilizar esta directiva para desinstalar Kaspersky Embedded Systems Security para Windows (o la Consola de la aplicación).

La aplicación puede desinstalarse únicamente con los parámetros de desinstalación predeterminados.

Se ofrece información detallada sobre el uso de las directivas de grupo de Active Directory en la documentación provista por Microsoft.

Si la administración de la aplicación está protegida por contraseña, no puede desinstalar Kaspersky Embedded Systems Security para Windows utilizando directivas del grupo de Active Directory.

Para desinstalar Kaspersky Embedded Systems Security para Windows (o la Consola de la aplicación):

1. En el controlador de dominio, seleccione la unidad organizativa desde cuyos dispositivos protegidos desea desinstalar Kaspersky Embedded Systems Security para Windows o la Consola de la aplicación.
2. Seleccione la directiva creada para la instalación de Kaspersky Embedded Systems Security para Windows, y en el **Editor de objetos de directivas de grupo**, en el nodo **Instalación de software** (**Configuración del equipo** > **Configuración de software** > **Instalación de software**), abra el menú contextual del paquete de instalación de Kaspersky Embedded Systems Security para Windows (o la Consola de la aplicación) y seleccione el comando **Todas las tareas** > **Eliminar**.
3. Seleccione el método de desinstalación **Desinstalar inmediatamente el software de usuarios y equipos**.
4. Aplique los cambios utilizando el comando `gpupdate / force`.

   Kaspersky Embedded Systems Security para Windows se eliminará de los dispositivos protegidos después de que se hayan reiniciado y antes de iniciar sesión en Microsoft Windows.

Verificación de funciones de Kaspersky Embedded Systems Security para Windows. Uso del virus de prueba EICAR

Esta sección describe el virus de prueba EICAR y cómo debe utilizarse para verificar las funciones Protección de archivos en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security para Windows.

Acerca del virus de prueba EICAR

El virus de prueba fue diseñado para comprobar el funcionamiento de las aplicaciones antivirus. Fue desarrollado por el Instituto Europeo para la Investigación de los Antivirus Informáticos (EICAR).

El virus de prueba no es un objeto malicioso y no contiene código ejecutable para su dispositivo, aunque las aplicaciones antivirus de la mayoría de los proveedores lo detectan como una amenaza.

El archivo contiene el virus de prueba llamado eicar.com. Puede descargarse del sitio web de EICAR.

Antes de guardar el archivo en una carpeta en el disco duro de su dispositivo, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada en esa unidad.

El archivo eicar.com contiene una línea de texto. Al analizar el archivo, Kaspersky Embedded Systems Security para Windows detecta la amenaza de prueba en la línea de texto, le asigna el estado **Infectado** al archivo y lo elimina. La información acerca de la amenaza detectada en el archivo aparecerá en la Consola de la aplicación y en el registro de tareas.

Puede utilizar el archivo eicar.com para comprobar cómo Kaspersky Embedded Systems Security desinfecta los objetos infectados y cómo detecta objetos probablemente infectados. Para tal fin, abra el archivo con un editor de texto y, al comienzo de la línea de texto del archivo, agregue uno de los prefijos enumerados en la tabla a continuación. Hecho esto, guarde el archivo con un nuevo nombre, como eicar_cure.com.

Para asegurarse de que Kaspersky Embedded Systems Security para Windows procese el archivo eicar.com con un prefijo, en la sección **Protección de objetos** de la configuración de seguridad, establezca el valor **Todos los objetos** en las tareas de Protección del equipo en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security para Windows.

Prefijos de archivos EICAR

Prefijo	Estado del archivo después del análisis y la acción tomada por Kaspersky Embedded Systems Security para Windows
Sin prefijo	**Kaspersky Embedded Systems Security para Windows le asigna el estado Infectado al objeto y lo elimina.**
SUSP–	Kaspersky Embedded Systems Security para Windows le asigna el estado **Probablemente infectado** al objeto detectado por el analizador heurístico y lo elimina, ya que los objetos probablemente infectados no estén desinfectados.
WARN–	Kaspersky Embedded Systems Security para Windows le asigna el estado **Probablemente infectado** al objeto (el código del objeto coincide en parte con el código de una amenaza conocida) y lo elimina, ya que los objetos probablemente infectados no estén desinfectados.
CURE–	Kaspersky Embedded Systems Security para Windows le asigna el estado **Infectado** al objeto y lo desinfecta. Si la desinfección se realiza correctamente, la totalidad del texto del archivo se reemplaza con la palabra "CURE".

Verificación de las funciones Protección de archivos en tiempo real y Análisis a pedido

Después de instalar Kaspersky Embedded Systems Security para Windows, puede verificar que Kaspersky Embedded Systems Security para Windows sea capaz de detectar objetos que contengan código malicioso. Para tal fin, utilice el virus de prueba EICAR.

Para verificar la función Protección de archivos en tiempo real:

1. Descargue el archivo eicar.com en el sitio web de EICAR. Guárdelo en una carpeta compartida en el disco local de cualquier dispositivo de la red.

   Antes de guardar el archivo en la carpeta, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada para la carpeta.

2. Si desea comprobar el funcionamiento de las notificaciones del usuario de red, asegúrese de que el servicio Windows Messenger de Microsoft esté habilitado tanto en el dispositivo protegido como en el dispositivo donde guardó el archivo eicar.com.

3. Abrir la Consola de la aplicación en el dispositivo protegido.

4. Copie el archivo eicar.com guardado en el disco local del dispositivo protegido mediante alguno de los siguientes métodos:

   - Para probar las notificaciones a través de una ventana Terminal Services, copie el archivo eicar.com en el dispositivo protegido después de conectarlo al dispositivo protegido mediante la utilidad Conexión remota a escritorio.

   - Para probar notificaciones a través del servicio Windows Messenger de Microsoft, use los sitios de la red del dispositivo para copiar el archivo eicar.com del dispositivo donde lo guardó.

La Protección de archivos en tiempo real funciona correctamente si se cumplen las siguientes condiciones:

- El archivo eicar.com se elimina del dispositivo protegido.

- En la Consola de la aplicación, se le asigna el estado *Crítico* al registro de tareas. El registro tiene una nueva línea con información sobre una amenaza en el archivo eicar.com.

- El siguiente mensaje del Servicio de Microsoft Windows Messenger aparece en el dispositivo desde el que copió el archivo: `Kaspersky Embedded Systems Security para Windows bloqueó el acceso a <ruta del archivo en el dispositivo>\eicar.com en el equipo <nombre de red del dispositivo> a las <hora del evento>. Motivo: Amenaza detectada. Virus: EICAR-Test-File. Nombre de usuario: <nombre del usuario>. Nombre del equipo: <nombre de red del dispositivo desde el que se copió el archivo>`.

  Asegúrese de que el servicio Windows Messenger de Microsoft esté en ejecución en el dispositivo desde el que se copió el archivo eicar.com.

Para verificar la función de Análisis a pedido:

1. Descargue el archivo eicar.com en el sitio web de EICAR. Guárdelo en una carpeta compartida en el disco local de cualquier dispositivo de la red.

   Antes de guardar el archivo en la carpeta, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada para la carpeta.

2. Abra la Consola de la aplicación y expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.

3. Seleccione el nodo secundario **Análisis de áreas críticas**.

4. En la pestaña **Configuración del área de análisis**, abra el menú contextual del nodo **Red** y seleccione **Agregar archivo de red**.

5. Introduzca la ruta de acceso de red al archivo eicar.com en el dispositivo remoto con el formato UNC (convención de nomenclatura universal).

6. Seleccione la casilla **Ruta de acceso a un objeto** para incluir la ruta de acceso de red agregada en el área del análisis.

7. Ejecute la tarea Análisis de áreas críticas.

El Análisis a pedido funciona correctamente si se cumplen las siguientes condiciones:

- El archivo eicar.com se elimina del disco duro del dispositivo.

- En la Consola de la aplicación, se le asigna el estado *Crítico* al registro de tareas. El registro de tareas de Análisis de áreas críticas tiene una nueva línea con información sobre una amenaza en el archivo eicar.com.

Icono de interfaz de la aplicación

Puede controlar Kaspersky Embedded Systems Security para Windows mediante las siguientes interfaces:

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

Consola de administración de Kaspersky Security Center

Kaspersky Security Center le permite instalar y desinstalar, iniciar y detener Kaspersky Embedded Systems Security para Windows de forma remota, configurar la configuración de la aplicación, cambiar el grupo de componentes de la aplicación disponibles, agregar claves e iniciar y detener tareas.

La aplicación puede administrarse a través de Kaspersky Security Center mediante el complemento de administración de Kaspersky Embedded Systems Security para Windows. Consulte la información detallada sobre la interfaz de Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Kaspersky Security Center Web Console y Cloud Console

Kaspersky Security Center Web Console (de ahora en más denominada Web Console) es una aplicación web destinada a realizar, de forma centralizada, tareas principales para administrar y mantener el sistema de seguridad de la red de una organización. Web Console es un componente de Kaspersky Security Center que proporciona una interfaz de usuario. Para obtener más información acerca de Kaspersky Security Center Web Console, consulte la *Ayuda de Kaspersky Security Center*.

Kaspersky Security Center Cloud Console (de ahora en más denominada Cloud Console) es una solución basada en la nube para proteger y administrar la red de una organización. Para obtener más información acerca de Kaspersky Security Center Cloud Console, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Web Console y Cloud Console le permiten hacer lo siguiente:

- Supervisar el estado del sistema de seguridad de su organización.
- Instalar aplicaciones de Kaspersky en dispositivos dentro de su red.
- Administrar aplicaciones instaladas.
- Ver informes acerca del estado del sistema de seguridad.

Licencia de la aplicación

Esta sección brinda información sobre los conceptos principales relacionados con el otorgamiento de una licencia de la aplicación.

Acerca del Contrato de licencia de usuario final

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

Recomendamos revisar detenidamente los términos del Contrato de licencia de usuario final antes de comenzar a usar la aplicación.

Puede leer los términos del Contrato de licencia de usuario final y de la Política de privacidad, que describen el procesamiento y la transmisión de datos, de las siguientes maneras:

- Durante la instalación de la Consola de Kaspersky Embedded Systems Security para Windows.
- Después de la instalación, desde el menú **Inicio** (**Todos los programas** > **Kaspersky Embedded Systems Security para Windows** > **Contrato de licencia de usuario final y Política de privacidad**).
- Durante la instalación de Kaspersky Fraud Prevention Cloud.
- Al leer el documento de archivo license.txt incluido en el kit de distribución.
- En el sitio web de Kaspersky (https://latam.kaspersky.com/business/eula).

Al confirmar que acepta el Contrato de licencia de usuario final al instalar la aplicación, debe indicar su aceptación de los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe anular la instalación de la aplicación y no debe usarla.

Acerca de la licencia

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

Una licencia válida le da derecho a recibir el uso de la aplicación de acuerdo con los términos del Contrato de licencia de usuario final, así como a recibir soporte técnico cuando sea necesario.

El área de servicio y el periodo de uso de la aplicación dependen del tipo de licencia que se utilizó para activar la aplicación.

Puede activar la aplicación de dos maneras:

- Con un archivo de clave, que le otorga el uso con la licencia comercial.
- Con un código de activación para comprar una licencia comercial.

Puede comprar una licencia estándar de Kaspersky Embedded Systems Security para Windows o la licencia extendida de Kaspersky Embedded Systems Security para Windows Compliance Edition, que incluye dos componentes de inspección del sistema adicionales: Monitor de integridad de archivos e Inspección de registros.

Cuando una licencia comercial caduca, la aplicación continúa ejecutándose, pero las siguientes funciones dejan de estar disponibles:

- Integración con Kaspersky Security Network
- Actualización de las bases de datos de Kaspersky Embedded Systems Security para Windows

Si se elimina la clave de licencia, la aplicación continuará ejecutándose. Si elimina una clave de licencia, la aplicación seguirá ejecutándose y las tareas **Análisis a pedido** y **Protección de archivos en tiempo real** seguirán estándo disponibles, pero se perderá la capacidad de utilizar las demás tareas y de actualizar las bases de datos de Kaspersky Embedded Systems Security para Windows. Lo mismo ocurre si Kaspersky agrega su licencia a la lista de rechazadas.

Para seguir usando todas las funciones de Kaspersky Embedded Systems Security, debe renovar su licencia.

Para garantizar la máxima protección de su dispositivo, recomendamos que renueve la licencia antes de que caduque.

Asegúrese de que la fecha de caducidad de la clave adicional sea posterior a la de la licencia activa

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se le entrega junto con un archivo de clave o un código de activación (si corresponde).

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

- Número de pedido
- Información acerca del usuario a quien se le ha otorgado la licencia
- Información acerca de la aplicación que puede activarse con la licencia proporcionada
- Límite del número de unidades de licencia (es decir, dispositivos en los cuales puede usarse la aplicación con la licencia proporcionada)
- Fecha de inicio de validez de la licencia
- Fecha de caducidad de la licencia o término de la licencia
- Tipo de licencia

Acerca de la clave

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

Para agregar una clave a la aplicación, use un archivo de clave. Luego de agregar una clave a la aplicación, esta aparece en la interfaz de la aplicación como una secuencia alfanumérica exclusiva.

Kaspersky puede agregar una clave a la lista de rechazadas si hay infracciones del Contrato de licencia. Si se bloquea su clave, se debe agregar una clave diferente para que funcione la aplicación.

Una clave puede ser una "clave activa" o una "clave adicional".

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

Una *clave adicional* es una clave que confirma el derecho de usar la aplicación pero que actualmente no se encuentra en uso. La clave adicional se activa automáticamente cuando expira la licencia asociada con la clave activa actual. Se puede agregar una clave adicional solo si hay una clave activa.

Acerca del archivo de clave

Un *archivo de clave* es un archivo con la extensión .key provisto por Kaspersky. Los archivos de clave están diseñados para agregar una clave con la que se activa la aplicación.

Recibirá un archivo de clave por correo electrónico después de comprar Kaspersky Embedded Systems Security para Windows o de solicitar la versión de prueba de Kaspersky Embedded Systems Security para Windows.

No necesita conectarse con los servidores de activación de Kaspersky a fin de activar la aplicación con un archivo de clave.

Puede restaurar un archivo de clave si lo ha eliminado accidentalmente. Podría necesitar su archivo de clave para, por ejemplo, registrarse con Kaspersky CompanyAccount.

Para recuperar un archivo de clave, realice alguna de estas acciones:

- Comuníquese con el proveedor de su licencia.
- Obtenga un archivo de clave en el sitio web de Kaspersky, utilizando para ello el código de activación que tenga disponible.

Acerca del código de activación

Un *código de activación* es una secuencia única de 20 letras y números. Debe introducir un código de activación para poder agregar una clave de activación de Kaspersky Embedded Systems Security para Windows. Usted recibe el código de activación en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Embedded Systems Security para Windows o cuando solicitó la versión de prueba de Kaspersky Embedded Systems Security para Windows.

Para activar la aplicación con un código de activación, necesita acceso a Internet a fin de conectarse con los servidores de activación de Kaspersky.

Si ha perdido su código de activación después de instalar la aplicación, puede recuperarlo. Es posible que necesite el código de activación para registrar Kaspersky CompanyAccount, por ejemplo. Para recuperar su código de activación, comuníquese con el socio de Kaspersky Lab a quien le compró la licencia.

Sobre la provisión de datos

El Contrato de licencia para Kaspersky Embedded Systems Security para Windows, específicamente la sección titulada "Términos del procesamiento de datos", especifica los términos, la responsabilidad legal y el procedimiento para enviar y procesar los datos indicados en esta Guía. Antes de aceptar el Contrato de licencia, revise detenidamente sus términos, además de todos los documentos vinculados con el Contrato de licencia.

Los datos que Kaspersky recibe cuando usted utiliza la aplicación se protegen y se procesan de acuerdo con la Política de privacidad, disponible en www.kaspersky.com/Products-and-Services-Privacy-Policy.

Puede acceder a los términos del Contrato de licencia y la Política de privacidad durante la instalación de Kaspersky Embedded Systems Security para Windows (encontrará los documentos en el kit de distribución), como también desde el menú **Inicio** (**Todos los programas** > **Kaspersky Embedded Systems Security para Windows** > **Contrato de licencia de usuario final y Política de privacidad**) después de la instalación.

Durante la desinstalación de Kaspersky Embedded Systems Security para Windows se eliminan todos los datos almacenados por Kaspersky Embedded Systems Security para Windows en el dispositivo protegido.

Al aceptar los términos del Contrato de licencia de usuario final, acepta enviar automáticamente los siguientes datos a Kaspersky:

- Admitir el mecanismo para recibir actualizaciones; información sobre la aplicación instalada y su activación: el identificador de la aplicación instalada y su versión completa, incluido el número de compilación, el tipo, y el identificador de licencia, el identificador de instalación y el identificador de tarea de actualización.
- Usar la capacidad de explorar artículos de la Base de conocimientos cuando se produzcan errores en la aplicación (servicio de Redirección); información sobre la aplicación y el tipo del vínculo: el nombre, la configuración regional y el número de versión completo de la aplicación, el tipo de vínculo de redirección y el identificador del error.
- Administrar confirmaciones para el procesamiento de datos: información sobre el estado de aceptación de contratos de licencia y otros documentos que estipulan términos de transferencia de datos (identificador y versión del Contrato de licencia u otro documento), como parte de los cuales se aceptan o se rechazan los términos de procesamiento de datos; un atributo, que indique la acción del usuario (confirmación o retiro de la aceptación de los términos); la fecha y la hora de los cambios de estado de la aceptación de los términos de procesamiento de datos.

Procesamiento de datos local

Al ejecutar las funciones principales de la aplicación descritas en esta Guía, Kaspersky Embedded Systems Security para Windows procesa y almacena de forma local un conjunto de datos en el dispositivo protegido.

La siguiente tabla contiene información sobre el procesamiento y almacenamiento local que realiza Kaspersky Embedded Systems Security para Windows de los datos contenidos en los informes.

Procesamiento y almacenamiento de datos contenidos en informes

Área funcional	Registro de eventos
Tipo de uso	Kaspersky Embedded Systems Security para Windows almacena los datos de forma local y los envía al Servidor de administración. La base de datos del Servidor de administración almacena información sobre eventos de aplicaciones que ocurren en los dispositivos protegidos administrados.

Depósito	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<versión del producto>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Base de datos del Servidor de administración
Medidas de seguridad	Lista de control de acceso.
Periodo de almacenamiento	Kaspersky Embedded Systems Security para Windows almacena los datos hasta su desinstalación. Durante la desinstalación de Kaspersky Embedded Systems Security para Windows se eliminan todos los datos almacenados por Kaspersky Embedded Systems Security para Windows en el dispositivo protegido.
Objetivo	Proporcionar funcionalidad primaria.

Kaspersky Embedded Systems Security para Windows no elimina ningún evento del Registro de eventos de Windows, ni siquiera aquellos registrados durante la desinstalación de Kaspersky Embedded Systems Security para Windows.

Para proporcionar la funcionalidad de registro de eventos, Kaspersky Embedded Systems Security para Windows procesa los siguientes datos en forma local:

- Nombres, sumas de verificación (MD5, SHA-256) y atributos de archivos procesados y rutas completas a ellos en los medios analizados.
- Acciones tomadas en archivos analizados por Kaspersky Embedded Systems Security para Windows.
- Acciones realizadas por el usuario con los archivos analizados en el dispositivo protegido.
- Información sobre cuentas de usuarios que realizan acciones en la red protegida o el dispositivo protegido.
- Valores de la Ruta de acceso a la instancia del dispositivo para los dispositivos agregados a las reglas de Control de dispositivos.
- Información sobre procesos y scripts que se ejecutan en el sistema: sumas de verificación (MD5, SHA-256) y rutas completas a archivos ejecutables, información sobre certificados digitales.
- Configuración del firewall de Windows.
- Entradas del Registro de eventos de Windows.
- Nombres de las cuentas de usuario que realizan acciones con los archivos analizados en el dispositivo protegido.
- Instancias de archivos ejecutables que se inician y los tipos, nombres, sumas de verificación y atributos de estos archivos.
- Información sobre la actividad de red:
  - Las direcciones IP de los dispositivos externos bloqueados.
  - Direcciones IP procesadas.

- Información sobre el estado del Windows USN Journal.

La siguiente tabla contiene información sobre los datos de servicio procesados por Kaspersky Embedded Systems Security para Windows. Los datos de servicio incluyen lo siguiente: parámetros del programa, archivos en cuarentena y en copia de seguridad, información en las bases de datos de servicio del programa, datos de la licencia.

La siguiente tabla contiene información sobre el procesamiento y almacenamiento local que realiza Kaspersky Embedded Systems Security para Windows de datos sobre parámetros especificados por un usuario.

Procesamiento y almacenamiento de datos sobre parámetros especificados por un usuario

Área funcional	Toda la funcionalidad de Kaspersky Embedded Systems Security para Windows
Tipo de uso	Kaspersky Embedded Systems Security para Windows almacena los datos de forma local y los envía al Servidor de administración. Los datos se almacenan en la base de datos del Servidor de administración. Los datos que la aplicación procesa localmente no se envían automáticamente a Kaspersky ni a otros sistemas de terceros.
Depósito	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<versión del producto>\ • Base de datos del Servidor de administración
Medidas de seguridad	Lista de control de acceso.
Periodo de procesamiento	Kaspersky Embedded Systems Security para Windows almacena los datos hasta su desinstalación. Durante la desinstalación de Kaspersky Embedded Systems Security para Windows se eliminan todos los datos almacenados por Kaspersky Embedded Systems Security para Windows en el dispositivo protegido. Kaspersky Embedded Systems Security para Windows no elimina los datos sobre los parámetros exportados al archivo de configuración. Kaspersky Embedded Systems Security para Windows no elimina los objetos en cuarentena y en copia de seguridad si las casillas de verificación **Exportar objetos de Cuarentena** y **Exportar objetos de Copia de seguridad** están seleccionadas en el Asistente de configuración.
Objetivo	Proporcionar funcionalidad primaria.

Kaspersky Embedded Systems Security para Windows procesa de forma local los siguientes datos para los objetivos especificados.

- Objetos colocados en cuarentena o copia de seguridad.
- Información sobre las cuentas de usuario (nombres de usuario y contraseñas) con las que Kaspersky Embedded Systems Security para Windows ejecuta las tareas.
- Contraseña de Kaspersky Embedded Systems Security para Windows.
- Direcciones IP e identificadores de sesiones bloqueadas.
- Configuración del Firewall de Windows y configuración de reglas del Firewall de Windows.

- Sumas de verificación (MD5, SHA-256) y rutas de acceso a archivos ejecutables agregados a las reglas de la tarea Control de inicio de aplicaciones.
- Valores de la Ruta de acceso a la instancia del dispositivo para los dispositivos agregados a las reglas de Control de dispositivos.
- Información sobre archivos y carpetas incluidas en las áreas de las tareas de Kaspersky Embedded Systems Security para Windows.
- Direcciones IP incluidas o excluidas del alcance de protección.
- Información sobre eventos en el Registro de eventos de Windows.
- Información sobre detecciones con el uso de la tecnología iSwift o iChecker.
- Sumas de verificación (MD5, SHA-256), rutas completas y máscaras especificadas en la configuración de exclusiones.
- Información sobre procesos agregados a la Zona de confianza.
- Información sobre claves de licencia agregadas.
- Información sobre certificados digitales.
- Archivos desempaquetados de un archivo de almacenamiento u otro objeto compuesto durante el análisis.

Kaspersky Embedded Systems Security para Windows procesa y almacena datos como parte de la funcionalidad básica de la aplicación, lo cual incluye registrar eventos de la aplicación y recibir datos de diagnóstico. Los datos procesados localmente están protegidos según las opciones configuradas y aplicadas.

Kaspersky Embedded Systems Security para Windows le permite configurar el nivel de protección para los datos procesados de forma local (Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security para Windows, Registro de eventos. Registros de Kaspersky Embedded Systems Security para Windows). Puede cambiar los privilegios del usuario para acceder a los datos procesados, cambiar los periodos de retención para tales datos, deshabilitar de manera parcial o total la funcionalidad que involucra el registro de datos y cambiar la ruta y los atributos de la carpeta en la que se registran los datos.

Los datos que la aplicación procesa localmente no se envían automáticamente a Kaspersky ni a otros sistemas de terceros.

De forma predeterminada, todos los datos que la aplicación procesa localmente mientras está en funcionamiento se eliminan tras desinstalar Kaspersky Embedded Systems Security para Windows del dispositivo protegido.

Quedan exceptuados los archivos con información de diagnóstico (archivos de seguimiento y de volcado), los eventos que la aplicación almacena en el Registro de eventos de Windows y los archivos a los que se pueda haber exportado la configuración de Kaspersky Embedded Systems Security para Windows. Recomendamos que elimine estos archivos manualmente.

Puede encontrar información detallada sobre cómo trabajar con archivos que contienen datos de diagnóstico de la aplicación en las secciones correspondientes de esta Guía.

Para eliminar los archivos del Registro de eventos de Windows que contienen eventos de la aplicación Kaspersky Embedded Systems Security para Windows, puede usar las herramientas estándar del sistema operativo.

Procesamiento local de datos mediante la aplicación de componentes auxiliares.

El paquete de instalación de Kaspersky Embedded Systems Security para Windows comprende los componentes auxiliares de la aplicación, que se pueden instalar en su dispositivo incluso si Kaspersky Embedded Systems Security para Windows no está instalado en él. Los componentes auxiliares son los siguientes:

- Consola de la aplicación. Este componente forma parte de las Herramientas de administración de Kaspersky Embedded Systems Security para Windows. Es un complemento para Microsoft Management Console.

- El Complemento de administración. Este componente proporciona una integración completa con la aplicación de Kaspersky Security Center.

Al realizar las funciones principales de la aplicación que se detallan en esta Guía, los componentes auxiliares de la aplicación procesan y almacenan localmente un conjunto de datos en el dispositivo protegido donde están instalados, incluso si se instalan por separado de Kaspersky Embedded Systems Security para Windows.

Los componentes de la aplicación procesan y almacenan localmente los siguientes datos:

- La Consola de la aplicación: el nombre del dispositivo protegido que tiene instalado Kaspersky Embedded Systems Security para Windows (dirección IP o nombre de dominio) y al que se conectó por última vez la Consola de la aplicación de forma remota; parámetros de visualización configurados en el complemento de Microsoft Management Console; datos sobre la última carpeta en la que el usuario seleccionó objetos a través de la Consola de la aplicación (mediante el cuadro de diálogo del sistema que se abre al hacer clic en el botón **Examinar**). Los archivos de seguimiento de la Consola de la aplicación también pueden contener los siguientes datos: el nombre del dispositivo protegido que tiene instalada la aplicación Kaspersky Embedded Systems Security para Windows y con el cual se estableció la conexión remota, y el nombre de la cuenta de usuario que se usó para establecer la conexión remota.

- El Complemento de administración puede procesar y almacenar temporalmente ciertos datos procesados por Kaspersky Embedded Systems Security para Windows (por ejemplo, los ajustes configurados para las tareas y los componentes de la aplicación, los ajustes de las directivas de Kaspersky Security Center y los datos enviados en las listas de red).

La siguiente tabla contiene información sobre el procesamiento y almacenamiento local que realiza Kaspersky Embedded Systems Security para Windows de los datos escritos en archivos de volcado y seguimiento.

Kaspersky Embedded Systems Security para Windows procesa y almacena de forma local los siguientes datos escritos en archivos de volcado y seguimiento:

- Información sobre acciones realizadas por Kaspersky Embedded Systems Security para Windows en el dispositivo protegido.

- Información sobre los objetos procesados por Kaspersky Embedded Systems Security para Windows.

- Información sobre la actividad en el dispositivo protegido que es procesada por Kaspersky Embedded Systems Security para Windows.

- Información sobre errores que ocurrieron durante la ejecución de Kaspersky Embedded Systems Security para Windows.

Los datos que los componentes auxiliares procesan no se envían automáticamente a Kaspersky ni a otros sistemas de terceros.

De forma predeterminada, todos los datos que los componentes auxiliares de la aplicación procesan localmente durante la operación se eliminan después de la eliminación de estos componentes.

La excepción son los archivos de seguimiento de los componentes auxiliares de la aplicación. Recomendamos que elimine estos archivos manualmente.

Datos en archivos de seguimiento y volcado

Kaspersky Embedded Systems Security para Windows puede, de acuerdo con la configuración, escribir información de depuración en archivos de rastreo con fines de soporte técnico durante la operación de Kaspersky Embedded Systems Security para Windows.

Los archivos de volcado de Kaspersky Embedded Systems Security para Windows son generados por el sistema operativo cuando la aplicación deja de funcionar y se sobrescriben la próxima vez que sucede.

Los archivos de seguimiento y volcado pueden incluir datos personales de un usuario o datos confidenciales de su organización.

No utilice Kaspersky Embedded Systems Security para Windows en dispositivos para los que la directiva de su organización prohíbe el envío de datos.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows no registra información de depuración.

Los archivos de seguimiento y volcado no se envían automáticamente más allá del host en el que se generaron. El contenido de los archivos de seguimiento se puede visualizar con visores de archivos de texto estándar. Los archivos de seguimiento y de volcado se guardan indefinidamente y no se eliminan al desinstalar Kaspersky Embedded Systems Security para Windows.

La información de depuración puede ser útil para el Servicio de soporte técnico.

No se proporcionan mecanismos especiales para limitar el acceso a los archivos de seguimiento y volcado. El administrador puede configurar que estos datos se escriban en una carpeta protegida.

La ruta a la carpeta de archivos de seguimiento y volcado no está configurada de manera predeterminada. Para usar la carpeta de seguimiento y volcado, el administrador debe especificarla.

Los datos en los archivos de seguimiento y volcado pueden contener:

- Información sobre acciones realizadas por Kaspersky Embedded Systems Security para Windows en el dispositivo protegido.
- Información sobre objetos procesados por Kaspersky Endpoint Agent.
- Errores que surgen durante la operación de Kaspersky Endpoint Agent.

Activación de la aplicación con un archivo de clave

Puede activar Kaspersky Embedded Systems Security para Windows al aplicar un archivo de clave.

Si ya se ha agregado una clave activa a Kaspersky Embedded Systems Security para Windows y se agrega otra clave como clave activa, la nueva clave sustituye a la clave agregada previamente. La clave agregada previamente se elimina.

Si ya se ha agregado una clave adicional a Kaspersky Embedded Systems Security para Windows y se agrega otra clave como clave adicional, la nueva clave sustituye a la clave agregada previamente. La clave adicional agregada previamente se elimina.

Si ya se han agregado una clave activa y una clave adicional a Kaspersky Embedded Systems Security para Windows y se agrega una nueva clave como clave activa, la nueva clave sustituye a la clave activa agregada anteriormente y la clave adicional no se elimina.

Para activar Kaspersky Embedded Systems Security para Windows con un archivo de clave:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.
2. En el panel de resultados del nodo **Licencia**, haga clic en el vínculo **Agregar clave**.
3. En la ventana que se abre, haga clic en el botón **Examinar**.
4. Seleccione un archivo de clave con la extensión .key.

   También puede agregar una clave como clave adicional. Para agregar una clave como clave adicional, seleccione la casilla de verificación **Usar como clave adicional**.

5. Haga clic en el botón **Aceptar**.

   Se aplicará el archivo de clave seleccionado. La información sobre la clave agregada estará disponible en el nodo **Licencia**.

Activación de la aplicación con un código de activación

Para activar la aplicación utilizando un código de activación, el dispositivo protegido debe estar conectado a Internet.

Puede activar Kaspersky Embedded Systems Security para Windows mediante un código de activación.

Al activar la aplicación con este método, Kaspersky Embedded Systems Security para Windows envía datos al servidor de activación para verificar el código ingresado:

- Si la verificación del código de activación es exitosa, la aplicación se activa.
- Si la verificación del código de activación falla, aparece la notificación correspondiente. En este caso, debe comunicarse con el proveedor de software al que compró su licencia de Kaspersky Embedded Systems Security para Windows.
- Si se excede la cantidad de activaciones con el código de activación, aparece la notificación correspondiente. El procedimiento de activación de la aplicación se interrumpe, y la aplicación le indica que debe ponerse en contacto con el Servicio de soporte técnico.

Puede activar Kaspersky Embedded Systems Security para Windows con un código de activación mediante la Consola de la aplicación o si crea la tarea de grupo Activación de la aplicación mediante el Complemento de administración o el Complemento web.

Para activar Kaspersky Embedded Systems Security para Windows con un código de activación mediante la Consola de la aplicación, realice lo siguiente:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.
2. En el panel de resultados del nodo **Licencia**, haga clic en el vínculo **Agregar código de activación**.

3. En la ventana que se abre, ingrese el código de activación en el campo **Código de activación**.

   - Si desea utilizar el código de activación como una clave adicional, active la casilla de verificación **Usar como clave adicional**.
   - Para ver información sobre una licencia, haga clic en el botón **Ver información de licencia**. La información se mostrará en el bloque **Información sobre la licencia**.

4. Haga clic en el botón **Aceptar**.

   Kaspersky Embedded Systems Security para Windows envía información sobre el código de activación que se ingresó al servidor de activación.

Ver información acerca de la licencia actual

Visualización de información de la licencia

Puede ver información sobre el estado de la licencia actual en el panel de detalles del nodo **Kaspersky Embedded Systems Security** de la Consola de la aplicación. Una clave puede tener los siguientes estados:

- **Verificando el estado de la clave**: Kaspersky Embedded Systems Security para Windows está comprobando el archivo de clave o código de activación aplicado y espera una respuesta sobre el estado de la clave actual.
- **Fecha de caducidad de la licencia**: Kaspersky Embedded Systems Security para Windows está activo hasta la fecha y la hora especificadas. El estado de la clave se resalta en amarillo en los siguientes casos:
  - La licencia caducará en 14 días, y no se aplicó ninguna clave adicional.
  - La clave agregada se ha añadido a la lista de rechazadas y se bloqueará.
- **La licencia ha caducado**: Kaspersky Embedded Systems Security para Windows no se activa porque la licencia ha caducado. El estado se resalta en rojo.
- **Infracción del Contrato de licencia de usuario final**: Kaspersky Embedded Systems Security para Windows no se activa porque se han infringido los términos del Contrato de licencia de usuario final. El estado se resalta en rojo.
- **La clave está en la lista de rechazadas**: la clave agregada se ha bloqueado y Kaspersky la ha agregado a la lista de rechazadas, por ejemplo, en el caso de que terceros utilicen la clave para activar la aplicación ilegalmente. El estado se resalta en rojo.

Ver información acerca de la licencia actual

Para ver la información acerca de la licencia actual:

En el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.

La información general acerca de la licencia actual se muestra en el panel de detalles del nodo **Licencia** (consulte la tabla a continuación).

Información general acerca de la licencia en el nodo Licencia

Campo	Descripción

Código de activación	El código de activación. Este campo se completa si activa la aplicación con un código de activación.
Estado de activación	Información sobre el estado de la activación de la aplicación. La columna **Estado de activación** del panel de detalles del nodo **Licencia** puede tener los siguientes estados: • **Aplicada**: si ha activado la aplicación con un código de activación o archivo de clave. • **Activación**: si ha aplicado un código de activación para activar la aplicación, pero el proceso de activación aún no ha finalizado. Se han completado los cambios de estado a **Aplicada** después de la activación de la aplicación y la actualización de los contenidos del panel de detalles del nodo. • **Error de activación**: si se produjo un error en la activación de la aplicación. Puede ver la causa del error en la activación en el registro de tareas.
Clave	La clave utilizada para activar la aplicación.
Tipo de licencia	Tipo de licencia: comercial o de prueba.
Fecha de caducidad	La fecha y hora de caducidad de la licencia asociada con una clave activa.
Estado del código de activación o estado de la clave	Estado del código de activación o estado de la clave: *Activa* o *Adicional*.

Para ver información detallada acerca de la licencia:

en el nodo **Licencia**, abra el menú contextual en la línea con los datos de la licencia que desea ampliar y seleccione **Propiedades**.

En la ventana **Propiedades de la clave**, la pestaña **General** contiene información detallada acerca de la licencia actual y, en la pestaña **Avanzado**, está disponible información sobre el cliente e información de contacto de Kaspersky o el distribuidor donde compró Kaspersky Embedded Systems Security para Windows (consulte la tabla a continuación).

Información detallada de la licencia en la ventana Propiedades: <Estado del código de activación o estado de la clave>

Campo	Descripción
Ficha General	
Clave	La clave utilizada para activar la aplicación.
Fecha de adición de clave	Fecha en la que se agregó la clave a la aplicación.
Tipo de licencia	Tipo de licencia: comercial o de prueba.
Días hasta la fecha de caducidad	Cantidad de días restantes hasta la caducidad de la licencia asociada con la clave activa.
Fecha de caducidad	La fecha y hora de caducidad de la licencia asociada con una clave activa. Si la aplicación se activa con una suscripción ilimitada, el valor del campo es *Ilimitado*. Si Kaspersky Embedded Systems Security para Windows no puede determinar la fecha de caducidad de la licencia, el valor del campo es *Desconocido*.

Aplicación	El nombre de la aplicación activada con el archivo de clave o código de activación.
Restricción de uso de la clave	La restricción de uso de la clave (si corresponde).
Brinda acceso a soporte técnico	Información sobre si Kaspersky o uno de nuestros socios proporcionará soporte técnico según los términos de la licencia.
Pestaña Avanzado	
Información sobre la licencia	Clave de licencia actual.
Información de soporte	Información de contacto de Kaspersky o del socio que brinda el servicio de soporte técnico. Este campo puede estar vacío si no se proporciona el Servicio de soporte técnico.
Información del propietario	Información sobre el propietario de la licencia: el nombre del cliente y el nombre de la organización para la cual se adquirió la licencia.

Limitaciones funcionales cuando caduca la licencia

Cuando la licencia actual caduque, se aplicarán las siguientes limitaciones a los componentes funcionales:

- Todas las tareas se detienen, excepto las tareas Protección de archivos en tiempo real, Análisis a pedido y Control de integridad de la aplicación.
- No puede iniciar ninguna tarea, excepto Protección de archivos en tiempo real, Análisis a pedido y Control de integridad de la aplicación. Estas tareas continúan ejecutándose usando las bases de datos antivirus viejas.
- Se limita la funcionalidad de Prevención de exploits:
  - Los procesos se protegen hasta que se reinician.
  - Los procesos nuevos no se pueden agregar al área de protección.

Otras funciones (repositorios, registros, información de diagnóstico) todavía están disponibles.

Renovación de la licencia

De forma predeterminada, Kaspersky Embedded Systems Security para Windows notifica cuando la licencia está a catorce días de caducar. En este caso, el estado **Fecha de caducidad de la licencia** se resalta en amarillo en el panel de resultados del nodo **Kaspersky Embedded Systems Security para Windows**.

Puede renovar la licencia antes de la fecha de caducidad mediante una clave adicional. Esto asegura que su dispositivo permanezca protegido después de la caducidad de la licencia actual y antes de que active la aplicación con una licencia nueva.

Para renovar una licencia:

1. Adquiera un nuevo código de activación o un archivo de clave.

2. En el árbol de la Consola de la aplicación, seleccione el nodo **Licencia**.
3. En el panel de resultados del nodo **Licencia**, realice una de las siguientes acciones:
   - Si desea renovar la licencia con un archivo de clave:
     a. Haga clic en el vínculo **Agregar clave**.
     b. En la ventana que se abre, haga clic en el botón **Examinar**.
     c. Seleccione un nuevo archivo de clave con la extensión .key.
     d. Seleccione la casilla de verificación **Usar como clave adicional**.
   - Si desea renovar una licencia con un código de activación:
     a. Haga clic en el vínculo **Agregar código de activación**.
     b. Escriba el código de activación comprado en la ventana que se abre.
     c. Seleccione la casilla de verificación **Usar como clave adicional**.

   Se requiere una conexión a Internet para aplicar el código de activación.
4. Haga clic en el botón **Aceptar**.

La clave adicional se agregará y se aplicará automáticamente cuando venza la licencia actual de Kaspersky Embedded Systems Security para Windows.

Eliminación de la clave

Se puede eliminar la clave agregada.

Si una clave adicional se ha agregado a Kaspersky Embedded Systems Security para Windows y la clave activa se elimina, la clave adicional se convierte automáticamente en la clave activa.

Si se elimina una clave adicional, se puede restaurar volviendo a aplicar el archivo de clave.

Para eliminar una clave que se ha agregado:

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Licencia**.
2. En el panel de resultados del nodo **Licencia**, en la tabla que contiene información sobre claves agregadas, seleccione la clave que desee eliminar.
3. En el menú contextual de la línea que contiene información sobre la clave seleccionada, seleccione **Eliminar**.
4. Haga clic en el botón **Sí** de la ventana de confirmación para confirmar que desea eliminar la clave.

Se eliminará la clave seleccionada.

Cómo usar el Complemento de administración

Esta sección proporciona información sobre el Complemento de administración de Kaspersky Embedded Systems Security para Windows y describe cómo administrar la aplicación instalada en un dispositivo protegido o en un grupo de dispositivos protegidos.

Administración de Kaspersky Embedded Systems Security para Windows mediante Kaspersky Security Center

Si ha instalado Kaspersky Embedded Systems Security para Windows en una serie de dispositivos protegidos que forman parte de un mismo grupo de administración, puede administrarlos en forma centralizada mediante el Complemento de administración de Kaspersky Embedded Systems Security para Windows. Kaspersky Security Center también permite configurar individualmente los ajustes de cada dispositivo protegido incluido en el grupo de administración.

Un *grupo de administración* se crea manualmente a través de Kaspersky Security Center. El grupo incluye varios dispositivos con Kaspersky Embedded Systems Security para Windows instalado, para los cuales es conveniente configurar las mismas opciones de control y protección. Para obtener más información sobre la utilización de grupos de administración, consulte la *Ayuda de Kaspersky Security Center*.

La configuración de la aplicación para un solo dispositivo protegido no está disponible si el funcionamiento de Kaspersky Embedded Systems Security para Windows en el dispositivo protegido está controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Embedded Systems Security para Windows puede administrarse desde Kaspersky Security Center de las siguientes maneras:

- **Utilización de directivas de Kaspersky Security Center**. Es posible usar directivas de Kaspersky Security Center para configurar remotamente la misma configuración de protección para un grupo de dispositivos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre las opciones de la tarea configuradas de forma local en la Consola de la aplicación o remotamente en la ventana **Propiedades: <Nombre del dispositivo protegido>** de Kaspersky Security Center.

  Las directivas se pueden usar para configurar los ajustes generales de la aplicación, los ajustes de las tareas de protección del equipo en tiempo real, las tareas de control de actividades en los dispositivos y los ajustes que regulan el inicio programado de tareas del sistema local.

- **Utilización de tareas de grupo de Kaspersky Security Center**. Las tareas de grupo de Kaspersky Security Center permiten configurar a distancia las opciones comunes de las tareas que tienen un periodo de vencimiento para un grupo de dispositivos.

  Puede usar tareas de grupo para activar la aplicación, configurar la tarea de Análisis a pedido, actualizar la configuración de tareas y configurar la tarea Generador de reglas de Control de inicio de aplicaciones.

- **Utilización de tareas para un conjunto de dispositivos**. Las tareas para un conjunto de dispositivos permiten la configuración remota de las opciones comunes de las tareas con un periodo de ejecución limitado para dispositivos protegidos que no pertenecen a ningún grupo de administración.

- **Utilización de la ventana de propiedades de un solo dispositivo**. En la ventana **Propiedades: <Nombre del dispositivo protegido>**, puede configurar a distancia las opciones de tareas de un dispositivo protegido específico que forme parte de un grupo de administración. También puede establecer tanto la configuración general de la aplicación como la configuración para todas las tareas de Kaspersky Embedded Systems Security para Windows si el dispositivo protegido seleccionado no está controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Security Center le permite configurar los parámetros de la aplicación y las funciones avanzadas y, también, trabajar con registros y notificaciones. Puede configurar estos parámetros para un grupo de dispositivos protegidos y para un dispositivo protegido en particular.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar las configuraciones generales de Kaspersky Embedded Systems Security para Windows en Kaspersky Security Center Web Console.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración general mediante la directiva

Para abrir la configuración de la aplicación de Kaspersky Embedded Systems Security para Windows mediante la directiva:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Configuración de la aplicación**.
6. Haga clic en el botón **Configuración**, en la subsección de la configuración que desee ajustar.

Cómo abrir la configuración general en la ventana de propiedades de la aplicación

Para abrir la ventana de propiedades de Kaspersky Embedded Systems Security para Windows para un solo dispositivo protegido:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:

- Haga doble clic en el nombre del dispositivo protegido.
- Abra el menú contextual del nombre del dispositivo protegido y seleccione el elemento **Propiedades**.

Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.

5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security 3.3 para Windows**.
6. Haga clic en el botón **Propiedades**.
   Se abrirá la ventana **Configuración de Kaspersky Embedded Systems Security 3.3 para Windows**.
7. Seleccione la sección **Configuración de la aplicación**.

Configuración de las opciones generales de la aplicación en Kaspersky Security Center

Puede establecer la configuración general de Kaspersky Embedded Systems Security para Windows desde Kaspersky Security Center para un grupo de dispositivos protegidos o para un dispositivo protegido.

Ajustes de escalabilidad, interfaz y configuración del análisis en Kaspersky Security Center

Para establecer los parámetros de la escalabilidad, la interfaz y la configuración del análisis, realice lo siguiente:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Configuración de la aplicación**, en la subsección **Configuración de la escalabilidad, interfaz y análisis**, haga clic en el botón **Configuración**.
5. En la ventana **Configuración avanzada de la aplicación** en la pestaña **General**, establezca la siguiente configuración:
   - En la sección **Configuración de escalabilidad**, establezca la configuración que define el número de procesos usados por Kaspersky Embedded Systems Security para Windows:
     - Detectar automáticamente la configuración de escalabilidad
     - Configurar manualmente el número de procesos de trabajo

- Número de procesos para la protección en tiempo real
- Número de procesos para tareas de análisis a pedido en segundo plano

- En la sección **Interacción con el usuario**, configure si el Icono de la bandeja del sistema se visualizará en el área de notificación al seleccionar o desactivar la casilla de verificación **Mostrar ícono de la bandeja del sistema en la barra de tareas**.

6. En la pestaña **Configuración del análisis**, establezca los siguientes parámetros:

   - Restaurar los atributos del archivo luego del análisis
   - Restringir el uso de CPU para los subprocesos del análisis
     - Límite máximo (en porcentaje)
   - Carpeta para los archivos temporales creados durante el análisis

7. En la pestaña **Depósito jerárquico**, seleccione la opción para acceder al depósito jerárquico.

8. Haga clic en el botón **Aceptar**.

Se guarda la configuración de la aplicación.

Configuración de opciones de seguridad en Kaspersky Security Center

Para configurar las opciones de seguridad manualmente:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Configuración de la aplicación**, haga clic en el botón **Seguridad y confiabilidad** en la subsección **Configuración**.

5. En la ventana **Configuración de seguridad**, configure las siguientes opciones:

   - En la sección **Configuración de protección con contraseña**, habilite o deshabilite la opción **Proteger los procesos de la aplicación de amenazas externas**.
   - En la sección **Configuración de protección con contraseña**, establezca una contraseña para proteger el acceso a las funciones de Kaspersky Embedded Systems Security para Windows.
   - En la sección **Defensa propia**, establezca la configuración de la recuperación de las tareas de Kaspersky Embedded Systems Security para Windows cuando la aplicación devuelva un error o deje de funcionar.

- Ejecutar recuperación de tarea
- Configuración de confiabilidad

- En la sección **No recuperar tareas de análisis a pedido más de (veces)**, especifique limitaciones de la carga del dispositivo protegido creadas por Kaspersky Embedded Systems Security para Windows después de cambiar a la alimentación de UPS:
  - No iniciar las tareas de análisis programadas
  - Detener las tareas de análisis en curso
- En la sección **Configuración de protección con contraseña**, establezca una contraseña para proteger el acceso a las funciones de Kaspersky Embedded Systems Security para Windows.

6. Haga clic en el botón **Aceptar**.

Se guarda la configuración establecida de escalabilidad y de confiabilidad.

Configuración de opciones de conexión mediante Kaspersky Security Center

Los parámetros de conexión configurados se utilizan para conectar Kaspersky Embedded Systems Security para Windows a servidores de activación y actualización durante la integración de aplicaciones con Servicios KSN.

Para configurar los parámetros de conexión, siga estos pasos:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Configuración de la aplicación**, haga clic en el botón **Conexiones** en la subsección **Configuración**.

   Se abrirá la ventana **Configuración de conexión**.
5. En la ventana **Configuración de conexión**, configure las siguientes opciones:
   - En la sección **Configuración del servidor proxy**, seleccione la configuración de uso del servidor proxy:
     - No usar un servidor proxy
     - Usar el servidor proxy especificado
     - **La dirección IP o el nombre simbólico del servidor proxy y el número de puerto**

- No usar el servidor proxy para las direcciones locales.

- En la sección **Configuración de autenticación del servidor proxy**, especifique la configuración de autenticación:

  - Seleccione la configuración de autenticación en la lista desplegable.

    - **No usar autenticación**: no se realiza la autenticación. Este modo está seleccionado en forma predeterminada.

    - **Usar autenticación NTLM**: la autenticación se realiza usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.

    - **Usar autenticación NTLM con nombre de usuario y contraseña**: la autenticación se realiza con un nombre de usuario y contraseña usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.

    - **Aplicar nombre de usuario y contraseña**: la autenticación se realiza usando el nombre de usuario y contraseña.

  - Escriba el nombre de usuario y la contraseña, de ser necesario.

- En la sección **Licencia**, desactive o seleccione la casilla **Usar Kaspersky Security Center como servidor proxy al activar la aplicación**.

6. Haga clic en el botón **Aceptar**.

Los parámetros de conexión configurados se guardan.

Configuración del inicio programado de las tareas locales del sistema

Puede usar directivas para autorizar o bloquear el inicio de las tareas de Análisis a pedido y de Actualización del sistema local según la programación configurada localmente en cada dispositivo protegido en el grupo de administración:

- Si el inicio programado de un tipo específico de tarea local del sistema está prohibido por una directiva, estas tareas no se realizarán en el dispositivo protegido según la programación. Puede iniciar las tareas locales del sistema manualmente.

- Si el inicio programado de un tipo específico de tarea local del sistema está permitido por una directiva, estas tareas se realizarán según los parámetros programados y configurados localmente para esta tarea.

De forma predeterminada, la directiva prohíbe el inicio de una tarea local del sistema.

Recomendamos que no habilite el inicio de tareas locales del sistema si las actualizaciones o los análisis a pedido están administrados por tareas de grupo de Kaspersky Security Center.

Si no utiliza la actualización del grupo o las tareas de análisis a pedido, permita que las tareas locales del sistema se inicien en la directiva. Kaspersky Embedded Systems Security para Windows realizará actualizaciones del módulo y de la base de datos de la aplicación e iniciará todas las tareas locales de análisis a pedido del sistema, de acuerdo con el programa predeterminado.

Puede usar directivas para autorizar o bloquear el inicio programado de las siguientes tareas del sistema locales:

- Tareas de Análisis a pedido: Análisis de áreas críticas, Análisis de archivos en cuarentena, Análisis al inicio del sistema operativo, Control de integridad de la aplicación, Monitor comparativo de integridad de archivos.
- Tareas de Actualización: Actualización de bases de datos, Actualización de módulos del programa, Copia de actualizaciones.

Si el dispositivo protegido se excluye del grupo de administración, la programación de tareas locales del sistema se habilitará automáticamente.

Para autorizar o bloquear el inicio programado de tareas locales del sistema de Kaspersky Embedded Systems Security para Windows en una directiva realice lo siguiente:

1. En el nodo **Dispositivos administrados** del árbol de la consola de administración, expanda el grupo requerido y seleccione la pestaña **Directivas**.
2. En la pestaña **Directivas**, en el menú contextual de la directiva para la que desee programar tareas del sistema local de Kaspersky Embedded Systems Security para Windows del grupo de dispositivos protegidos, seleccione **Propiedades**.
3. En la ventana **Propiedades: <Nombre de la directiva>**, abra la sección **Configuración de la aplicación**. En la sección **Ejecutar tareas locales del sistema**, haga clic en el botón **Configuración** y realice una de las siguientes acciones:
   - Seleccione las casillas de verificación **Tareas de análisis a pedido** y **Tareas de actualización y tarea Copia de actualizaciones** para autorizar el inicio programado de estas tareas.
   - Desactive las casillas de verificación **Tareas de análisis a pedido** y **Tareas de actualización y tarea Copia de actualizaciones** para deshabilitar el inicio programado estas tareas.

   La selección o la desactivación de la casilla de verificación no afectará la configuración del inicio de ninguna tarea local personalizada de este tipo.
4. Asegúrese de que la directiva que configura esté activa y se aplique al grupo seleccionado de dispositivos protegidos.
5. Haga clic en el botón **Aceptar**.

La configuración establecida de programación de tareas se aplica para las tareas seleccionadas.

Configuración de opciones de Cuarentena y Copia de seguridad en Kaspersky Security Center

Para establecer la configuración general de Copia de seguridad en Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

- Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

- Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Adicional**, haga clic en el botón **Configuración** de la subsección **Depósitos**.

5. Use la pestaña **Configuración de depósitos** de la ventana **Copia de seguridad** para configurar las siguientes opciones de Copia de seguridad:

   - Si desea especificar la carpeta de copia de seguridad, utilice el campo **Carpeta de Copia de seguridad** para seleccionar la carpeta requerida en la unidad local del dispositivo protegido o, si lo prefiere, introduzca la ruta completa.

   - Para establecer el tamaño máximo de Copia de seguridad, seleccione la casilla de verificación **Tamaño máx. de Copia de seguridad (MB)** y especifique el valor necesario en megabytes en el campo de entrada.

   - Para configurar el límite de espacio libre de Copia de seguridad, realice lo siguiente:

     - Defina el valor de la configuración de **Tamaño máx. de Copia de seguridad (MB)**.

     - Seleccione la casilla de verificación **Valor umbral de espacio disponible (MB)**.

     - Especifique en megabytes el valor mínimo de espacio libre en la carpeta Copia de seguridad.

   - Para especificar una carpeta para objetos restaurados, realice una de las siguientes acciones:

     - Seleccione la carpeta relevante en una unidad local del dispositivo protegido en la sección **Configuración de restauración**.

     - Ingrese el nombre de la carpeta y la ruta completa a ella en el campo **Carpeta de destino para restaurar objetos**.

6. En la ventana **Configuración de depósitos** en la pestaña **Cuarentena**, configure las siguientes opciones de Cuarentena:

   - Para cambiar la carpeta de Cuarentena, en el campo de entrada de la **Carpeta de Cuarentena** especifique la ruta completa de la carpeta en el disco local del dispositivo protegido.

   - Para establecer el tamaño máximo de Cuarentena, seleccione la casilla de verificación **Tamaño máximo de cuarentena (MB)** y especifique el valor de este parámetro en megabytes en el campo de entrada.

   - Para establecer la cantidad mínima de espacio libre en la Cuarentena, seleccione la casilla de verificación **Tamaño máximo de cuarentena (MB)** y la casilla de verificación **Valor umbral de espacio disponible (MB)** y, a continuación, especifique el valor de este parámetro en megabytes en el campo de entrada.

   - Para cambiar la carpeta de almacenamiento de los objetos restaurados desde Cuarentena, en el campo **Carpeta de destino para restaurar objetos**, especifique la ruta completa de la carpeta en el disco local del dispositivo protegido.

7. Haga clic en el botón **Aceptar**.

Los parámetros configurados de la Cuarentena y las Copia de seguridad se guardan.

Creación y configuración de directivas

Esta sección proporciona información sobre la utilización de directivas de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security para Windows en varios dispositivos protegidos.

Las directivas globales de Kaspersky Security Center pueden crearse para administrar la protección de varios dispositivos en los que está instalado Kaspersky Embedded Systems Security para Windows.

Una directiva implementa la configuración, las funciones y las tareas especificadas de Kaspersky Embedded Systems Security para Windows en todos los dispositivos protegidos para un grupo de administración.

Se pueden crear e implementar por turnos varias directivas para un grupo de administración. En la Consola de administración, la directiva activa actualmente para un grupo tiene el estado *activa*.

La información sobre la implementación de la directiva se carga en el registro de auditoría del sistema de Kaspersky Embedded Systems Security para Windows. Esta información se puede visualizar en la Consola de la aplicación, en el nodo **Registro de auditoría del sistema**.

Kaspersky Security Center ofrece una manera de aplicar directivas en dispositivos protegidos: *no permitir los cambios a la configuración*. Después de aplicar una directiva, Kaspersky Embedded Systems Security para Windows utiliza los valores de configuración para los cuales seleccionó el icono en las propiedades de la directiva en dispositivos protegidos. En este caso, Kaspersky Embedded Systems Security para Windows no utiliza los valores de configuración vigentes antes de que se aplicara la directiva. Kaspersky Embedded Systems Security para Windows no aplica los valores de configuración de la directiva activa para los cuales ha seleccionado el icono en las propiedades de la directiva.

Si una directiva está activa, los valores de configuración marcados con el icono en la directiva se muestran en la Consola de la aplicación, pero no se pueden modificar. Los valores de otras opciones de configuración (marcados con el icono en la directiva) pueden modificarse en la Consola de la aplicación.

La configuración establecida en la directiva activa y marcada con el icono también bloquea los cambios en Kaspersky Security Center para un dispositivo protegido en la ventana **Propiedades: <Nombre del dispositivo protegido>**.

La configuración que se especifica y se envía al dispositivo protegido usando una directiva activa se guarda en la configuración de las tareas locales después de que se deshabilita la directiva activa.

Si una directiva define la configuración de una tarea de Protección del equipo en tiempo real que se encuentra en ejecución, la configuración definida por la directiva cambiará en cuanto se aplique la directiva. Si la tarea no está en ejecución, la configuración se implementará cuando se inicie.

Creación de directiva

Para crear una directiva para un grupo de dispositivos protegidos en los que la aplicación esté instalada y en ejecución:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la consola de administración de Kaspersky Security Center y, a continuación, seleccione el grupo de administración que contiene los dispositivos protegidos para los que desea crear una directiva.

2. En el panel de detalles del grupo de administración seleccionado, seleccione la pestaña **Directivas** y haga clic en el vínculo **Crear una directiva** para iniciar el asistente y crear una directiva.

   Se abre la ventana **Asistente de nueva directiva**.

3. En la ventana **Seleccionar la aplicación para la cual desea crear una directiva de grupo**, seleccione Kaspersky Embedded Systems Security para Windows y haga clic en **Siguiente**.

4. Ingrese un nombre de la directiva de grupo en el campo **Nombre**.

   El nombre de la directiva no puede contener los siguientes símbolos: `" * < : > ? \ |`.

5. Para aplicar una configuración de directiva que se utilizó en una versión anterior de la aplicación:

   a. Seleccione la casilla de verificación **Usar configuración de la directiva para versiones anteriores de la aplicación**.

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

   c. Seleccione la directiva que desea aplicar.

   d. Haga clic en el botón **Siguiente**.

6. En la ventana **Selección del tipo de operación**, en el bloque **Método de creación de la directiva**, seleccione una de estas opciones:

   - **Nueva**, para crear una directiva nueva con las opciones predeterminadas.
   - **Importar directiva creada con versiones anteriores de Kaspersky Embedded Systems Security para Windows**, para usar la directiva importada como una plantilla.

7. En la ventana **Protección del equipo en tiempo real**, configure los componentes de la aplicación:

   a. De ser necesario, cambie la configuración predeterminada de los componentes de Protección del equipo en tiempo real:

      1. Haga clic en **Configuración** en la subsección del componente.
      2. En la ventana que se abre, configure los ajustes del componente:
      3. Haga clic en el botón **Aceptar**.

   b. Permita o bloquee la aplicación de los ajustes configurados para los componentes de Protección del equipo en tiempo real en los dispositivos protegidos de la red:

      - Haga clic en el botón para que los ajustes de los componentes puedan configurarse en los dispositivos protegidos de la red y evitar que se apliquen los ajustes configurados en la directiva para los componentes.
      - Haga clic en el botón para que los ajustes de los componentes no puedan configurarse en los dispositivos protegidos de la red y permitir que se apliquen los ajustes configurados en la directiva para los componentes.

   c. Haga clic en el botón **Siguiente**.

8. Seleccione uno de los siguientes estados de la directiva en la ventana **Crear la directiva de grupo para la aplicación**:

   - **Directiva activa**, si desea que la directiva se aplique inmediatamente después de su creación. Si ya existiera una directiva activa en el grupo, se la desactivará y se aplicará la directiva nueva.

   - **Directiva inactiva**, si no desea aplicar la directiva creada inmediatamente. En este caso, la directiva se puede activar más tarde.

   - Seleccione la casilla de verificación **Abrir propiedades de la directiva inmediatamente después de su creación** para cerrar automáticamente el **Asistente de nueva directiva** y configurar la directiva recién creada después de hacer clic en el botón **Siguiente**.

9. Haga clic en el botón **Finalizar**.

La directiva creada se mostrará en la lista de directivas de la pestaña **Directivas** del grupo de administración seleccionado. En la ventana **Propiedades: <Nombre de la directiva>**, puede establecer otra configuración, tareas y funciones de Kaspersky Embedded Systems Security para Windows.

Cuando se crea una nueva directiva, se crea también un conjunto de reglas de autorización que evita que las aplicaciones se bloqueen y garantiza que continúen funcionando sin interrupciones. Puede ver las reglas predeterminadas en la configuración de tareas. Encontrará los detalles y las limitaciones más abajo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red entrante:

- Dos reglas de autorización para el proceso de compartir el escritorio de Windows mediante el Agente de red de Kaspersky Security Center, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

- Dos reglas de autorización para el puerto local 15000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red saliente:

- Dos reglas de autorización para el servicio de Kaspersky Embedded Systems Security para Windows, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

- Dos reglas de autorización para el proceso de trabajo de Kaspersky Embedded Systems Security para Windows, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

- Dos reglas de autorización para el puerto local 13000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

Secciones de configuraciones de las directivas de Kaspersky Embedded Systems Security para Windows

General

En la sección **General**, puede configurar las siguientes opciones de la directiva:

- Especificar el estado de la directiva.
- Configurar las opciones de herencia para las directivas principales y las secundarias.

Notificaciones de eventos

En la sección **Notificación de eventos**, puede configurar las opciones de las siguientes categorías de eventos:

- *Evento crítico*
- *Fallo funcional*
- *Advertencia*
- *Información*
  Puede usar el botón **Propiedades** para configurar las siguientes opciones de los eventos seleccionados:
- Indicar la ubicación de almacenamiento y el periodo de retención para la información sobre los eventos registrados.
- Indicar el método de notificación para los eventos registrados.

Configuración de la aplicación

Configuración de la sección Configuración de la aplicación

Sección	Opciones
Configuración de la escalabilidad, interfaz y análisis	En la subsección **Configuración de la escalabilidad, interfaz y análisis**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Elija si desea ajustar la configuración de la escalabilidad automáticamente o manualmente. • Establecer la configuración de la visualización del icono de la aplicación.
Seguridad y confiabilidad	En la subsección **Seguridad y confiabilidad**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Configurar las opciones de inicio de tareas. • Especificar cómo debería comportarse la aplicación cuando el dispositivo protegido se está ejecutando con energía de UPS. • Habilitar o deshabilitar la protección con contraseña de funciones de la aplicación.
Conexiones	En la subsección **Conexiones**, puede usar el botón **Configuración** para configurar las siguientes opciones del servidor proxy para la conexión a KSN y a los servidores de actualizaciones y activación: • Configurar las opciones del servidor proxy • Especificar la configuración de autenticación del servidor proxy

Ejecutar tareas locales del sistema	En la subsección **Ejecutar tareas locales del sistema**, puede usar el botón **Configuración** para autorizar o bloquear el inicio de las siguientes tareas locales del sistema según la programación configurada en los dispositivos protegidos: • Tarea Análisis a pedido. • Tareas Actualización y tarea Copia de actualización.

Adicional

Configuración de la sección Adicional

Sección	Opciones
Zona de confianza	En la subsección **Configuración**, puede hacer clic en el botón **Zona de confianza** para configurar las siguientes opciones relativas a la zona de confianza: • Crear una lista de exclusiones para la Zona de confianza. • Habilitar o deshabilitar el análisis de las operaciones de copia de seguridad de archivos. • Crear una lista de procesos de confianza.
Análisis de unidades extraíbles	En la subsección **Análisis de unidades extraíbles**, puede usar el botón **Configuración** para configurar los parámetros de análisis para unidades extraíbles.
Permisos de acceso de usuario para administrar la aplicación	En la subsección **Permisos de acceso de usuario para administrar la aplicación**, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar Kaspersky Embedded Systems Security para Windows.
Permisos de acceso de usuario para la administración del servicio de Kaspersky Security	En la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security**, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar el servicio de Kaspersky Security.
Depósitos	En la sección **Depósitos**, haga clic en el botón **Configuración** para configurar las siguientes opciones de Cuarentena, Copia de seguridad y Hosts bloqueados: • Especificar la ruta de la carpeta donde desea colocar objetos en Cuarentena o Copia de seguridad. • Configurar el tamaño máximo de Copia de seguridad y Cuarentena, y especificar el umbral de espacio disponible. • Especificar la ruta de la carpeta donde desea colocar objetos restaurados de la Cuarentena o la Copia de seguridad. • Configurar la duración del bloqueo de hosts.

Protección del equipo en tiempo real

Configuración de la sección Protección del equipo en tiempo real

Sección	Opciones
Protección de archivos en tiempo real	En la subsección **Protección de archivos en tiempo real**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Indicar el modo de protección. • Configurar el uso del Analizador heurístico. • Configurar el uso de la zona de confianza. • Indicar el área de protección. • Configurar el nivel de seguridad para el área de protección seleccionada: puede seleccionar un nivel de seguridad predefinido o establecer la configuración de la seguridad manualmente. • Configurar las opciones de inicio de tareas.
Uso de KSN	En la subsección **Uso de KSN**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Indicar las acciones a realizar en objetos no confiables según KSN. • Configurar la transferencia de datos y el uso de Kaspersky Security Center como servidor KSN Proxy. Haga clic en el botón **Declaración de KSN** para aceptar o rechazar la Declaración de KSN y configurar las opciones de intercambio de datos.
Prevención de exploits	En la subsección **Prevención de exploits**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de protección de memoria del proceso. • Indicar acciones para reducir el riesgo que suponen los exploits. • Añadir elementos a la lista de procesos protegidos y editar dicha lista.

Control de actividad local

Configuración de la sección Control de actividad local

Sección	Opciones
Control de inicio de aplicaciones	En la subsección **Control de inicio de aplicaciones**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones para controlar los inicios subsiguientes de la aplicación. • Indicar el área de las reglas de Control de inicio de aplicaciones. • Configurar el uso de KSN. • Configurar las opciones de inicio de tareas.

Control de dispositivos	En la subsección **Control de dispositivos**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones de inicio de tareas.

Control de actividad de red

Configuración de la sección Control de actividad de red

Sección	Opciones
Administración de firewall	En la subsección **Administración de firewall**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Configurar las reglas de firewall. • Configurar las opciones de inicio de tareas.

Inspección del sistema

Configuración de la sección Inspección del sistema

Sección	Opciones
Monitor de integridad de archivos	En la subsección **Monitor de integridad de archivos**, puede configurar el control de los cambios en archivos que pueden significar una infracción de la seguridad en un dispositivo protegido.
Inspección de registros	En la subsección **Inspección de registros**, puede configurar un monitoreo de la integridad del dispositivo protegido basado en los resultados de un análisis del Registro de eventos de Windows.

Registros y notificaciones

Configuración de la sección Registros y notificaciones

Sección	Opciones
Registros de tareas	En la subsección **Registros de tareas**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Especificar el nivel de importancia de los eventos registrados para los componentes de la aplicación seleccionados. • Especificar la configuración de depósitos de almacenamiento del registro de tareas. • Especificar la integración de SIEM con la configuración de Kaspersky Security Center.
Notificaciones de eventos	En la subsección **Notificaciones de eventos**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Especifique la configuración de la notificación del usuario para los eventos *Objeto detectado*, *Dispositivo externo no confiable detectado y bloqueado* y *La sesión de red*

	está en la lista de sesiones dudosas. • Especificar la configuración de notificaciones del administrador para cualquier evento seleccionado en la lista de eventos en la sección **Configuración de notificaciones**.
Interacción con Servidor de administración	En la sección **Interacción con Servidor de administración**, puede hacer clic en el botón **Configuración** para seleccionar los tipos de objetos (incluidos los objetos de Cuarentena y Copia de seguridad) que Kaspersky Embedded Systems Security para Windows informará al Servidor de administración.

Diagnóstico de mal funcionamiento

Configuración de la sección Diagnóstico de mal funcionamiento

Sección	Opciones
Configuración de diagnóstico de mal funcionamiento	En la subsección **Configuración de Solución de problemas**, puede establecer la siguiente configuración: • Seleccione la opción **Habilitar seguimiento**. • Defina la **carpeta para los archivos de rastreo**. • Especifique el **Nivel de detalles**. • Especifique el **tamaño máximo de los archivos de rastreo**. • Seleccione la opción **Eliminar los archivos de rastreo más antiguos**. • Defina el **número máximo de archivos para un registro de rastreo**. La configuración de la directiva de grupo y la configuración local agregan parámetros coincidentes. Para más información sobre las opciones y sus limitaciones, vea la configuración de los ajustes locales. Puede establecer una serie de valores para los ajustes en el dispositivo local y otros valores diferentes en la directiva de grupo para varios dispositivos, con las siguientes consideraciones: • La configuración de la directiva de grupo del servidor de Kaspersky Security Center tiene mayor prioridad que la configuración local. • La configuración de la directiva de grupo del dispositivo local tiene menor prioridad que la configuración local.
Configuración de archivos de volcado	En la subsección **Configuración de archivos de volcado**, puede configurar las siguientes opciones según corresponda: • Seleccione la opción **Crear el archivo de volcado**. • Defina la **carpeta de archivos de volcado**. La configuración de la directiva de grupo y la configuración local agregan parámetros coincidentes. Para más información sobre las opciones y sus limitaciones, vea la configuración de los ajustes locales. Puede establecer una serie de valores para los ajustes en el dispositivo local y otros valores diferentes en la directiva de grupo para varios dispositivos, con las siguientes consideraciones: • La configuración de la directiva de grupo del servidor de Kaspersky Security Center tiene mayor prioridad que la configuración local.

	• La configuración de la directiva de grupo del dispositivo local tiene menor prioridad que la configuración local.

Historial de revisiones

En la sección **Historial de revisiones**, puede administrar revisiones: compararlas con la revisión actual u otra directiva, agregue descripciones de revisiones, guardar revisiones de un archivo o realizar una reversión.

Configuración de directivas

Para establecer la configuración de la directiva:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Expanda el grupo de administración, para el cual desee configurar las opciones de la directiva asociada, y abra la pestaña **Directivas** en el panel de detalles.
3. Haga clic en el nombre de la directiva que desea configurar.
4. Abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - Al seleccionar la opción **Propiedades** en el menú contextual de la directiva.
   - Al hacer clic en el vínculo **Configurar directiva** en el panel de detalles de la directiva seleccionada.
   - Al hacer doble clic en la directiva seleccionada.
5. En la pestaña **General** en la sección **Estado de la directiva**, habilite o deshabilite la directiva. Para esto, seleccione una de las siguientes opciones:
   - **Directiva activa**, si desea que la directiva se aplique en todos los dispositivos protegidos dentro del grupo de administración seleccionado.
   - **Directiva inactiva**, si desea activar la directiva más tarde en todos los dispositivos protegidos dentro del grupo de administración seleccionado.

   El parámetro **Directiva fuera de oficina** no está disponible cuando se administra Kaspersky Embedded Systems Security para Windows.
6. Vuelva a configurar la aplicación en otras secciones de la directiva.

Puede habilitar o deshabilitar la ejecución de cualquier tarea en todos los dispositivos protegidos dentro del grupo de administración mediante una directiva de Kaspersky Security Center.

Puede configurar la aplicación de la configuración de la directiva en todos los dispositivos protegidos en red para cada componente de la aplicación particular.

7. Haga clic en el botón **Aceptar**.

La configuración establecida se aplica en la directiva.

Creación y configuración de tareas con Kaspersky Security Center

Esta sección contiene información sobre las tareas de Kaspersky Embedded Systems Security para Windows y cómo crearlas, ajustar sus configuraciones, e iniciarlas y detenerlas.

Acerca de la creación de tareas en Kaspersky Security Center

Puede crear tareas de grupo para grupos de administración y conjuntos de dispositivos protegidos. Puede crear los siguientes tipos de tareas a través de Kaspersky Security Center:

- Activación de la aplicación
- Copia de actualizaciones
- Actualización de bases de datos
- Actualización de módulos del programa
- Reversión de la actualización de bases de datos
- Análisis a pedido
- Control de integridad de la aplicación
- Monitor comparativo de integridad de archivos
- Generador de reglas de Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos

Puede crear tareas de grupo y locales de las siguientes maneras:

- Para un dispositivo protegido: en la ventana **Propiedades <Nombre del dispositivo protegido>** en la sección **Tareas**.
- Para un grupo de administración: en el panel de detalles del nodo del grupo seleccionado de dispositivos protegidos en la pestaña **Tareas**.
- Para un conjunto de dispositivos protegidos: en el panel de detalles del nodo **Selecciones de dispositivos**.

Puede usar directivas para deshabilitar programaciones de tareas del sistema local de actualizaciones y de Análisis a pedido en todos los dispositivos protegidos desde el mismo grupo de administración.

Se proporciona información general sobre tareas en Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Creación de tareas mediante Kaspersky Security Center

Para crear una tarea nueva en la Consola de administración de Kaspersky Security Center:

1. Inicie el asistente de tareas de una de las siguientes maneras:

   - Para crear una tarea local:

     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración y seleccione el grupo al cual pertenezca el servidor protegido.

     b. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual del dispositivo protegido y seleccione **Propiedades**.

     c. En la ventana que se abre, haga clic en el botón **Agregar** en la sección **Tareas**.

   - Para crear una tarea de grupo:

     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

     b. Seleccione el grupo de administración para el cual desea crear una tarea.

     c. En el panel de resultados, abra la pestaña **Tareas** y seleccione **Crear una tarea**.

   - Para crear una tarea para un conjunto personalizado de dispositivos protegidos:

     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

     b. Seleccione el grupo de administración que contiene los dispositivos protegidos.

     c. Seleccione un dispositivo protegido o un conjunto personalizado de dispositivos protegidos.

     d. En la lista desplegable **Realizar acción**, seleccione la opción **Crear una tarea**.

   Se abre la ventana del asistente de tareas.

2. En la ventana **Seleccionar el tipo de tarea**, en el encabezado **Kaspersky Embedded Systems Security 3.3 para Windows**, seleccione el tipo de tarea que se creará.

3. Si selecciona cualquier tipo de tarea que no sea Reversión de la actualización de bases de datos, Control de integridad de la aplicación o Activación de la aplicación, se abrirá la ventana **Configuración**. Es posible que varíe la configuración según el tipo de tarea:

   - Cree una tarea de Análisis a pedido.

   - Para crear una tarea de actualización, configure los valores de la tarea según sus requisitos:

     a. Seleccione un origen de actualizaciones en la ventana **Origen de actualizaciones**.

     b. Haga clic en el botón **Configuración de conexión**. En la ventana **Configuración de conexión**, configure las opciones de acceso al servidor proxy al conectarse a la fuente de actualización.

- Para crear una tarea de Actualización de módulos del programa, configure los parámetros de actualización de módulos de la aplicación requeridos en la ventana **Configuración**:

  a. Seleccione una de estas opciones si desea copiar e instalar actualizaciones del módulo del programa críticas o solo comprobar su disponibilidad sin instalarlas.

  b. Si la opción **Copiar e instalar actualizaciones críticas de módulos del programa** está seleccionada: es posible que deba reiniciarse el dispositivo protegido para aplicar los módulos de software instalados. Si desea que Kaspersky Embedded Systems Security para Windows reinicie el dispositivo protegido automáticamente después de la finalización de la tarea, seleccione la casilla de verificación **Permitir el reinicio del sistema operativo**.

  c. Para obtener información sobre actualizaciones de módulos de Kaspersky Embedded Systems Security para Windows, seleccione **Informarme de las actualizaciones programadas que estén disponibles para los módulos del programa**.

  Kaspersky no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la instalación automática; se deben descargar manualmente desde el sitio web de Kaspersky. Es posible configurar una notificación de administrador del evento **Está disponible una nueva actualización programada de módulos del programa**. Esto incluirá la URL de nuestro sitio web desde donde puede descargar las actualizaciones programadas.

- Para crear la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la ventana **Configuración de la copia de actualizaciones**.

- Para crear la tarea de Activación de la aplicación:

  a. En la ventana **Configuración de la activación**, especifique el archivo de clave que desea usar para activar la aplicación.

  b. Seleccione la casilla de verificación **Usar como clave adicional** si desea crear una tarea para renovar la licencia.

- Cree la tarea de Generador de reglas de control de inicio de aplicaciones.

- Cree la tarea de Generador de reglas para Control de dispositivos.

4. Configure la programación de la tarea.

   Puede configurar una programación para todos los tipos de tareas excepto Reversión de la actualización de bases de datos.

5. Haga clic en el botón **Aceptar**.

6. Si la tarea se crea para un conjunto de dispositivos protegidos, seleccione la red (o el grupo) de los dispositivos protegidos en los que se ejecutará esta tarea.

7. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desee usar para ejecutar la tarea.

8. En la ventana **Especificar nombre de tarea**, especifique el nombre de la tarea (100 caracteres como máximo) que no contenga los símbolos " * < > ? \ | :.

   Le recomendamos agregar el tipo de tarea al nombre de la tarea (por ejemplo, "Análisis a pedido de carpetas compartidas").

9. En la ventana **Finalizando la creación de la tarea**, realice lo siguiente:

a. Seleccione la casilla de verificación **Ejecutar la tarea después de que finalice el asistente** si desea que la tarea se inicie tan pronto como se cree.

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

La tarea creada se mostrará en la lista **Tareas**.

Ir a los ajustes de una tarea local y a los ajustes generales de la aplicación para un equipo individual

Si una aplicación se encuentra sujeta a una directiva de Kaspersky Security Center y dicha directiva no permite cambiar los ajustes de la aplicación, no podrá modificar esos ajustes para un equipo puntual.

Para ir a los ajustes de una tarea local para un equipo puntual:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Seleccione el grupo al cual pertenece el dispositivo protegido.
3. En el panel de resultados, seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del dispositivo protegido.
   - En el menú contextual del nombre del dispositivo protegido, seleccione **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
5. Vaya a la sección **Tareas**.
6. En la lista de tareas, realice alguna de estas acciones para seleccionar la tarea local que desee configurar:
   - haga doble clic en el nombre de la tarea
   - seleccione la tarea en la lista y haga clic en el botón **Propiedades**
   - en el menú contextual del nombre de la tarea, seleccione **Propiedades**

   Se abre la ventana **Propiedades: <Nombre de la tarea>**.

Para ir a los ajustes generales de la aplicación para un equipo puntual:

1. Amplíe el nodo **Dispositivos administrados** en el árbol del Servidor de administración de Kaspersky Security Center y seleccione el grupo al cual pertenece el dispositivo protegido.
2. En el panel de resultados, seleccione la pestaña **Dispositivos**.
3. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del dispositivo protegido.

- En el menú contextual del nombre del dispositivo protegido, seleccione **Propiedades**.

Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.

4. Vaya a la sección **Aplicaciones**.
5. En la lista de aplicaciones instaladas, realice alguna de las siguientes acciones para seleccionar Kaspersky Embedded Systems Security para Windows:
   - haga doble clic en el nombre de Kaspersky Embedded Systems Security para Windows
   - seleccione Kaspersky Embedded Systems Security para Windows en la lista y haga clic en el botón **Propiedades**
   - en el menú contextual del nombre de Kaspersky Embedded Systems Security para Windows, seleccione el elemento **Propiedades**

   Se abre la ventana **Configuración** de **Kaspersky Embedded Systems Security para Windows**.

Configuración de tareas de grupo en Kaspersky Security Center

Cuando administra Kaspersky Embedded Systems Security para Windows desde Kaspersky Security Center Cloud Console, no puede agregar servidores HTTP y FTP o carpetas de red de forma manual.

Para configurar una tarea de grupo para varios dispositivos protegidos:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas.
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

   En la sección **Notificación**, configure las opciones de notificación del evento de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - Para configurar una tarea de Análisis a pedido:
     - En la sección **Área del análisis**, configure un área del análisis.

- En la sección **Opciones**, configure el nivel de prioridad de la tarea y la integración con otros componentes del programa.

- Para configurar una tarea de actualización, establezca los valores de la tarea según sus requisitos:
  - En la sección **Configuración**, establezca la configuración del origen de actualizaciones y la optimización del subsistema del disco.
  - Haga clic en el botón **Configuración de conexión** para configurar las opciones de conexión con el origen de actualizaciones.
- Para configurar la tarea de Actualización de módulos del programa:
  - Vaya a la sección **Configuración**.
  - Elija una acción a realizar: copiar e instalar actualizaciones críticas de módulos del programa o solo buscarlas.
- Para configurar la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la sección **Configuración de la copia de actualizaciones**.
- Para configurar una activación de la tarea Aplicación:
  - En la sección **Configuración de la activación**, especifique el archivo de clave que desea usar para activar la aplicación.
  - Seleccione la casilla de verificación **Usar como clave adicional** si desea agregar un código de activación o archivo de clave para renovar la licencia.
- Para configurar la generación automática de reglas de autorización para el Control de dispositivos, en la sección **Configuración** especifique la configuración que se utilizará para crear la lista de reglas de autorización.

6. Configure la programación de tareas en la sección **Programación**. Puede configurar una programación para todos los tipos de tareas excepto Reversión de la actualización de bases de datos.
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
9. Haga clic en el botón **Aceptar** en la ventana **Propiedades: <Nombre de la tarea>**.

Se guardan las opciones de la tarea de grupo recientemente configuradas.

Las opciones configurables de la tarea de grupo se resumen en la siguiente tabla.

Configuración de tareas de grupo de Kaspersky Embedded Systems Security para Windows

Tipos de tareas de Kaspersky Embedded Systems	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas

Security para Windows		
Generador de reglas de Control de inicio de aplicaciones	**Configuración**	Al configurar la tarea de Generador de reglas de Control de inicio de aplicaciones, puede seleccionar cómo crear las reglas de autorización: • **Crear reglas de autorización para las aplicaciones en ejecución** • **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**
	Opciones	Puede especificar las acciones que desea realizar mientras crea reglas de autorización de Control de inicio de aplicaciones: • **Usar certificado digital** • **Usar sujeto y huella digital del certificado digital** • **De no haber un certificado, usar** • **Usar hash SHA256** • **Generar reglas para este usuario o grupo de usuarios** Puede establecer la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security para Windows crea después de finalizar la tarea.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Generador de reglas para Control de dispositivos	**Configuración**	• Seleccione el modo de operación: tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado o tener en cuenta solo los dispositivos externos conectados actualmente. • Ajuste la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security para Windows crea después de finalizar la tarea.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Activación de la aplicación	**Configuración de la activación**	Para activar la aplicación o renovar la licencia, puede agregar un archivo de clave.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Copia de actualizaciones	**Origen de actualizaciones**	Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualizaciones de Kaspersky como un origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualizaciones de Kaspersky si los servidores personalizados manualmente no están disponibles.

	Ventana **Configuración de conexión**	En la ventana **Configuración de conexión** vinculada a la sección **Origen de actualizaciones**, puede especificar si se debe utilizar un servidor proxy para establecer la conexión con los servidores de actualizaciones de Kaspersky o con cualquier otro servidor.
	Configuración de la copia de actualizaciones	Puede especificar el conjunto de actualizaciones que desea copiar. En el campo **Carpeta de almacenamiento local para las actualizaciones copiadas**, especifique una ruta a la carpeta que Kaspersky Embedded Systems Security para Windows utilizará para almacenar las actualizaciones copiadas.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Actualización de bases de datos	**Configuración**	Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualizaciones de Kaspersky como un origen de actualizaciones de la aplicación en el cuadro de grupo **Origen de actualizaciones**. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualizaciones de Kaspersky si los servidores personalizados manualmente no están disponibles. En la sección Optimización de lectura y escritura en disco, puede configurar la función que reduce la carga de trabajo en el subsistema del disco: • **Reducir la carga de lectura y escritura en disco** • **RAM usada para la optimización (MB)**
	Ventana **Configuración de conexión**	En la ventana **Configuración de conexión** vinculada a la sección **Origen de actualizaciones**, puede especificar si se debe utilizar un servidor proxy para establecer la conexión con los servidores de actualizaciones de Kaspersky o con cualquier otro servidor.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Actualización de módulos del programa	**Origen de actualizaciones**	Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualizaciones de Kaspersky como un origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualizaciones de Kaspersky si los servidores personalizados manualmente no están disponibles.
	Ventana **Configuración de conexión**	En el cuadro de grupo **Configuración de la conexión al origen de actualizaciones** puede especificar si se debe utilizar un servidor proxy para establecer la conexión con los servidores de actualizaciones de Kaspersky o con cualquier otro servidor.
	Configuración	Puede especificar las acciones que Kaspersky Embedded Systems Security para Windows realizará cuando se necesiten actualizaciones críticas para los módulos de la aplicación y cuando se complete la instalación de tales actualizaciones. También puede indicar si

		Kaspersky Embedded Systems Security para Windows recibirá información sobre las actualizaciones programadas disponibles.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Configuración del análisis a pedido	**Área del análisis**	Puede especificar un área del análisis para la tarea de Análisis a pedido y configurar las opciones del nivel de seguridad.
	Ventana **Configuración del análisis a pedido**	En la ventana **Configuración del análisis a pedido** vinculada a la sección **Área del análisis**, puede seleccionar uno de los niveles de seguridad predefinidos o personalizar un nivel de seguridad manualmente.
	Opciones	En el bloque de opciones del **Analizador heurístico**, puede habilitar o deshabilitar el uso del analizador heurístico en la tarea Análisis a pedido y definir, mediante un control deslizante, el nivel de análisis que se usará. En el cuadro de grupo **Integración con otros componentes**, puede configurar los siguientes componentes: • Aplicar la zona de confianza para tareas de Análisis a pedido. • Aplicar el Uso de KSN para las tareas de Análisis a pedido. • Configurar una prioridad para la tarea de Análisis a pedido: ejecutar tarea en segundo plano (prioridad baja) o considerar la tarea de Análisis de áreas críticas.
	Programación	Puede configurar las opciones para iniciar la tarea en base a una programación.
Control de integridad de la aplicación	**Programación**	Puede configurar las opciones para iniciar la tarea en base a una programación.
Monitor comparativo de integridad de archivos	**Programación**	Puede configurar las opciones para iniciar la tarea en base a una programación.

Para la tarea Reversión de la actualización de bases de datos, puede establecer solo la configuración de la tarea estándar controlada por Kaspersky Security Center en las secciones **Notificación** y **Exclusiones del área de la tarea**.

Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

Activación de la tarea Aplicación

Para configurar una activación de la tarea Aplicación:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.

2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas.
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

   En la sección **Notificación**, configure las opciones de notificación del evento de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
5. En la sección **Configuración de la activación**, especifique el archivo de clave que desea usar para activar la aplicación. Active la casilla **Usar como clave adicional** si desea agregar una clave para renovar la licencia.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.
9. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

   Se guardan las opciones de la tarea de grupo recientemente configuradas.

Tareas de actualización

Para configurar las tareas Copia de actualizaciones, Actualización de bases de datos o Actualización de módulos del programa:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas.

- Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
- Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

En la sección **Notificación**, configure las opciones de notificación del evento de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. En la sección **Origen de actualizaciones**, realice lo siguiente:

   a. Seleccione el origen de actualizaciones:

   - Servidor de administración de Kaspersky Security Center.
   - Servidores de actualizaciones de Kaspersky.
   - Servidores FTP o HTTP personalizados o carpetas de red.

   Para usar una carpeta compartida de SMB como origen de actualizaciones, debe especificar una cuenta de usuario para iniciar una tarea.

   Puede especificar el uso de Servidores de actualizaciones de Kaspersky si los servidores personalizados manualmente no están disponibles.

   b. Haga clic en el botón **Configuración de conexión**.

   c. En la ventana **Configuración de conexión** que se abre, configure el uso de un servidor proxy para conectarse a servidores de actualizaciones de Kaspersky y otros servidores.

   d. Para la tarea Actualización de bases de datos, en la sección **Optimización de lectura y escritura en disco**, configure la función que reduce la carga de trabajo en el subsistema del disco:

   La sección **Optimización de lectura y escritura en disco** está disponible solo para la tarea Actualización de bases de datos.

   - **Reducir la carga de lectura y escritura en disco**
   - **RAM usada para la optimización (MB)**

6. Para la tarea Actualización de módulos del programa, en la sección **Configuración**, especifique qué acciones debe realizar Kaspersky Embedded Systems Security para Windows cuando hay actualizaciones críticas disponibles de módulos del programa o cuando la información acerca de actualizaciones planificadas está disponible.

   También puede especificar qué acciones debe realizar Kaspersky Embedded Systems Security para Windows cuando se instalan actualizaciones críticas.

La sección **Configuración** está disponible solo para la tarea Actualización de módulos del programa.

7. Para la tarea Copia de actualizaciones, en la sección **Configuración de la copia de actualizaciones**, especifique el grupo de actualizaciones y la carpeta de destino.

   La sección **Configuración de la copia de actualizaciones** está disponible solo para la tarea Copia de actualizaciones.

8. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).

9. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

10. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

Se guardan las opciones de la tarea de grupo recientemente configuradas.

Para la tarea Reversión de la actualización de bases de datos, puede establecer solo la configuración de la tarea estándar controlada por Kaspersky Security Center en las secciones **Notificaciones** y **Exclusiones del área de la tarea**. Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

Control de integridad de la aplicación

Para configurar la tarea de grupo Control de integridad de la aplicación:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.

2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.

3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar.

4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:

   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas.
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

   En la sección **Notificación**, configure las opciones de notificación del evento de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. En la sección **Dispositivos**, seleccione los dispositivos para los cuales desea configurar la tarea Control de integridad de la aplicación.

6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).

7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.

8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

9. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

   Se guardan las opciones de la tarea de grupo recientemente configuradas.

Configuración del diagnóstico de la interrupción en Kaspersky Security Center

Si ocurre un error durante el funcionamiento de Kaspersky Embedded Systems Security para Windows (por ejemplo, la aplicación se detiene), puede diagnosticarlo. Para tal fin, puede habilitar la creación de archivos de seguimiento y de un archivo de volcado para el proceso de Kaspersky Embedded Systems Security para Windows y enviar estos archivos al Servicio de soporte técnico para que sean analizados.

Kaspersky Embedded Systems Security para Windows no envía ningún archivo de volcado o rastreo automáticamente. Solo el usuario que posea los permisos requeridos podrá enviar datos de diagnóstico.

Kaspersky Embedded Systems Security para Windows escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security para Windows. Puede configurar los permisos de acceso y permitir que solo los usuarios necesarios puedan acceder a los registros, los archivos de rastreo y los archivos de volcado.

Para configurar el diagnóstico de interrupciones en Kaspersky Security Center:

1. En la Consola de administración de Kaspersky Security Center, abra la ventana **Configuración de la aplicación**.

2. Abra la sección **Diagnóstico de mal funcionamiento**.

3. Para registrar información de depuración en un archivo, en la sección **Configuración de resolución de problemas**, active la casilla **Habilitar seguimiento**.

4. En el campo **Carpeta de archivos de seguimiento**, indique la ruta absoluta a la carpeta local donde Kaspersky Embedded Systems Security para Windows guardará los archivos de seguimiento.

   La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

5. Configure el nivel de detalle de la información de depuración.

6. Especifique el **Tamaño máximo de los archivos de seguimiento (MB)**.

Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 50 MB.

7. Para que los archivos de seguimiento más antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.

8. Especifique el **Cantidad máxima de archivos para un registro de seguimiento**.

   Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. Para que este campo esté disponible, la casilla **Eliminar los archivos de seguimiento más antiguos** debe estar seleccionada.

9. Si desea que la aplicación cree un archivo de volcado de memoria, seleccione la casilla de verificación **Crear archivo de volcado**.

10. En el campo **Carpeta de archivos de volcado**, especifique la ruta absoluta a la carpeta local donde Kaspersky Embedded Systems Security para Windows guardará los archivos de volcado.

    La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. No puede indicar una carpeta de red, una unidad o una variable de entorno como ruta.

11. Haga clic en el botón **Aceptar**.

La configuración de la aplicación establecida se aplica en el dispositivo protegido.

Administración de programaciones de tareas

Puede programar tareas de Kaspersky Embedded Systems Security para Windows.

Tareas de programación

Puede programar las tareas personalizadas y las tareas locales del sistema en la Consola de la aplicación. No puede programar tareas de grupo en la Consola de la aplicación.

Para programar tareas de grupo mediante el Complemento de administración, realice lo siguiente:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

2. Seleccione el grupo al cual pertenece el dispositivo protegido.

3. En el panel de detalles, seleccione la pestaña **Tareas**.

4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:

   - Haga doble clic en el nombre de la tarea.
   - Abra el menú contextual del nombre de la tarea y seleccione el elemento Propiedades.

5. Seleccione la sección **Programación**.

6. En el bloque **Configuración de programación**, seleccione la casilla de verificación **Ejecutar según programación**.

Los campos con la configuración de programación para las tareas análisis a pedido y actualización no estarán disponibles si una directiva de Kaspersky Security Center bloquea la programación de estas tareas.

7. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:

   a. En la lista **Frecuencia**, seleccione uno de los siguientes valores:

   - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
   - **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
   - **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
   - **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security para Windows.
   - **Tras actualizarse las bases de datos**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

   b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

   c. En el campo **Fecha de inicio**, especifique la fecha de inicio de la programación.

   Luego de programar la hora de inicio, fecha y frecuencia de la tarea, se muestra el tiempo estimado hasta el próximo inicio.

   Vaya a la pestaña **Programación** y abra la ventana **Configuración de tareas**. En el campo **Próximo inicio** en la parte superior de la ventana, se muestra la hora de inicio estimada. Cada vez que abre la ventana, la hora estimada de inicio se actualiza y se muestra.

   El campo **Próximo inicio** muestra el valor **Bloqueado por directiva** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas locales del sistema programadas.

8. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos.

   - En la sección **Configuración de detención de tareas**:

     a. Seleccione la casilla de verificación **Duración** y, en los campos a la derecha, ingrese el número máximo de horas y minutos de la ejecución de la tarea.

     b. Seleccione la casilla de verificación **Pausar de** y, en los campos a la derecha, introduzca los valores de inicio y final de un intervalo de tiempo inferior a 24 horas durante el cual se detendrá la ejecución de la tarea.

   - En el bloque **Configuración avanzada**:

a. Seleccione la casilla de verificación **Cancelar programación desde** y especifique la fecha desde la cual la programación dejará de aplicar.

b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.

c. Seleccione la casilla de verificación **Aleatorizar la hora de inicio de la tarea usando un margen de** y especifique el valor en minutos.

9. Haga clic en el botón **Aceptar**.

10. Haga clic en el botón **Aplicar** para guardar la configuración del inicio de la tarea.

Si desea establecer la configuración de la aplicación para una sola tarea con Kaspersky Security Center, consulte la sección "Configuración de tareas locales en la ventana de configuración de la aplicación de Kaspersky Security Center".

Cómo habilitar y deshabilitar tareas programadas

Puede habilitar y deshabilitar tareas programadas antes o después de configurar las opciones de programación.

Para habilitar o deshabilitar la programación de inicio de tareas:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.

2. Seleccione el grupo al cual pertenece el dispositivo protegido.

3. En el panel de detalles, seleccione la pestaña **Tareas**.

4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:

   - Haga doble clic en el nombre de la tarea.
   - Abra el menú contextual del nombre de la tarea y seleccione el elemento Propiedades.

5. Seleccione la sección **Programación**.

6. Realice una de las siguientes opciones:

   - Seleccione la casilla de verificación **Ejecutar según programación** si desea habilitar el inicio programado de la tarea.
   - Cancele la selección de la casilla de verificación **Ejecutar según programación** si desea deshabilitar el inicio programado de la tarea.

   La programación configurada para la tarea no se eliminará y se aplicará la próxima vez que habilite el inicio de una tarea programada.

7. Haga clic en el botón **Aceptar**.

8. Haga clic en el botón **Aplicar**.

Se guardan las opciones de programación de inicio de tareas configuradas.

Informes en Kaspersky Security Center

Los informes en Kaspersky Security Center contienen información sobre el estado de dispositivos administrados. Los informes se basan en información almacenada en el Servidor de administración.

A partir de Kaspersky Security Center 11, los siguientes tipos de informes están disponibles para Kaspersky Embedded Systems Security para Windows:

- Informe sobre el estado de componentes de la aplicación
- Informe sobre aplicaciones prohibidas
- Informe sobre aplicaciones prohibidas en modo de prueba

Consulte la *Ayuda de Kaspersky Security Center* para obtener información detallada sobre todos los informes de Kaspersky Security Center y cómo configurarlos.

Informe de estado de los componentes de Kaspersky Embedded Systems Security para Windows

Puede supervisar el estado de protección de todos los dispositivos de red y acceder a un panorama estructurado del conjunto de componentes en cada dispositivo.

El informe muestra uno de los siguientes estados para cada componente: *En ejecución*, *En pausa*, *Detenido*, *Mal funcionamiento*, *No instalado*, *Iniciando*.

El estado *No instalado* hace referencia al componente, no a la aplicación. Si la aplicación no se instala, Kaspersky Security Center asigna el estado N/D (No disponible).

Puede crear selecciones de componentes y utilizar filtros para mostrar dispositivos de red con un conjunto especificado de componentes y su estado.

Consulte la *Ayuda de Kaspersky Security Center* para acceder a información detallada sobre la creación y el uso de selecciones.

Para revisar los estados de componentes en la configuración de la aplicación:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. Seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación**.
3. Seleccione la sección **Componentes**.
4. Revise la tabla de estado.

Para revisar un informe estándar de Kaspersky Security Center:

1. Seleccione el nodo **Servidor de administración <nombre del Servidor de administración>** en el árbol de la Consola de administración.
2. Abra la pestaña **Informes**.
3. Haga doble clic en el elemento de la lista **Informe sobre el estado de los componentes de la aplicación**.

   Se genera un informe.
4. Revise los siguientes detalles del informe:

   - Un diagrama gráfico.
   - Una tabla con un resumen de los componentes y los números sumados de los dispositivos de red donde se instala cada uno de los componentes, y los grupos a los que pertenecen.
   - Una tabla detallada donde se especifica el estado, la versión, el dispositivo y el grupo del componente.

Informes sobre aplicaciones prohibidas en los modos activo y de prueba

En base a los resultados de la tarea Control de inicio de aplicaciones, pueden generarse dos tipos de informes: un informe sobre las aplicaciones prohibidas (si la tarea se inicia en modo Activo) y un informe sobre las aplicaciones prohibidas en modo de prueba (si la tarea se inició en modo Solo estadísticas). Estos informes muestran información sobre las aplicaciones bloqueadas en los dispositivos protegidos de la red. Cada informe se genera para todos los grupos de administración y acumula datos de todas las aplicaciones de Kaspersky instaladas en los dispositivos protegidos.

Para revisar un informe sobre aplicaciones prohibidas en modo Solo estadísticas:

1. Ejecute la tarea Control de inicio de aplicaciones en el modo Solo estadísticas.

Seleccione el nodo **Servidor de administración <nombre del Servidor de administración>** en el árbol de la Consola de administración.

1. Abra la pestaña **Informes**.
2. Haga doble clic en el elemento **Informe sobre aplicaciones prohibidas en modo de prueba**.

   Se genera un informe.
3. Revise los siguientes detalles del informe:

   - Diagrama gráfico que muestra las diez primeras aplicaciones con el mayor número de inicios bloqueados.
   - Una tabla que resume los bloqueos de aplicaciones, donde se especifican el nombre del archivo ejecutable, el motivo, el tiempo de bloqueo y el número de dispositivos donde se bloqueó.
   - Una tabla detallada donde se especifican datos sobre el dispositivo, la ruta de acceso del archivo y el criterio para el bloqueo.

Para revisar un informe sobre aplicaciones prohibidas en modo Activo:

1. Ejecute la tarea Control de inicio de aplicaciones en el modo Activo.

2. Seleccione el nodo **Servidor de administración <nombre del Servidor de administración>** en el árbol de la Consola de administración.

3. Abra la pestaña **Informes**.

4. Haga doble clic en el elemento **Informe sobre aplicaciones prohibidas**.

   Se genera un informe.

Este informe consiste en los mismos datos sobre bloqueos que el informe sobre aplicaciones prohibidas en modo de prueba.

Cómo usar la Consola de Kaspersky Embedded Systems Security para Windows

Esta sección proporciona información sobre la Consola de Kaspersky Embedded Systems Security para Windows y describe cómo administrar la aplicación mediante la Consola de la aplicación instalada en el dispositivo protegido o en otro dispositivo.

Acerca de la Consola de Kaspersky Embedded Systems Security para Windows

La Consola de Kaspersky Embedded Systems Security para Windows es un complemento aislado que puede agregar a Microsoft Management Console.

Puede administrar la aplicación mediante la Consola de la aplicación instalada en el dispositivo protegido o en cualquier otro dispositivo de la red corporativa.

Después de haber instalado la Consola de la aplicación en otro dispositivo, se requiere la configuración avanzada.

Puede instalar la Consola de la aplicación y Kaspersky Embedded Systems Security para Windows en diferentes dispositivos protegidos asignados a diferentes dominios. En este caso, puede haber limitaciones en el envío de información desde la aplicación a la Consola de la aplicación. Por ejemplo, después de que se inicia cualquier tarea de la aplicación, su estado puede permanecer sin cambios en la Consola de la aplicación.

Al instalar la Consola de la aplicación, el asistente de instalación crea el archivo kavfs.msc en la carpeta de instalación y agrega el complemento de Kaspersky Embedded Systems Security para Windows a la lista de complementos aislados de Microsoft Windows.

Puede iniciar la Consola de la aplicación en el menú **Inicio**. El archivo msc del complemento de Kaspersky Embedded Systems Security para Windows puede ejecutarse o agregarse a la instancia de Microsoft Management Console como un nuevo elemento en el árbol.

En una versión de 64 bits de Microsoft Windows, el complemento de Kaspersky Embedded Systems Security para Windows solo puede agregarse en la versión de 32 bits de Microsoft Management Console. Para agregar el componente de Kaspersky Embedded Systems Security para Windows, abra Microsoft Management Console desde la línea de comandos con el comando: mmc.exe /32.

Se pueden agregar varios componentes de Kaspersky Embedded Systems Security para Windows a una Microsoft Management Console abierta en modo de autor. Luego, puede administrar la protección de varios dispositivos en los que está instalado Kaspersky Embedded Systems Security para Windows.

Interfaz de la Consola de Kaspersky Embedded Systems Security para Windows

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

Ventana Consola de Kaspersky Embedded Systems Security para Windows

La Consola de Kaspersky Embedded Systems Security para Windows se muestra como un nodo en el árbol de Microsoft Management Console.

Una vez que se establece conexión con una copia de Kaspersky Embedded Systems Security para Windows instalada en un dispositivo protegido diferente, el nombre del nodo se complementa con el nombre del dispositivo protegido en el que se instaló la aplicación y el nombre de la cuenta de usuario con la que se estableció la conexión: **Kaspersky Embedded Systems Security para Windows <nombre del dispositivo> como <nombre de la cuenta>**. Cuando la conexión se establece con una copia de Kaspersky Embedded Systems Security para Windows que se encuentra instalada en el mismo dispositivo protegido que la Consola de la aplicación, el nombre del nodo es **Kaspersky Embedded Systems Security para Windows**.

El árbol de la Consola de la aplicación

El árbol de la Consola de la aplicación muestra el nodo **Kaspersky Embedded Systems Security para Windows** y los nodos secundarios de los componentes funcionales de la aplicación.

El nodo de **Kaspersky Embedded Systems Security para Windows** incluye los siguientes nodos secundarios:

- **Protección del equipo en tiempo real**: administra las tareas de Protección del equipo en tiempo real y los servicios de KSN. El nodo **Protección del equipo en tiempo real** permite configurar las siguientes tareas:
  - **Protección de archivos en tiempo real**
  - **Uso de KSN**
  - **Prevención de exploits**
- **Control del equipo**: control de las aplicaciones que se ejecutan en el dispositivo protegido y en los dispositivos conectados. El nodo **Control del equipo** permite configurar las siguientes tareas:
  - **Control de inicio de aplicaciones**
  - **Control de dispositivos**
  - **Administración de firewall**
- **Generadores automatizados de reglas**: configuración de la generación automática de reglas del grupo y del sistema para las tareas Control de inicio de aplicaciones y Control de dispositivos.
  - **Generador de reglas de control de inicio de aplicaciones**
  - **Generador de reglas para Control de dispositivos**
  - Tareas de grupo de generación de reglas **<Nombres de las tareas>** (si corresponde)

    Las tareas del grupo se crean mediante Kaspersky Security Center. No puede administrar tareas de grupo a través de la Consola de la aplicación.
- **Inspección del sistema**: configuración del control de operaciones de archivos y configuración de inspección de Registros de eventos de Windows.

- **Monitor de integridad de archivos**
- **Inspección de registros**

- **Análisis a pedido**: administra las tareas de Análisis a pedido. Hay un nodo independiente para cada tarea:
  - **Análisis al inicio del sistema operativo**
  - **Análisis de áreas críticas**
  - **Análisis de archivos en cuarentena**
  - **Control de integridad de la aplicación**
  - Tareas personalizadas **<Nombres de las tareas>** (si corresponde)

  El nodo muestra tareas del sistema que se crean cuando la aplicación se instala, tareas personalizadas y tareas de grupo de análisis a pedido creadas y enviadas a un dispositivo protegido mediante Kaspersky Security Center.

- **Actualización**: administra las actualizaciones para los módulos y las bases de datos de Kaspersky Embedded Systems Security para Windows y copia las actualizaciones a una carpeta local de origen de actualizaciones. El nodo contiene nodos secundarios para administrar cada tarea de actualización y la tarea más reciente de **Reversión de la actualización de bases de datos de la aplicación**:
  - **Actualización de bases de datos**
  - **Actualización de módulos del programa**
  - **Copia de actualizaciones**
  - **Reversión de la actualización de bases de datos de la aplicación**

  El nodo muestra todas las tareas personalizadas y de actualización de grupo creadas y enviadas a un dispositivo protegido mediante Kaspersky Security Center.

- **Depósitos**: administración de ajustes de Cuarentena y de Copia de seguridad.
  - **Cuarentena**
  - **Copia de seguridad**

- **Registros y notificaciones**: administra registros de tareas locales, el registro de seguridad y el registro de auditoría del sistema de Kaspersky Embedded Systems Security para Windows.
  - **Registro de seguridad**
  - **Registro de auditoría del sistema**
  - **Registros de tareas**

- **Licencia**: permite agregar y eliminar claves de Kaspersky Embedded Systems Security para Windows y ver los detalles de la licencia.

Panel de detalles

El panel de detalles muestra información sobre el nodo seleccionado. Si se selecciona el nodo **Kaspersky Embedded Systems Security para Windows**, el panel de detalles muestra información sobre el estado de protección actual del dispositivo e información sobre Kaspersky Embedded Systems Security para Windows, el estado de protección de sus componentes funcionales y la fecha de caducidad de la licencia.

Menú contextual del nodo Kaspersky Embedded Systems Security para Windows

Puede usar los elementos del menú contextual del nodo **Kaspersky Embedded Systems Security para Windows** para realizar las operaciones siguientes:

- **Conectarse a otro equipo**. Conectarse a otro dispositivo para administrar las instancias de Kaspersky Embedded Systems Security para Windows instalados en él. También puede realizar esta operación si hace clic en el vínculo en la esquina inferior derecha del panel de detalles del nodo **Kaspersky Embedded Systems Security para Windows**.
- **Iniciar el servicio** / **Detener el servicio**. Iniciar o detener la aplicación o una tarea seleccionada. Para llevar a cabo estas operaciones, también puede usar los botones de la barra de herramientas. También puede realizar estas operaciones en los menús contextuales de tareas de la aplicación.
- **Configurar análisis de unidades extraíbles**. Configure el análisis de unidades extraíbles conectadas al dispositivo protegido a través del puerto USB.
- **Configurar los parámetros de Zona de confianza**. Consulte y configure las opciones de la Zona de confianza.
- **Modificar los derechos de usuario para administrar la aplicación**. Consulte y configure los permisos para acceder a las funciones de Kaspersky Embedded Systems Security para Windows.
- **Modificar los derechos de usuario para administrar el servicio de Kaspersky Security**. Vea y configure los derechos de usuario para administrar el servicio de Kaspersky Security.
- **Exportar configuración**. Guarde la configuración de la aplicación en un archivo de configuración con formato XML. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Importar configuración**. Importe los parámetros de la aplicación desde un archivo de configuración con formato XML. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Información acerca de la aplicación y las actualizaciones de módulos disponibles**. Vea información sobre Kaspersky Embedded Systems Security para Windows y las actualizaciones disponibles para los módulos de la aplicación.
- **Actualizar**. Actualice el contenido de la ventana Consola de la aplicación. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Propiedades**. Consulte y configure Kaspersky Embedded Systems Security para Windows o una tarea seleccionada. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.

  Para hacerlo, también puede usar el vínculo **Propiedades de la aplicación** en el panel de detalles del nodo **Kaspersky Embedded Systems Security para Windows** o usar el botón en la barra de herramientas.

- **Ayuda**. Consulte la información en la ayuda de Kaspersky Embedded Systems Security para Windows. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.

Barra de herramientas y menú contextual de las tareas de Kaspersky Embedded Systems Security para Windows

Puede administrar las tareas de Kaspersky Embedded Systems Security para Windows con los menús contextuales disponibles para cada tarea en el árbol de la Consola de la aplicación.

Puede usar los elementos del menú contextual para realizar las siguientes operaciones:

- **Iniciar/Detener**. Inicie o detenga la ejecución de tareas. Para llevar a cabo estas operaciones, también puede usar los botones de la barra de herramientas.
- **Reanudar/Pausar**. Reanuda o pausa la ejecución de tareas. Para llevar a cabo estas operaciones, también puede usar los botones de la barra de herramientas. Esta operación está disponible para las tareas de Protección del equipo en tiempo real y Análisis a pedido.
- **Agregar tarea**. Cree una nueva tarea personalizada. Esta operación está disponible para las tareas de Análisis a pedido.
- **Abrir registro**. Vea y administre el registro de la tarea. Esta operación está disponible para todas las tareas.
- **Eliminar tarea**. Elimine la tarea personalizada. Esta operación está disponible para las tareas de Análisis a pedido.
- **Plantillas de configuración**. Administre las plantillas. Esta operación está disponible para la Protección de archivos en tiempo real y Análisis a pedido.

Icono de la bandeja del sistema en el área de notificación

Cada vez que Kaspersky Embedded Systems Security para Windows se inicia automáticamente después del reinicio de un dispositivo protegido, el icono de la bandeja del sistema se muestra en el área de notificación de la barra de tareas  . Aparece de manera predeterminada si se instaló el componente del icono de la bandeja del sistema durante la instalación de la aplicación.

La apariencia del icono de la bandeja del sistema refleja el estado actual de la protección del dispositivo. Hay dos tipos de estados:

	Activo (icono en color) si se está ejecutando al menos una de estas tareas: Protección de archivos en tiempo real o Control de inicio de aplicaciones.
	Inactivo (icono gris) si ninguna de las tareas siguientes se encuentra en ejecución: Protección de archivos en tiempo real y Control de inicio de aplicaciones

Para abrir el menú contextual del icono de la bandeja del sistema, haga clic sobre él con el botón derecho.

El menú contextual ofrece diversos comandos para mostrar ventanas de aplicaciones (consulte la tabla a continuación).

Comandos del menú contextual en el icono de la bandeja del sistema

Comando	Descripción
Abrir la Consola de la aplicación	Abre la Consola de Kaspersky Embedded Systems Security para Windows (si está instalada).
Abrir Interfaz	Abre la Interfaz de diagnóstico compacto.

de diagnóstico compacto	
Acerca de la aplicación	Abre la ventana **Acerca de la aplicación** que contiene información sobre Kaspersky Embedded Systems Security para Windows. Para los usuarios registrados de Kaspersky Embedded Systems Security para Windows, la ventana **Acerca de la aplicación** contiene información sobre las actualizaciones urgentes que se instalaron.
Ocultar	Oculta el icono de la bandeja del sistema en el área de notificación de la barra de herramientas.

Puede volver a ver el icono de la bandeja del sistema oculto en cualquier momento.

Para volver a mostrar el Icono de la bandeja del sistema,

En el menú **Inicio** de Microsoft Windows, seleccione **Todos los programas** > **Kaspersky Embedded Systems Security para Windows** > **Ícono de la bandeja del sistema**.

Los nombres de configuración pueden variar en los diferentes sistemas operativos instalados.

En la configuración general de Kaspersky Embedded Systems Security para Windows, puede activar o desactivar la visualización del icono de la bandeja del sistema cada vez que la aplicación se inicia automáticamente después del reinicio de un dispositivo protegido.

Administración de Kaspersky Embedded Systems Security para Windows mediante la Consola de la aplicación en otro dispositivo

Puede administrar Kaspersky Embedded Systems Security para Windows mediante la Consola de la aplicación instalada en un dispositivo remoto.

Para administrar la aplicación con la Consola de Kaspersky Embedded Systems Security para Windows en un dispositivo remoto, asegúrese de lo siguiente:

- Los usuarios de la Consola de la aplicación en el dispositivo remoto se agregan al grupo de Administradores ESS en el dispositivo protegido.
- Las conexiones a la red se habilitan mediante el proceso del servicio de Kaspersky Security Management (kavfsgt.exe) si el firewall de Windows está habilitado en el dispositivo protegido.
- Durante la instalación de Kaspersky Embedded Systems Security para Windows, se selecciona la casilla de verificación **Permitir el acceso remoto** en la ventana del Asistente de instalación.

Si Kaspersky Embedded Systems Security para Windows en el dispositivo remoto está protegido con contraseña, ingrésela para acceder a la administración de aplicaciones mediante la Consola de la aplicación.

Configuración de las opciones generales de la aplicación a través de la Consola de la aplicación

La configuración general y la configuración del diagnóstico de mal funcionamiento de Kaspersky Embedded Systems Security para Windows establecen las condiciones generales operativas para la aplicación. Este parámetro le permite controlar el número de procesos de trabajo que utiliza Kaspersky Embedded Systems Security para Windows, habilitar la recuperación de las tareas de Kaspersky Embedded Systems Security para Windows después de una cancelación anormal, mantener el registro, habilitar la creación de archivos de volcado de los procesos de Kaspersky Embedded Systems Security para Windows después de una cancelación anormal y configurar otros parámetros generales.

Los ajustes de la aplicación no se pueden configurar en la Consola de la aplicación si la directiva activa de Kaspersky Security Center bloquea los cambios en estas opciones.

Para configurar Kaspersky Embedded Systems Security para Windows:

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security para Windows** y realice una de las siguientes acciones:

   - Haga clic en el vínculo **Propiedades de la aplicación** en el panel de detalles del nodo.
   - Seleccione **Propiedades** en el menú contextual del nodo.

   Se muestra la ventana **Configuración de la aplicación**.

2. En la ventana que se abre, configure las opciones generales de Kaspersky Embedded Systems Security para Windows de acuerdo con sus preferencias:

   - En la pestaña **Escalabilidad e interfaz**, se pueden configurar los valores siguientes:
     - En la sección **Configuración de escalabilidad**:
       - Número de procesos para la protección del equipo en tiempo real
       - Número de procesos de trabajo para tareas de Análisis a pedido en segundo plano
   - En la sección **Interacción con el usuario**, seleccione si se mostrará el icono de la bandeja del sistema en la barra de tareas después del inicio de cada aplicación.
   - En la pestaña **Seguridad y fiabilidad**, se pueden configurar los valores siguientes:
     - En la sección **Configuración de protección con contraseña**, configure la protección de los procesos de la aplicación.
     - En la sección **Configuración de protección con contraseña**, configure las opciones de acceso protegido por contraseña de las funciones de la aplicación.
     - En la sección **Defensa propia**, especifique el número de intentos para recuperar una tarea de Análisis a pedido si esta deja de funcionar.
   - En la sección **No recuperar tareas de análisis a pedido más de (veces)**, indique las acciones que realizará Kaspersky Embedded Systems Security para Windows cuando comience a utilizarse la energía de una UPS.
   - En la pestaña **Configuración del análisis**:
     - **Restaurar los atributos del archivo luego del análisis**

- Restringir el uso de CPU para los subprocesos del análisis
- Límite máximo (en porcentaje)
- Carpeta para los archivos temporales creados durante el análisis

- En la pestaña **Configuración de conexión**:
  - En la sección **Configuración del servidor proxy**, especifique la configuración del servidor proxy.
  - En la sección **Configuración de autenticación del servidor proxy**, especifique el tipo de autenticación y los detalles necesarios para la autenticación del servidor proxy.
  - En la sección **Licencia**, especifique si Kaspersky Security Center se usará como un servidor proxy para la activación de la aplicación.
- En la pestaña **Diagnóstico de mal funcionamiento**:
  - Si desea que la aplicación escriba información de depuración en un archivo, en la subsección **Configuración de Solución de problemas**, seleccione la casilla **Habilitar seguimiento**.
  - En el campo **Carpeta de archivos de seguimiento**, especifique la ruta absoluta a una carpeta local donde Kaspersky Embedded Systems Security para Windows guardará los archivos de seguimiento.

    La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.
  - Configure el nivel de detalle de la información de depuración.
  - Especifique el **tamaño máximo de los archivos de rastreo**.

    Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 50 MB.
  - Si desea que la aplicación elimine los archivos más antiguos una vez que se alcance el número máximo de archivos de rastreo, seleccione la casilla **Eliminar los archivos de rastreo más antiguos**.
  - Especifique el **número máximo de archivos para un registro de rastreo**.

    Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. El campo está disponible solo si la casilla **Eliminar los archivos de rastreo más antiguos** está seleccionada.
  - Si desea que la aplicación cree un archivo de volcado de memoria, seleccione la casilla de verificación **Crear archivo de volcado**.
  - En el campo **Carpeta de archivos de volcado**, especifique la ruta absoluta a una carpeta local donde Kaspersky Embedded Systems Security para Windows guardará el archivo de volcado.

    La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

Kaspersky Embedded Systems Security para Windows escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security para Windows. Puede configurar los permisos de acceso y permitir que solo los usuarios necesarios puedan acceder a los registros, los archivos de rastreo y los archivos de volcado.

3. Haga clic en el botón **Aceptar**.

Se guarda la configuración de Kaspersky Embedded Systems Security para Windows.

Administración de tareas de Kaspersky Embedded Systems Security para Windows

En esta sección, encontrará información sobre cómo crear, configurar, iniciar y detener tareas de Kaspersky Embedded Systems Security para Windows.

Categorías de tareas de Kaspersky Embedded Systems Security para Windows

Las funciones de Protección del equipo en tiempo real, Control del equipo, Análisis a pedido y Actualización en Kaspersky Embedded Systems Security para Windows se implementan como tareas.

Puede administrar estas tareas con el menú contextual de la tarea en el árbol de la Consola de la aplicación, la barra de herramientas y la barra de acceso rápido. Puede consultar información sobre el estado de la tarea en el panel de resultados. Las operaciones de administración de tareas se registran en el registro de auditoría del sistema.

Existen dos tipos de tareas de Kaspersky Embedded Systems Security para Windows: *locales* y *de grupo*.

Tareas locales

Las tareas locales solo pueden ejecutarse en el dispositivo protegido para el que fueron creadas. Según el método de inicio, existen los siguientes tipos de tareas locales:

- **Tareas locales del sistema**. Estas tareas se crean automáticamente durante la instalación de Kaspersky Embedded Systems Security para Windows. Puede modificar la configuración de todas las tareas locales del sistema, excepto las tareas Análisis de archivos en cuarentena y Reversión de la actualización de bases de datos. Las tareas locales del sistema no se pueden renombrar o eliminar. Puede ejecutar al mismo tiempo tareas de análisis a pedido personalizadas y locales del sistema.

- **Tareas locales personalizadas**. En la Consola de la aplicación, puede crear tareas de Análisis a pedido. En Kaspersky Security Center, puede crear tareas Análisis a pedido, Actualización de bases de datos, Reversión de la actualización de bases de datos y Copia de actualizaciones. Puede volver a nombrar, configurar y eliminar tareas personalizadas. Puede ejecutar varias tareas personalizadas simultáneamente.

Tareas de grupo

Puede administrar tareas de grupo y tareas para grupos de dispositivos protegidos desde Kaspersky Security Center. Todas las tareas de grupo son tareas personalizadas. Las tareas de grupo también se muestran en la Consola de la aplicación. En la Consola de la aplicación, solo puede ver el estado de las tareas de grupo. No puede usar la Consola de la aplicación para administrar o configurar tareas de grupo.

Cómo iniciar, pausar, reanudar y detener tareas manualmente

Solo puede pausar y reanudar las tareas Protección del equipo en tiempo real y Análisis a pedido. Ninguna otra tarea se puede pausar o reanudar de forma manual.

Para iniciar, pausar, reanudar o detener una tarea, realice lo siguiente:

1. En la Consola de la aplicación, abra el menú contextual de la tarea.
2. Seleccione una de las siguientes opciones: **Iniciar**, **Pausar**, **Reanudar** o **Detener**.

La operación se realiza y se registra en el Registro de auditoría del sistema.

Cuando reanuda una tarea Análisis a pedido, Kaspersky Embedded Systems Security para Windows reinicia el análisis desde el objeto en el que se encontraba al momento de la pausa.

Administración de programaciones de tareas

Puede programar tareas de Kaspersky Embedded Systems Security para Windows.

Configuración de las opciones de programación de tareas

En la Consola de la aplicación, puede programar el tiempo de inicio de tareas locales del sistema y tareas personalizadas. Sin embargo, no puede programar el tiempo de inicio de tareas de grupo.

Para programar una tarea, realice lo siguiente:

1. Abra el menú contextual de la tarea que quiere programar.
2. Seleccione **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
3. En la ventana que se abre, en la pestaña **Programación**, seleccione la casilla de verificación **Ejecutar según programación**.
4. Siga estos pasos para especificar la configuración de programación:

   a. En el menú desplegable **Frecuencia**, seleccione uno de los siguientes:

   - **Horaria**: para ejecutar la tarea con una frecuencia medida en horas; indique el número de horas a través del campo **Cada<número>hora(s)**.
   - **Diaria**: para ejecutar la tarea con una frecuencia medida en días; indique el número de días a través del campo **Cada<número>día(s)**.
   - **Semanal**: para ejecutar la tarea con una frecuencia medida en semanas; indique el número de semanas a través del campo **Cada<número>semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
   - **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security para Windows.

- **Tras actualizarse las bases de datos**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

c. En el campo **Fecha de inicio**, especifique la fecha para iniciar la tarea por primera vez.

Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La hora estimada del próximo inicio de la tarea se actualizará y mostrará cada vez que abra la ventana **Configuración de tareas** en la pestaña **Programación**.

El campo **Próximo inicio** muestra el valor **Bloqueado por directiva** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas locales del sistema programadas.

5. Use la pestaña **Avanzado** para especificar la siguiente configuración de programación:

- En la sección **Configuración de detención de tareas**:

a. Seleccione la casilla de verificación **Duración**. En los campos a la derecha, ingrese la duración máxima de la tarea en horas y minutos.

b. Seleccione la casilla de verificación **Pausar de**. En los campos a la derecha, especifique cuándo pausar y reanudar la tarea (menos de 24 horas).

- En el bloque **Configuración avanzada**:

a. Seleccione la casilla de verificación **Cancelar programación desde** y especifique la fecha de finalización de la programación de la tarea.

b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para iniciar las tareas omitidas.

c. Seleccione la casilla de verificación **Aleatorizar el inicio de la tarea usando un margen de** y especifique el valor en minutos.

6. Haga clic en el botón **Aceptar**.

Se guarda la configuración de programación de la tarea.

Cómo habilitar y deshabilitar tareas programadas

Puede habilitar y deshabilitar tareas programadas antes o después de configurar las opciones de programación.

Para habilitar o deshabilitar el inicio de una tarea programada, realice lo siguiente:

1. En el árbol de la Consola de la aplicación, abra el menú contextual para la tarea programada.

2. Seleccione **Propiedades**.

Aparece la ventana **Configuración de tareas**.

3. En la ventana que se abre, en la pestaña **Programación**, seleccione una de las siguientes opciones:

- Seleccione la casilla de verificación **Ejecutar según programación** si desea habilitar el inicio programado de la tarea.
- Cancele la selección de la casilla de verificación **Ejecutar según programación** si desea deshabilitar el inicio programado de la tarea.

  La programación configurada para la tarea no se eliminará y se aplicará la siguiente vez que habilite el inicio de una tarea programada.

4. Haga clic en el botón **Aceptar**.

Se guarda la configuración de programación de la tarea.

Uso de cuentas de usuario para iniciar tareas

Puede iniciar tareas con la cuenta de sistema o bien especificar una cuenta diferente.

Acerca del uso de cuentas para iniciar tareas

Puede especificar la cuenta para ejecutar las siguientes tareas de Kaspersky Embedded Systems Security para Windows:

- Generador de reglas de Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos
- Análisis a pedido
- Actualización

De forma predeterminada, estas taras se ejecutan según los permisos de la cuenta de sistema.

Se recomienda especificar una cuenta diferente con los permisos de acceso adecuados en los siguientes casos:

- Tarea **Actualización**: si definió una carpeta compartida de otro dispositivo de la red como origen de actualizaciones.
- Tarea **Actualización**: si utiliza un servidor proxy con autenticación NTLM de Windows incorporada para acceder al origen de actualizaciones.
- Tareas de **análisis a pedido**: si la cuenta de sistema no posee permiso para acceder a los objetos analizados (por ejemplo, archivos en carpetas compartidas en el dispositivo protegido).
- Tarea **Generador de reglas de Control de inicio de aplicaciones**: si las reglas generadas se exportan a un archivo de configuración al cual la cuenta de sistema no puede acceder (por ejemplo, en una carpeta compartida en el dispositivo protegido).

Puede ejecutar tareas de Actualización, Análisis a pedido y Generador de reglas de Control de inicio de aplicaciones con los permisos de la cuenta de sistema. Kaspersky Embedded Systems Security para Windows realiza estas tareas y accede a las carpetas compartidas en otro dispositivo en la red si este dispositivo está registrado en el mismo dominio que el dispositivo protegido. En este caso, la cuenta del sistema debe tener permisos de acceso a estas carpetas. Kaspersky Embedded Systems Security accede al dispositivo mediante los permisos de la cuenta **<nombre de dominio \ nombre_de_dispositivo>**.

Especificación de una cuenta de usuario para iniciar una tarea

Para especificar una cuenta para iniciar una tarea:

1. En el árbol de la Consola de la aplicación, abra el menú contextual de la tarea para la cual desea comenzar con el uso de una cuenta específica.
2. Seleccione **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
3. En la ventana que se abre, en la pestaña **Ejecutar como**, siga estos pasos:
   a. Seleccione **Nombre de usuario**.
   b. Escriba el nombre de usuario y la contraseña de la cuenta que desea usar.

      El usuario seleccionado debe estar registrado en el dispositivo protegido o en el mismo dominio que este equipo.

   c. Confirme la contraseña.
4. Haga clic en el botón **Aceptar**.

La configuración modificada se guarda.

Cómo importar y exportar la configuración

En esta sección, se explica cómo exportar la configuración de Kaspersky Embedded Systems Security para Windows. También aprenderá cómo exportar una configuración de software específica a un archivo de configuración XML y cómo importarla desde un archivo de configuración a la aplicación.

Acerca de la importación y exportación de la configuración

Puede exportar la configuración de Kaspersky Embedded Systems Security para Windows a un archivo de configuración XML e importar los parámetros a Kaspersky Embedded Systems Security para Windows desde el archivo de configuración. Puede guardar todos los ajustes de la aplicación o únicamente los ajustes de componentes individuales a un archivo de configuración.

Cuando exporta toda la configuración de Kaspersky Embedded Systems Security para Windows a un archivo, se guarda la configuración de la aplicación general y la configuración de los siguientes componentes y funciones de Kaspersky Embedded Systems Security para Windows:

- Protección de archivos en tiempo real
- Uso de KSN
- Control de dispositivos
- Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos
- Generador de reglas de Control de inicio de aplicaciones
- Tareas de Análisis a pedido
- Monitor de integridad de archivos
- Inspección de registros
- Base de datos y actualización de módulos del programa de Kaspersky Embedded Systems Security para Windows
- Cuarentena
- Copia de seguridad
- Registros
- Notificaciones de administrador y usuario
- Zona de confianza
- Prevención de exploits
- Protección con contraseña

Además, se puede guardar la configuración general de Kaspersky Embedded Systems Security para Windows en el archivo, así como los derechos de las cuentas de usuario.

No puede exportar la configuración de la tarea de grupo.

Kaspersky Embedded Systems Security para Windows exporta todas las contraseñas usadas por la aplicación, por ejemplo, la configuración de la cuenta de usuario para ejecutar tareas o conectarse a un servidor proxy. Las contraseñas exportadas se guardan en forma cifrada en el archivo de configuración. Puede importar contraseñas solo usando Kaspersky Embedded Systems Security para Windows instalado en este dispositivo protegido si no se ha instalado de nuevo ni se ha actualizado.

No puede importar contraseñas guardadas anteriormente con Kaspersky Embedded Systems Security para Windows instalado en un dispositivo protegido diferente. Tras importar la configuración en el dispositivo protegido, deberá introducir todas las contraseñas manualmente.

Si una directiva de Kaspersky Security Center está activa en el momento de la exportación, la aplicación exporta los valores especificados usados por esa directiva.

Se pueden importar ajustes de un archivo de configuración que contenga ajustes para componentes individuales de Kaspersky Embedded Systems Security para Windows (por ejemplo, de un archivo creado en una copia de Kaspersky Embedded Systems Security para Windows que se ha instalado con un juego de componentes incompleto). Después de la importación de la configuración, solo se modifican los parámetros de Kaspersky Embedded Systems Security para Windows incluidos en el archivo de configuración. Todos los demás parámetros permanecen iguales.

La configuración de una directiva activa de Kaspersky Security Center que se ha bloqueado no cambia al importar la configuración.

Exportación de la configuración

Para exportar configuraciones a un archivo de configuración:

1. En el árbol de la Consola de la aplicación, realice una de las siguientes acciones:

   - En el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**, seleccione **Exportar configuración** para exportar toda la configuración de Kaspersky Embedded Systems Security para Windows.
   - En el menú contextual de una tarea específica, seleccione **Exportar configuración** para exportar la configuración de un componente funcional e individual de la aplicación.
   - Para exportar la configuración de la Zona de confianza, realice lo siguiente:

     a. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.

     b. Seleccione **Configurar los parámetros de Zona de confianza**.

     Se abre la ventana **Zona de confianza**.

     c. Haga clic en el botón **Exportar**.

     Se abre el Asistente de exportación de configuración.

2. Siga las instrucciones en el **Asistente de exportación de configuración**: especifique el nombre y la ruta de acceso del archivo de configuración que desee usar para guardar la configuración.

   Puede usar variables de entorno del sistema cuando especifica la ruta, pero no puede usar variables de entorno de usuarios.

   Si una directiva de Kaspersky Security Center está activa en el momento de la exportación, la aplicación exporta la configuración usada por esa directiva.

3. Haga clic en el botón **Finalizó la exportación de la configuración de la aplicación** en la ventana **Cerrar**.

El Asistente de exportación de configuración se cierra y guarda la configuración de exportación.

Importación de la configuración

Para importar configuraciones desde un archivo de configuración guardado:

1. En el árbol de la Consola de la aplicación, realice una de las siguientes acciones:

   - En el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**, seleccione **Importar configuración** para importar todos los parámetros de Kaspersky Embedded Systems Security para Windows.
   - En el menú contextual de una tarea específica, seleccione **Importar configuración** para importar la configuración de un componente funcional e individual de la aplicación.
   - Para importar la configuración de la Zona de confianza, realice lo siguiente:

     a. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.

     b. Seleccione **Configurar los parámetros de Zona de confianza**.

     Se abre la ventana **Zona de confianza**.

     c. Haga clic en el botón **Importar**.

     Se abre el Asistente de importación de configuración.

2. Siga las instrucciones en el **Asistente de importación de configuración**: especifique el archivo de configuración con la configuración que desea importar.

   Después de importar la configuración general de Kaspersky Embedded Systems Security para Windows o la configuración funcional de los componentes en el dispositivo protegido, no puede volver a la configuración anterior.

3. Haga clic en el botón **Finalizó la importación de la configuración de la aplicación** en la ventana **Cerrar**.

   El Asistente de importación de configuración se cierra y guarda la configuración importada.

4. En la barra de tareas de la Consola de la aplicación, haga clic en el botón **Actualizar**.

La ventana de la Consola de la aplicación muestra la configuración importada.

Kaspersky Embedded Systems Security para Windows no importa contraseñas (credenciales de la cuenta utilizada para iniciar tareas o establecer conexión con el servidor proxy) de un archivo creado en otro dispositivo protegido o en el mismo dispositivo protegido después de que Kaspersky Embedded Systems Security para Windows se haya reinstalado o actualizado. Después de finalizar la importación, las contraseñas deben ingresarse manualmente.

Uso de plantillas de configuración de seguridad

Esta sección contiene información sobre el uso de las plantillas de configuración de seguridad en las tareas de análisis y protección de Kaspersky Embedded Systems Security para Windows.

Acerca de las plantillas de configuración de seguridad

Puede configurar manualmente los ajustes de seguridad de un nodo en el árbol o en una lista de recursos del archivo del dispositivo protegido y guardar los valores de ajuste configurados como plantilla. Esta plantilla se puede utilizar entonces para especificar las opciones de seguridad de otros nodos en las tareas de análisis y protección de Kaspersky Embedded Systems Security para Windows.

Puede usar plantillas para especificar las opciones de seguridad de las siguientes tareas de Kaspersky Embedded Systems Security para Windows:

- Protección de archivos en tiempo real
- Análisis al inicio del sistema operativo
- Análisis de áreas críticas
- Tareas de Análisis a pedido

La configuración de seguridad de una plantilla aplicada a un nodo principal en el árbol de recursos de archivos del dispositivo protegido se aplica en todos los nodos secundarios. La plantilla del nodo principal no se aplica a nodos secundarios en los casos siguientes:

- Si especificó la configuración de seguridad de los nodos secundarios por separado.
- Si los nodos secundarios son virtuales. En este caso, debe aplicar la plantilla a cada nodo virtual por separado.

Creación de una plantilla de configuración de seguridad

Para guardar manualmente la configuración de seguridad de un nodo en una plantilla:

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desee crear la plantilla de configuración de seguridad.
2. En el panel de detalles de la tarea seleccionada, haga clic en el vínculo **Configurar el área de protección** o **Configurar el área de análisis**.
3. En el árbol o lista de los recursos de archivos en red del dispositivo protegido, seleccione la plantilla que desee visualizar.
4. En la pestaña **Nivel de seguridad**, haga clic en el botón **Guardar como plantilla**.

   Se abre la ventana **Propiedades de la plantilla**.
5. En el campo **Nombre de la plantilla**, ingrese el nombre de la plantilla.
6. En el campo **Descripción**, ingrese información adicional de la plantilla.
7. Haga clic en el botón **Aceptar**.

Se guarda la plantilla de configuración de seguridad.

Visualización de la configuración de seguridad en una plantilla

Para ver la configuración de seguridad en una plantilla que creó, realice lo siguiente:

1. En el árbol de la Consola de la aplicación, seleccione la tarea con la plantilla de configuración de seguridad que desee ver.
2. En el menú contextual de la tarea seleccionada, seleccione **Plantillas de configuración**.

   Se abre la ventana **Plantillas**.
3. En la lista de plantillas, seleccione la plantilla que desee ver.
4. Haga clic en el botón **Ver**.

Se abre la ventana **<Nombre de la plantilla>**. La pestaña **General** muestra el nombre de la plantilla e información adicional sobre la plantilla. La pestaña **Opciones** enumera las configuraciones de seguridad guardadas en la plantilla.

Aplicación de una plantilla de configuración de seguridad

Para aplicar la configuración de seguridad de una plantilla a un nodo seleccionado:

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desea aplicar una plantilla de configuración de seguridad.
2. En el panel de detalles de la tarea seleccionada, haga clic en el vínculo **Configurar el área de protección** o **Configurar el área de análisis**.
3. En el árbol o lista de los recursos de archivos en red del dispositivo protegido, abra el menú contextual del nodo o del elemento al cual desee aplicar la plantilla.
4. Seleccione **Aplicar plantilla** → **<Nombre de la plantilla>**.
5. Haga clic en el botón **Guardar**.

Esto aplica la plantilla de configuración de seguridad al nodo seleccionado en el árbol de recursos del archivo del dispositivo protegido. El valor en la pestaña **Nivel de seguridad** para el nodo seleccionado cambia a **Personalizado**.

Si la configuración de seguridad de una plantilla se aplica a un nodo principal en el árbol de recursos de archivos del dispositivo protegido, esta configuración se aplica a todos los nodos secundarios.

Puede configurar la protección o el alcance del análisis para nodos secundarios en el árbol de recursos del archivo del dispositivo protegido por separado. En este caso, la configuración de seguridad de la plantilla aplicada al nodo principal no se aplica de forma automática a los nodos secundarios.

Para aplicar la configuración de seguridad de una plantilla a todos los nodos seleccionados:

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desea aplicar una plantilla de configuración de seguridad.
2. En el panel de detalles de la tarea seleccionada, haga clic en el vínculo **Configurar el área de protección** o **Configurar el área de análisis**.
3. En el árbol o lista de los recursos de archivos en red del dispositivo protegido, seleccione un nodo principal para aplicar la plantilla al nodo seleccionado y a los nodos secundarios.
4. En el menú contextual, seleccione **Aplicar plantilla → <Nombre de la plantilla>**.
5. Haga clic en el botón **Guardar**.

La plantilla de configuración de seguridad se aplica a los nodos principales y a todos los nodos secundarios en el árbol de recursos de archivos del dispositivo protegido. El valor en la pestaña **Nivel de seguridad** para el nodo seleccionado cambia a **Personalizado**.

Eliminación de una plantilla de configuración de seguridad

Para eliminar una plantilla de configuración de seguridad:

1. En el árbol de la Consola de la aplicación, seleccione la tarea con la plantilla de configuración de seguridad que desea eliminar.
2. En el menú contextual de la tarea seleccionada, seleccione **Plantillas de configuración**.

   Se abre la ventana **Plantillas**.

   En el panel de resultados del nodo principal de **Análisis a pedido**, puede ver plantillas de configuración para tareas de análisis a pedido.
3. En la lista de plantillas, seleccione la plantilla que desee eliminar.
4. Haga clic en el botón **Eliminar**.

   Se abre una ventana para confirmar la eliminación.
5. En la ventana que se abre, haga clic en **Sí**.

La plantilla seleccionada se elimina.

Puede aplicar la plantilla de configuración de seguridad para proteger o analizar nodos en el árbol de recursos del archivo del dispositivo protegido. En este caso, la configuración de seguridad para dichos nodos permanece sin cambios luego de la eliminación de la plantilla.

Consultar el estado de protección e información de Kaspersky Embedded Systems Security para Windows

Para consultar información sobre el estado de protección del dispositivo de Kaspersky Embedded Systems Security para Windows,

seleccione el nodo **Kaspersky Embedded Systems Security para Windows** en el árbol de la Consola de la aplicación.

De forma predeterminada, la información en el panel de detalles de la Consola de la aplicación se actualiza automáticamente:

- Cada 10 segundos en caso de una conexión local.
- Cada 15 segundos en caso de una conexión remota.

La información se puede actualizar en forma manual.

*Para actualizar la información del nodo **Kaspersky Embedded Systems Security para Windows** de forma manual,*

seleccione el comando **Actualizar** del menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.

La siguiente información de la aplicación se muestra en el panel de detalles de la Consola de la aplicación:

- Estado de Uso de Kaspersky Security Network.
- Estado de Protección del dispositivo.
- Información sobre las actualizaciones del módulo de aplicación y la base de datos.
- Datos de diagnóstico reales.
- Datos sobre las tareas de control de dispositivos protegidos.
- Información sobre la licencia.
- Estado de integración con Kaspersky Security Center: los detalles del servidor que tiene Kaspersky Security Center instalado y al cual se ha conectado la aplicación e información sobre las tareas de la aplicación que se encuentran controladas por la directiva activa.

El estado de protección se representa mediante el siguiente esquema de colores:

- *Verde*. La tarea se está ejecutando de acuerdo con los parámetros configurados. La protección está activa.
- *Amarillo*. La tarea no se inició, se pausó o se detuvo. Pueden ocurrir amenazas para la seguridad. Se le aconseja configurar e iniciar la tarea.
- *Rojo*. Se detectó una tarea completada con un error o una amenaza para la seguridad mientras la tarea se ejecutaba. Se le aconseja iniciar la tarea o tomar medidas para eliminar la amenaza de la seguridad detectada.

Algunos detalles en este bloque (por ejemplo, los nombres de las tareas o el número de amenazas detectadas) son vínculos que, cuando se hace clic en ellos, abren el nodo de la tarea relevante o abren el registro de tareas.

La sección **Uso de Kaspersky Security Network** muestra el estado de la tarea actual, por ejemplo, *En ejecución*, *Detenida* o *Nunca ejecutada*. El indicador puede tener los siguientes valores:

- El color verde significa que la tarea Uso de KSN se está ejecutando y las solicitudes de estado de archivos están enviando a KSN.

- El color amarillo significa que se acepta una de las declaraciones, pero la tarea no está en ejecución; o bien que la tarea está en ejecución, pero no se envían solicitudes de archivos a KSN.

Protección del equipo

La sección **Protección del equipo** (consulte la tabla a continuación) muestra información sobre el estado de protección actual del dispositivo.

Información sobre el estado de protección del dispositivo

Sección Protección	Información
Indicador del estado de protección del dispositivo	El color del panel con el nombre de la sección refleja el estado de las tareas realizadas en dicha sección. El indicador puede tener los siguientes valores: • Verde – Este color se muestra de forma predeterminada y significa que el componente Protección de archivos en tiempo real está instalado y la tarea está en ejecución. • Amarillo – El componente Protección de archivos en tiempo real no está instalado, y la tarea Análisis de áreas críticas no se ha realizado hace mucho tiempo. • Rojo – La tarea Protección de archivos en tiempo real no está en ejecución.
Protección de archivos en tiempo real	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Detectado**: número de objetos que detectó Kaspersky Embedded Systems Security para Windows. Por ejemplo, si Kaspersky Embedded Systems Security para Windows detecta una misma aplicación maliciosa en cinco archivos, el valor de este campo aumenta en uno. Si el número de aplicaciones maliciosas detectadas supera 0, el valor se resalta en rojo.
Análisis de áreas críticas	**Fecha del último análisis**: fecha y hora del último Análisis de áreas críticas en busca de virus y otras amenazas de seguridad informática. *Nunca ejecutada*: evento que ocurre cuando la tarea de Análisis de áreas críticas no se ha ejecutado en treinta días o más (valor predeterminado). Se puede cambiar el umbral para la generación de este evento.
Prevención de exploits	**Estado**: el estado actual de las técnicas de prevención de exploits, por ejemplo, *Aplicada* o *No aplicado*. **Modo de prevención**: uno de los dos modos disponibles, seleccionados durante la configuración de la protección de la memoria del proceso: **Finalizar en caso de exploit** o **Solo estadísticas**. **Procesos protegidos**: el número total de procesos agregados al área de protección y gestionados de acuerdo con el modo seleccionado.
Objetos guardados en Copia de seguridad	*Se superó el umbral de espacio disponible para Copia de seguridad*: este evento se produce cuando la cantidad de espacio libre en Copia de seguridad se está acercando al límite especificado. Kaspersky Embedded Systems Security para Windows continúa trasladando los objetos a Copia de seguridad. En este caso, el valor en el campo **Espacio usado** se resalta en amarillo. *Se superó el tamaño máximo de Copia de seguridad*: este evento ocurre cuando el tamaño de Copia de seguridad alcanza el límite especificado. Kaspersky Embedded Systems Security para Windows continúa trasladando los objetos a Copia de seguridad. En este caso, el valor en el campo **Espacio usado** se resalta en rojo. **Objetos guardados en Copia de seguridad**: cantidad de objetos que se encuentran actualmente en Copia de seguridad. **Espacio usado**: cantidad de espacio de Copia de seguridad que ya se ha utilizado.

Actualización

La sección **Actualización** (consulte la siguiente tabla) muestra qué tan actuales son las bases de datos antivirus y los módulos de la aplicación.

Información sobre el estado de los módulos y las bases de datos de Kaspersky Embedded Systems Security para Windows

Sección Actualización	Información
Indicador del estado de las bases de datos y los módulos de software	El color del panel con el nombre de la sección refleja el estado de las bases de datos y los módulos de la aplicación. El indicador puede tener los siguientes valores: • Verde: este color se muestra de forma predeterminada, y significa que las bases de datos de la aplicación están actualizadas y que la última tarea de actualización de bases de datos se completó correctamente. • Amarillo: las bases de datos están desactualizadas o la última tarea de actualización de bases de datos produjo un error. • Rojo: se produjo el evento *Las bases de datos de la aplicación son obsoletas* o *Las bases de datos de la aplicación están dañadas*.
Actualización de bases de datos y **Actualización de módulos del programa**	**Estado de las bases de datos**: evaluación del estado de actualización de las bases de datos. La opción puede tener los siguientes valores: • **Las bases de datos de la aplicación están actualizadas**: las bases de datos de la aplicación se actualizaron en los siete días anteriores (predeterminado). • **Las bases de datos de la aplicación están desactualizadas**: las bases de datos de la aplicación se actualizaron en los siete a catorce días anteriores (predeterminado). • **Las bases de datos de la aplicación son obsoletas**: las bases de datos de la aplicación se actualizaron hace más de 14 días (predeterminado). Se pueden cambiar los umbrales para la generación de los eventos *Las bases de datos de la aplicación están actualizadas* y *Las bases de datos de la aplicación son obsoletas*. **Fecha de lanzamiento de las bases de datos**: fecha y hora en que se publicó la actualización de bases de datos más reciente. La fecha y la hora se especifican en formato UTC. **Estado de la última actualización de bases de datos**: fecha y hora de la última actualización de bases de datos. La fecha y hora se especifican de acuerdo con la hora local del dispositivo protegido. El campo aparece de color rojo si se produjo un evento con *Error*. **Actualizaciones de módulos disponibles**: número de actualizaciones de módulos de Kaspersky Embedded Systems Security para Windows que están disponibles para descargar e instalar. **Actualizaciones de módulos instaladas**: número de actualizaciones de módulos de Kaspersky Embedded Systems Security para Windows que se han instalado.

Control

La sección **Control** (consulte la tabla a continuación) muestra información sobre las tareas Control de inicio de aplicaciones, Control de dispositivos y Administración de firewall.

Información sobre el estado de control de dispositivos protegidos

Sección Control	Información
Indicador de estado para el Control de dispositivos protegidos	El color del panel con el nombre de la sección refleja el estado de las tareas realizadas en dicha sección. El indicador puede tener los siguientes valores: • Verde: este color se muestra de forma predeterminada y significa que el componente Control de inicio de aplicaciones está instalado y la tarea se está ejecutando en el modo **Activo**. • Amarillo: Control de inicio de aplicaciones se está ejecutando en el modo **Solo estadísticas**. • Rojo: la tarea Control de inicio de aplicaciones no está en ejecución o ha generado errores.
Control de inicio de aplicaciones	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Modo de operación**: uno de los dos modos disponibles para la tarea Control de inicio de aplicaciones: **Activo** o **Solo estadísticas**. **Inicios de aplicaciones denegados**: número de veces que Kaspersky Embedded Systems Security para Windows bloqueó la ejecución de una aplicación mientras la tarea de Control de inicio de aplicaciones estaba en funcionamiento. Si el número de inicios de aplicaciones bloqueados supera 0, el campo se muestra en rojo. **Tiempo promedio de procesamiento (ms)**: tiempo que le tomó a Kaspersky Embedded Systems Security para Windows procesar un intento de iniciar aplicaciones en el dispositivo protegido.
Control de dispositivos	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Modo de operación**: uno de los dos modos disponibles para la tarea Control de dispositivos: **Activo** o **Solo estadísticas**. **Dispositivos bloqueados**: el número de intentos de conexión de un dispositivo externo que fueron bloqueados por Kaspersky Embedded Systems Security para Windows durante la tarea Control de dispositivos. Si el número de dispositivos externos bloqueados supera 0, el valor del campo se muestra en rojo.
Administración de firewall	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Intentos de conexiones bloqueados**: número de conexiones a un dispositivo protegido que fueron bloqueadas por las reglas especificadas en el firewall.

Diagnósticos

La sección **Diagnósticos** (consulte la tabla a continuación) muestra información sobre las tareas Inspección de registros y Monitor de integridad de archivos.

Información sobre estado de inspección del sistema

Sección Diagnósticos	Información
Indicador de estado del diagnóstico	El color del panel con el nombre de la sección refleja el estado de las tareas realizadas en dicha sección. El indicador puede tener los siguientes valores: • Verde: este color se muestra de forma predeterminada y significa que uno o los dos componentes de inspección del sistema están instalados y las tareas están en ejecución.

	• Amarillo: los dos componentes están instalados, pero una de las tareas de inspección del sistema no está en ejecución; ocurre el evento *No está en ejecución*. • Rojo: una de las tareas tuvo un error.
Monitor de integridad de archivos	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Operaciones de archivos no sancionadas**: número de cambios en archivos del área de supervisión. Estos cambios pueden indicar que la seguridad de un dispositivo protegido ha sido violada.
Inspección de registros	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Infracciones de las reglas configuradas**: número de infracciones registradas según datos del registro de eventos de Windows. Este número se determina según las reglas de la tarea especificadas o el uso del analizador heurístico.

La información sobre la licencia de Kaspersky Embedded Systems Security para Windows se muestra en la fila ubicada en la esquina inferior izquierda del panel de detalles del nodo **Kaspersky Embedded Systems Security para Windows**.

Puede configurar las propiedades de Kaspersky Embedded Systems Security para Windows a través del vínculo **Propiedades de la aplicación**.

Puede conectarse a otro dispositivo protegido a través del vínculo **Conectarse a otro equipo**.

Trabajo con el complemento web desde Web Console y Cloud Console

Esta sección proporciona información sobre el Complemento de administración de Kaspersky Embedded Systems Security para Windows y describe cómo administrar la aplicación instalada en un dispositivo protegido o en un grupo de dispositivos protegidos.

Administración de Kaspersky Embedded Systems Security para Windows mediante Web Console y Cloud Console

Si ha instalado Kaspersky Embedded Systems Security para Windows en una serie de dispositivos protegidos que forman parte de un mismo grupo de administración, puede administrarlos en forma centralizada mediante el Complemento de web de Kaspersky Embedded Systems Security para Windows. Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console también permiten configurar por separado los ajustes de cada dispositivo protegido incluido en un grupo de administración.

Un grupo de administración se crea manualmente en Kaspersky Security Center Web Console. El grupo incluye varios dispositivos con Kaspersky Embedded Systems Security para Windows instalado, para los cuales es conveniente configurar las mismas opciones de control y protección. Para obtener más información sobre la utilización de grupos de administración, consulte la *Ayuda de Kaspersky Security Center*.

La configuración de la aplicación para un solo dispositivo protegido no está disponible si el funcionamiento de Kaspersky Embedded Systems Security para Windows en el dispositivo protegido está controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Embedded Systems Security para Windows puede administrarse desde Kaspersky Security Center Web Console de las siguientes maneras:

- **Utilización de directivas de Kaspersky Security Center**. Es posible usar directivas de Kaspersky Security Center para configurar remotamente la misma configuración de protección para un grupo de dispositivos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre las opciones de la tarea configuradas de forma local en la Consola de la aplicación o remotamente en la ventana de propiedades del dispositivo de Kaspersky Security Center Web Console. Las directivas se pueden usar para configurar los ajustes generales de la aplicación, los ajustes de las tareas de protección del equipo en tiempo real, las tareas de control de actividades en los dispositivos y los ajustes que regulan el inicio programado de tareas del sistema local.

- **Utilización de tareas de grupo de Kaspersky Security Center**. Las tareas de grupo de Kaspersky Security Center permiten configurar a distancia las opciones comunes de las tareas que tienen un periodo de vencimiento para un grupo de dispositivos. Puede usar tareas de grupo para activar la aplicación, configurar la tarea de Análisis a pedido, actualizar la configuración de tareas y configurar la tarea Generador de reglas de Control de inicio de aplicaciones.

- **Utilización de tareas para un conjunto de dispositivos**. Las tareas para un conjunto de dispositivos permiten la configuración remota de las opciones comunes de las tareas con un periodo de ejecución limitado para dispositivos protegidos que no pertenecen a ningún grupo de administración.

- **Utilización de la ventana de propiedades de un solo dispositivo**. En la ventana de propiedades del dispositivo, puede configurar remotamente las opciones de tareas para un solo dispositivo protegido incluido en un grupo de administración. También puede establecer tanto la configuración general de la aplicación como la configuración para todas las tareas de Kaspersky Embedded Systems Security para Windows si el dispositivo protegido seleccionado no está controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console le permiten configurar los parámetros de la aplicación y las funciones avanzadas, y trabajar con registros y notificaciones. Puede configurar estos parámetros tanto para un grupo de dispositivos protegidos, como para dispositivos protegidos individuales.

Limitaciones del Complemento web

El Complemento web de Kaspersky Embedded Systems Security para Windows tiene las siguientes limitaciones en comparación con el Complemento de administración de Kaspersky Embedded Systems Security para Windows:

- Para agregar usuarios o grupos de usuarios, debe especificar las cadenas del descriptor de seguridad con el lenguaje de definición del descriptor de seguridad (SDDL).
- El nivel de seguridad predefinido no se puede cambiar para la tarea Protección de archivos en tiempo real.
- No se pueden crear reglas de la tarea Control de inicio de aplicaciones con un certificado digital ni con eventos de Kaspersky Security Center.
- No se pueden generar reglas de la tarea Control de dispositivos según los dispositivos conectados ni los datos del sistema.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar las configuraciones generales de Kaspersky Embedded Systems Security para Windows en Kaspersky Security Center Web Console.

Configuración de opciones generales de la aplicación en el Complemento web

Puede establecer la configuración general de Kaspersky Embedded Systems Security para Windows desde el Complemento web para un grupo de dispositivos protegidos o para un dispositivo protegido.

Ajustes de escalabilidad, interfaz y configuración del análisis en el Complemento web

Para ajustar la configuración de la escalabilidad y la interfaz de aplicación:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en el botón **Configuración** de la subsección **Configuración de la escalabilidad, interfaz y análisis**.

6. Configure las opciones que se describen en la tabla a continuación.

Configuración de escalabilidad

Configuración	Descripción
Detectar automáticamente la configuración de escalabilidad	Kaspersky Embedded Systems Security para Windows controla automáticamente el número de procesos usados. Este es el valor predeterminado.
Configurar manualmente el número de procesos de trabajo	Kaspersky Embedded Systems Security para Windows controla la cantidad de procesos en funcionamiento activos según los valores especificados.
Número de procesos para la protección en tiempo real	Número máximo de procesos usados por los componentes de la tarea Protección del equipo en tiempo real. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.
Número de procesos para tareas de análisis a pedido en segundo plano	Número máximo de procesos usados por el componente de Análisis a pedido al ejecutar tareas de Análisis a pedido en segundo plano. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.
Mostrar ícono de la bandeja del sistema en la barra de tareas	Configure si el icono de la bandeja del sistema se mostrará en el área de notificación.
Restaurar los atributos del archivo luego del análisis	Cuando Kaspersky Embedded Systems Security para Windows realiza tareas de Análisis a pedido y de Protección de archivos en tiempo real, se actualiza la hora en la que se accedió por última vez a cada archivo analizado. Después del análisis, Kaspersky Embedded Systems Security para Windows restablece la hora en la que se accedió por última vez al archivo al valor inicial. Este comportamiento puede afectar el trabajo de los sistemas de copia de seguridad, al provocar la creación de copias de seguridad de los archivos que no se modificaron. Esto también puede provocar detecciones falsas en las aplicaciones de seguimiento de cambios en archivos. De forma predeterminada, esta función está habilitada.
Restringir el uso de CPU para los subprocesos del análisis	Kaspersky Embedded Systems Security limita el uso de CPU del dispositivo protegido durante las tareas de análisis a pedido al valor especificado en el campo **Límite máximo (en porcentaje)**. La activación de esta opción puede afectar negativamente el rendimiento de Kaspersky Embedded Systems Security para Windows. De forma predeterminada, esta opción está deshabilitada.
Límite máximo (en porcentajes)	Valor máximo de uso de CPU que permite Kaspersky Embedded Systems Security para Windows. El campo de entrada está disponible si la opción Restringir el uso de CPU para los subprocesos del análisis está seleccionada.
Carpeta para los archivos	Carpeta en la que Kaspersky Embedded Systems Security para Windows necesita descomprimir los archivos comprimidos durante el análisis.

temporales creados durante el análisis	De forma predeterminada, se utiliza la carpeta C:\Windows\Temp.
Configuración del sistema HSM	Seleccione la opción para acceder al depósito jerárquico.

Configuración de seguridad de la aplicación en el Complemento web

Para configurar los valores de seguridad manualmente, siga estos pasos:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en el botón **Configuración** de la subsección **Seguridad y confiabilidad**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de seguridad

Configuración	Descripción
Proteger los procesos de la aplicación de amenazas externas	Si la casilla **Proteger los procesos de la aplicación de amenazas externas** está seleccionada, la aplicación protege sus procesos contra la inyección de código y el acceso a los datos de los mismos. Si habilita o deshabilita esta función, no es necesario que reinicie los servicios de la aplicación para que se apliquen los cambios. De forma predeterminada, esta función está habilitada.
Ejecutar recuperación de tarea	Esta casilla de verificación habilita o deshabilita la recuperación de las tareas de Kaspersky Embedded Systems Security para Windows cuando la aplicación devuelve un error o deja de funcionar. Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows recupera automáticamente las tareas de Kaspersky Embedded Systems Security para Windows cuando la aplicación devuelve un error o deja de funcionar. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no recupera las tareas de Kaspersky Embedded Systems Security para Windows cuando la aplicación devuelve un error o deja de funcionar. De forma predeterminada, la casilla está activada.
Recuperar tareas de Análisis a pedido no más de (veces) en el rango de 1 a 10 intentos	Número de intentos para recuperar una tarea de Análisis a pedido después de que Kaspersky Embedded Systems Security para Windows devuelve un error. El campo de entrada se encuentra disponible si se activa la casilla **Ejecutar recuperación de tarea**.
No iniciar las tareas de	

análisis programadas	Esta casilla de verificación habilita o deshabilita el inicio de una tarea de análisis programado después de que el dispositivo protegido cambia a una fuente de UPS hasta que el suministro de energía estándar se restaura. Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows no inicia tareas de análisis programado después de que el dispositivo protegido cambia a una fuente de UPS hasta que el suministro de energía estándar se restaura. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows inicia tareas de análisis programado sin tener en cuenta el suministro de energía. De forma predeterminada, la casilla está activada.
Detener las tareas de análisis en curso	La casilla de verificación habilita o deshabilita las tareas de análisis en ejecución después de que el dispositivo protegido cambia a una fuente de UPS. Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows pausa las tareas de análisis en ejecución después de que el dispositivo protegido cambia a una fuente de UPS. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows continúa las tareas de análisis en ejecución después de que el dispositivo protegido cambia a una fuente de UPS. De forma predeterminada, la casilla está activada.
Aplicar protección con contraseña	Establecer una contraseña para proteger el acceso a funciones de Kaspersky Embedded Systems Security para Windows.

Ajustes de la configuración de conexión en el Complemento web

Los parámetros de conexión configurados se utilizan para conectar Kaspersky Embedded Systems Security para Windows a servidores de activación y actualización durante la integración de aplicaciones con Servicios KSN.

Para configurar los parámetros de conexión, siga estos pasos:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en el botón **Configuración** de la subsección **Configuración de la escalabilidad, interfaz y análisis**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de conexión

Configuración	Descripción
No usar un servidor proxy	Si esta opción está seleccionada, Kaspersky Embedded Systems Security para Windows se conecta a Servicios KSN directamente, sin usar ningún servidor proxy.
Usar la configuración	Si esta opción está seleccionada, Kaspersky Embedded Systems Security para Windows se conecta al KSN con la configuración del servidor proxy especificada manualmente.

especificada del servidor proxy	
No usar el servidor proxy para las direcciones locales	Esta casilla de verificación habilita o deshabilita el uso de un servidor proxy al acceder a dispositivos ubicados en la misma red que el dispositivo protegido con Kaspersky Embedded Systems Security para Windows instalado. Si esta casilla de verificación está seleccionada, se accede a los dispositivos directamente desde la red que aloja el dispositivo protegido con Kaspersky Embedded Systems Security para Windows instalado. No se utiliza ningún servidor proxy. Si la casilla de verificación está desactivada, se utiliza un servidor proxy para la conexión a dispositivos locales. De forma predeterminada, la casilla está activada.
Configuración de autenticación del servidor proxy	Especifique la configuración de autenticación
No usar autenticación	La autenticación no se realiza. Este modo está seleccionado en forma predeterminada.
Usar autenticación NTLM	La autenticación se realiza usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.
Usar autenticación NTLM con nombre de usuario y contraseña	La autenticación se realiza con un nombre de usuario y contraseña usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.
Aplicar nombre de usuario y contraseña	La autenticación se realiza usando el nombre de usuario y la contraseña.

Configuración del inicio programado de las tareas locales del sistema

Puede utilizar directivas para permitir o bloquear el inicio de la tarea Análisis a pedido y la tarea Actualización del sistema local. Esto se hace de acuerdo con la programación configurada localmente en cada dispositivo protegido en el grupo de administración:

- Si el inicio programado de un tipo específico de tarea local del sistema está prohibido por una directiva, estas tareas no se realizarán en el dispositivo protegido según la programación. Puede iniciar las tareas locales del sistema manualmente.
- Si el inicio programado de un tipo específico de tarea local del sistema está permitido por una directiva, estas tareas se realizarán según los parámetros programados y configurados localmente para esta tarea.

De forma predeterminada, la directiva prohíbe el inicio de tareas locales del sistema.

Recomendamos que no habilite el inicio de tareas locales del sistema si las actualizaciones o los análisis a pedido están administrados por tareas de grupo de Kaspersky Security Center.

Si no utiliza las tareas de actualización de grupo o de análisis a pedido, permita que las tareas locales del sistema se inicien en la directiva: Kaspersky Embedded Systems Security para Windows realizará las actualizaciones de bases de datos y del módulo, e iniciará todas tareas locales de análisis a pedido del sistema de acuerdo con la programación predeterminada.

Puede usar directivas para autorizar o bloquear el inicio programado de las siguientes tareas del sistema locales:

- Tareas de Análisis a pedido: Análisis de áreas críticas, Análisis de archivos en cuarentena, Análisis al inicio del sistema operativo, Control de integridad de la aplicación, Monitor comparativo de integridad de archivos.
- Tareas de Actualización: Actualización de bases de datos, Actualización de módulos del programa, Copia de actualizaciones.

Si el dispositivo protegido se excluye del grupo de administración, la programación de tareas locales del sistema se habilitará automáticamente.

Para autorizar o bloquear el inicio programado de tareas locales del sistema de Kaspersky Embedded Systems Security para Windows en una directiva realice lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. Haga clic en el botón **Configuración** de la subsección **Ejecutar tareas locales del sistema**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de la ejecución programada de tareas locales del sistema

Configuración	Descripción
Permitir que se inicien las tareas de análisis a pedido	Seleccione o desactive la casilla de verificación para permitir o no permitir el inicio programado de tareas de análisis a pedido.
Permitir que se inicien las tareas de actualización y de Copia de actualizaciones	Seleccione o desactive la casilla de verificación para permitir o no permitir el inicio programado de las tareas de actualización y tarea Copia de actualizaciones.

Configuración de opciones de Cuarentena y Copia de seguridad en el Complemento web

Para configurar parámetros generales de Cuarentena y Copia de seguridad en Kaspersky Security Center, realice lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Adicional**.
5. Haga clic en el botón **Configuración** de la subsección **Depósitos**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de Cuarentena y Copia de seguridad

Configuración	Descripción
Carpeta de Copia de seguridad	Especificar la carpeta de Copia de seguridad.
Tamaño máx. de Copia de seguridad (MB)	Establecer el tamaño máximo de Copia de seguridad.
Valor umbral de espacio disponible (MB)	Especificar el valor mínimo de espacio libre en la carpeta de Copia de seguridad.
Carpeta de destino para restaurar objetos	Especificar una carpeta para objetos restaurados.
Carpeta de Cuarentena	Especificar la carpeta de Copia de seguridad.
Tamaño máximo de cuarentena (MB)	Establecer el tamaño máximo de Copia de seguridad.
Valor umbral de espacio disponible (MB)	Especificar el valor mínimo de espacio libre en la carpeta de Copia de seguridad.
Carpeta de destino para restaurar objetos	Especificar una carpeta para objetos restaurados.
Plazo de bloqueo de sesiones de red	Especifique la cantidad de días, horas y minutos después de los cuales las sesiones en la red bloqueadas recuperan el acceso a los recursos de archivos en red.

Creación y configuración de directivas

Esta sección proporciona información sobre la utilización de directivas de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security para Windows en varios dispositivos protegidos.

Las directivas globales de Kaspersky Security Center pueden crearse para administrar la protección de varios dispositivos en los que está instalado Kaspersky Embedded Systems Security para Windows.

Una directiva implementa la configuración, las funciones y las tareas especificadas de Kaspersky Embedded Systems Security para Windows en todos los dispositivos protegidos para un grupo de administración.

Se pueden crear e implementar por turnos varias directivas para un grupo de administración. En la Consola de administración, la directiva activa actualmente para un grupo tiene el estado *activa*.

La información sobre la implementación de la directiva se carga en el registro de auditoría del sistema de Kaspersky Embedded Systems Security para Windows. Esta información se puede visualizar en la Consola de la aplicación, en el nodo **Registro de auditoría del sistema**.

Kaspersky Security Center ofrece una manera de aplicar directivas en dispositivos protegidos: *no permitir los cambios a la configuración*. Después de aplicar una directiva, Kaspersky Embedded Systems Security para Windows utiliza la configuración para los cuales seleccionó el icono en las propiedades de la directiva en dispositivos protegidos. En este caso, se utiliza la configuración seleccionada en lugar de la configuración vigente antes de que se aplicara la directiva. Kaspersky Embedded Systems Security para Windows no aplica la configuración de la directiva activa para los cuales seleccionó el icono en las propiedades de la directiva.

Si una directiva está activa, los valores de configuración marcados con el icono en la directiva se muestran en la Consola de la aplicación, pero no se pueden modificar. Los valores de otras opciones de configuración (marcados con el icono en la directiva) pueden modificarse en la Consola de la aplicación.

Las opciones de configuración definidas en la directiva activa y marcadas con el icono no pueden modificarse para un dispositivo protegido en particular a través de la ventana **Propiedades: <Nombre del dispositivo protegido>** de Kaspersky Security Center.

La configuración que se especifica y se envía al dispositivo protegido usando una directiva activa se guarda en la configuración de las tareas locales después de que se deshabilita la directiva activa.

Si una directiva define la configuración de alguna tarea de Protección del equipo en tiempo real que se encuentra en ejecución, la configuración definida por la directiva cambiará en cuanto se aplique la directiva. Si la tarea no está en ejecución, la configuración se implementará cuando se inicie.

Creación de directiva

Para crear una directiva:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el botón **Agregar**.
3. Se abre la ventana **Nueva directiva**.
4. En la sección **Seleccionar aplicación**, seleccione Kaspersky Embedded Systems Security para Windows y haga clic en **Siguiente**.
5. En la pestaña **General**, puede realizar las siguientes acciones:
   - Cambiar el nombre de la directiva.

     El nombre de la directiva no puede contener los siguientes símbolos: `" * < : > ? \ |`.

   - Seleccionar el estado de la directiva.
     - **Activo**. Después de la próxima sincronización, se usará como la directiva activa en el equipo.

- **Inactivo**. Directiva de Copia de seguridad. Si es necesario, una directiva inactiva se puede cambiar al estado activo.

- **Fuera de la oficina**. La directiva se activa cuando un equipo abandona el perímetro de red de la organización.

- Configure la herencia de la configuración:

  - **Heredar la configuración de la directiva principal**. Si este botón está activado, los valores de configuración de la directiva se heredan de la directiva de nivel superior. La configuración de la directiva no se puede editar si está configurado para la directiva principal.

  - **Forzar la herencia de configuraciones en directivas secundarias**. Si el botón está activado, los valores de la configuración de la directiva se propagan a las directivas secundarias. En la configuración de la directiva secundaria, la casilla de verificación **Heredar la configuración de la directiva principal** se selecciona automáticamente. La configuración de la directiva secundaria se hereda de la directiva principal, a excepción de las configuraciones marcadas con . La configuración de la directiva secundaria no se puede editar si está configurado para la política principal.

6. En la pestaña **Configuración de la aplicación**, configure las opciones de directiva según sea necesario.

7. Haga clic en el botón **Guardar**.

La directiva creada se mostrará en la lista de directivas de la pestaña **Directivas y perfiles** del grupo de administración seleccionado. En la ventana **<Nombre de la directiva>**, puede establecer otra configuración, tareas y funciones de Kaspersky Embedded Systems Security para Windows.

Cuando se crea una nueva directiva, se crea también un conjunto de reglas de autorización para evitar que las aplicaciones se bloqueen y garantizar que continúen funcionando sin interrupciones. Puede ver las reglas predeterminadas en la configuración de tareas. Encontrará los detalles y las limitaciones más abajo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red entrante:

- Dos reglas de autorización para el proceso de compartir el escritorio de Windows mediante el Agente de red de Kaspersky Security Center, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

- Dos reglas de autorización para el puerto local 15000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

De manera predeterminada, cuando se crea una nueva directiva, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para el tráfico de red saliente:

- Dos reglas de autorización para el servicio de Kaspersky Embedded Systems Security para Windows, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

- Dos reglas de autorización para el proceso de trabajo de Kaspersky Embedded Systems Security para Windows, el cual se encuentra en las carpetas %Program Files% y %Program Files (x86)%. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

- Dos reglas de autorización para el puerto local 13000. Estado: habilitado. Direcciones externas permitidas: todas. Protocolos: TCP y UDP, una regla por protocolo.

Secciones de configuraciones de las directivas de Kaspersky Embedded Systems Security para Windows

General

En la sección **General**, puede configurar las siguientes opciones de la directiva:

- Especificar el estado de la directiva.
- Configurar las opciones de herencia para las directivas principales y las secundarias.

Configuración de eventos

En la sección **Configuración de eventos**, puede configurar las opciones de las siguientes categorías de eventos:

- *Evento crítico*
- *Fallo funcional*
- *Advertencia*
- *Información*

Puede usar el botón **Propiedades** para configurar las siguientes opciones de los eventos seleccionados:

- Indicar la ubicación de almacenamiento y el periodo de retención para la información sobre los eventos registrados.
- Indicar el método de notificación para los eventos registrados.

Configuración de la aplicación

Configuración de la sección Configuración de la aplicación

Sección	Opciones
Configuración de la escalabilidad, interfaz y análisis	En la subsección **Configuración de la escalabilidad, interfaz y análisis**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Elija si desea ajustar la configuración de la escalabilidad automáticamente o manualmente. • Establecer la configuración de la visualización del icono de la aplicación.
Seguridad y confiabilidad	En la subsección **Seguridad y confiabilidad**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Configurar las opciones de inicio de tareas. • Especificar cómo debería comportarse la aplicación cuando el dispositivo protegido se está ejecutando con energía de UPS.

	• Habilitar o deshabilitar la protección con contraseña de funciones de la aplicación.
Conexiones	En la subsección **Conexiones**, puede usar el botón **Configuración** para configurar las siguientes opciones del servidor proxy para la conexión a KSN y a los servidores de actualizaciones y activación: • Configurar las opciones del servidor proxy • Especificar la configuración de autenticación del servidor proxy
Ejecutar tareas locales del sistema	En la subsección **Ejecutar tareas locales del sistema**, puede usar el botón **Configuración** para autorizar o bloquear el inicio de las siguientes tareas locales del sistema según la programación configurada en los dispositivos protegidos: • Tarea Análisis a pedido. • Tareas Actualización y tarea Copia de actualización.

Adicional

Configuración de la sección Adicional

Sección	Opciones
Zona de confianza	En la subsección **Configuración**, puede hacer clic en el botón **Zona de confianza** para configurar las siguientes opciones relativas a la zona de confianza: • Crear una lista de exclusiones para la Zona de confianza. • Habilitar o deshabilitar el análisis de las operaciones de copia de seguridad de archivos. • Crear una lista de procesos de confianza.
Análisis de unidades extraíbles	En la subsección **Análisis de unidades extraíbles**, puede usar el botón **Configuración** para configurar los parámetros de análisis para unidades extraíbles.
Permisos de acceso de usuario para administrar la aplicación	En la subsección **Permisos de acceso de usuario para administrar la aplicación**, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar Kaspersky Embedded Systems Security para Windows.
Permisos de acceso de usuario para la administración del servicio de Kaspersky Security	En la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security**, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar el servicio de Kaspersky Security.
Depósitos	En la sección **Depósitos**, haga clic en el botón **Configuración** para configurar las siguientes opciones de Cuarentena, Copia de seguridad y Hosts bloqueados: • Especificar la ruta de la carpeta donde desea colocar objetos en Cuarentena o Copia de seguridad. • Configurar el tamaño máximo de Copia de seguridad y Cuarentena, y especificar el umbral de espacio disponible.

	• Especificar la ruta de la carpeta donde desea colocar objetos restaurados de la Cuarentena o la Copia de seguridad. • Configurar la transmisión de información sobre los objetos en Cuarentena y Copia de seguridad al Servidor de administración. • Configurar la duración del bloqueo de hosts.

Protección del equipo en tiempo real

Configuración de la sección Protección del servidor en tiempo real

Sección	Opciones
Protección de archivos en tiempo real	En la subsección **Protección de archivos en tiempo real**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Indicar el modo de protección. • Configurar el uso del Analizador heurístico. • Configurar el uso de la zona de confianza. • Indicar el área de protección. • Configurar el nivel de seguridad para el área de protección seleccionada: puede seleccionar un nivel de seguridad predefinido o establecer la configuración de la seguridad manualmente. • Configurar las opciones de inicio de tareas.
Uso de KSN	En la subsección **Uso de KSN**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Indicar las acciones a realizar en objetos no confiables según KSN. • Configurar la transferencia de datos y el uso de Kaspersky Security Center como servidor KSN Proxy.
Prevención de exploits	En la subsección **Prevención de exploits**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de protección de memoria del proceso. • Indicar acciones para reducir el riesgo que suponen los exploits. • Añadir elementos a la lista de procesos protegidos y editar dicha lista.

Control de actividad local

Configuración de la sección Control de actividad local

Sección	Opciones
Control de inicio	En la subsección **Control de inicio de aplicaciones**, puede hacer clic en el botón

de aplicaciones	**Configuración** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones para controlar los inicios subsiguientes de la aplicación. • Indicar el área de las reglas de Control de inicio de aplicaciones. • Configurar el uso de KSN. • Configurar las opciones de inicio de tareas.
Control de dispositivos	En la subsección **Control de dispositivos**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones de inicio de tareas.

Control de actividad de red

Configuración de la sección Control de actividad de red

Sección	Opciones
Administración de firewall	En la subsección **Administración de firewall**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Configurar las reglas de firewall. • Configurar las opciones de inicio de tareas.

Inspección del sistema

Configuración de la sección Inspección del sistema

Sección	Opciones
Monitor de integridad de archivos	En la subsección **Monitor de integridad de archivos**, puede configurar el control de los cambios en archivos que pueden significar una infracción de la seguridad en un dispositivo protegido.
Inspección de registros	En la subsección **Inspección de registros**, puede configurar un monitoreo de la integridad del dispositivo protegido basado en los resultados de un análisis del Registro de eventos de Windows.

Registros y notificaciones

Configuración de la sección Registros y notificaciones

Sección	Opciones
Registros de tareas	En la subsección **Registros de tareas**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones:

	• Especificar el nivel de importancia de los eventos registrados para los componentes de la aplicación seleccionados. • Especificar la configuración de depósitos de almacenamiento del registro de tareas. • Especificar la integración de SIEM con la configuración de Kaspersky Security Center.
Notificaciones de eventos	En la subsección **Notificaciones de eventos**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones: • Especifique la configuración de la notificación del usuario para los eventos *Objeto detectado*, *Almacenamiento masivo dudoso detectado y restringido* y *El host está en la lista de dudosos*. • Especificar la configuración de notificaciones del administrador para cualquier evento seleccionado en la lista de eventos en la sección **Configuración de notificaciones**.
Interacción con Servidor de administración	En la subsección **Interacción con Servidor de administración**, puede hacer clic en el botón **Configuración** para seleccionar los tipos de objetos que Kaspersky Embedded Systems Security para Windows informará al Servidor de administración.

Historial de revisiones

En la sección **Historial de revisiones**, puede administrar revisiones: compararlas con la revisión actual u otra directiva, agregue descripciones de revisiones, guardar revisiones de un archivo o realizar una reversión.

Creación y configuración de tareas con Kaspersky Security Center

Esta sección contiene información sobre las tareas de Kaspersky Embedded Systems Security para Windows y cómo crearlas, ajustar sus configuraciones, e iniciarlas y detenerlas.

Acerca de la creación de tareas en el Complemento web

Puede crear tareas de grupo para grupos de administración y conjuntos de dispositivos protegidos. Se pueden crear los siguientes tipos de tareas:

- Activación de la aplicación
- Copia de actualizaciones
- Actualización de bases de datos
- Actualización de módulos del programa
- Reversión de la actualización de bases de datos
- Análisis a pedido
- Control de integridad de la aplicación

- Monitor comparativo de integridad de archivos
- Generador de reglas de Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos

Puede crear tareas de grupo y locales de las siguientes maneras:

- Para un dispositivo protegido: en la ventana **Propiedades <Nombre del dispositivo protegido>** en la sección **Tareas**.
- Para un grupo de administración: en el panel de detalles del nodo del grupo seleccionado de dispositivos protegidos en la pestaña **Tareas**.
- Para un conjunto de dispositivos protegidos: en el panel de detalles del nodo **Selecciones de dispositivos**.

Puede usar directivas para deshabilitar programaciones de tareas del sistema local de actualizaciones y de Análisis a pedido en todos los dispositivos protegidos desde el mismo grupo de administración.

Se proporciona información general sobre tareas en Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Crear una tarea en el Complemento web

Para crear una tarea nueva en la Consola de administración de Kaspersky Security Center:

1. Inicie el asistente de tareas de una de las siguientes maneras:
   - Para crear una tarea local:
     a. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
     b. Haga clic en la pestaña **Grupos** para seleccionar el grupo de administración al que pertenece el dispositivo protegido.
     c. Haga clic en el nombre del dispositivo protegido.
     d. En la ventana **<Nombre del dispositivo>** que se abre, seleccione la pestaña **Tareas**.
     e. Haga clic en el botón **Agregar**.
   - Para crear una tarea de grupo:
     a. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
     b. Haga clic en la pestaña **Grupos** para seleccionar el grupo de administración para el cual desea crear una tarea.
     c. Haga clic en el botón **Agregar**.
   - Para crear una tarea para un conjunto personalizado de dispositivos protegidos:
     a. En la ventana principal de Web Console, seleccione **Dispositivos** → **Selecciones de dispositivos**.

b. Elija la selección para la cual desea crear una tarea.

c. Haga clic en el botón **Iniciar**.

d. En la ventana **Resultados de la selección**, seleccione los dispositivos para los que desea crear una tarea.

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

Se abre la ventana del asistente de tareas.

2. En la lista desplegable **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security para Windows**.

3. En la lista desplegable **Tipo de tarea**, seleccione el tipo de tarea que creará.

   Si selecciona cualquier tipo de tarea que no sea Reversión de la actualización de bases de datos, Control de integridad de la aplicación o Activación de la aplicación, se abrirá la ventana de configuración.

4. Según el tipo de tarea seleccionado, realice una de las siguientes acciones:

   - Cree una tarea de Análisis a pedido.
   - Para crear una tarea de actualización, configure los valores de la tarea según sus requisitos:

     a. Seleccione un origen de actualizaciones en la sección **Origen de actualizaciones de la base de datos**.

     b. En la ventana **Configuración de conexión**, configure las opciones del servidor proxy.

   - Después de crear una tarea de Actualización de módulos del programa, configure los parámetros de actualización de módulos de la aplicación requeridos en la ventana **Actualización de módulos del programa**:

     a. Seleccione una de estas opciones si desea copiar e instalar actualizaciones del módulo del programa críticas o solo comprobar su disponibilidad sin instalarlas.

     b. Si la opción **Copiar e instalar actualizaciones críticas de módulos del programa** está seleccionada: es posible que deba reiniciarse el dispositivo protegido para aplicar los módulos de software instalados. Si desea que Kaspersky Embedded Systems Security para Windows reinicie el dispositivo protegido automáticamente después de la finalización de la tarea, seleccione la casilla de verificación **Permitir el reinicio del sistema operativo**.

     c. Para obtener información sobre actualizaciones de módulos de Kaspersky Embedded Systems Security para Windows, seleccione **Informarme de las actualizaciones programadas que estén disponibles para los módulos del programa**.

     Kaspersky no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la instalación automática; se deben descargar manualmente desde el sitio web de Kaspersky. Es posible configurar una notificación de administrador del evento **Está disponible una nueva actualización programada de módulos del programa**. Esto incluirá la URL de nuestro sitio web desde donde puede descargar las actualizaciones programadas.

   - Para crear la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la ventana **Copia de actualizaciones**.

   - Para crear la tarea de Activación de la aplicación:

     a. En la ventana **Lista de claves del depósito de Kaspersky Security Center**, especifique el archivo de clave que desea usar para activar la aplicación.

b. Seleccione la casilla de verificación **Usar como clave adicional** si desea crear una tarea para renovar la licencia.

- Cree y configure la tarea Generador de reglas de Control de inicio de aplicaciones.
- Cree y configure la tarea Generador de reglas para Control de dispositivos.

5. Haga clic en el botón **Siguiente**.
6. Si la tarea se crea para un conjunto de dispositivos protegidos, seleccione la red (o el grupo) de los dispositivos protegidos en los que se ejecutará esta tarea.
7. Haga clic en el botón **Siguiente**.
8. En la ventana **Finalizar creación**, seleccione la casilla de verificación **Abrir detalles de la tarea cuando se complete la creación** si desea configurar las opciones de la tarea.
9. Haga clic en el botón **Finalizar**.

La tarea creada se mostrará en la lista **Tareas**.

Configurar tareas de grupo en el Complemento web

Para configurar una tarea de grupo para varios dispositivos protegidos:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.
3. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - Para configurar una tarea de Análisis a pedido:
     a. En la sección **Área del análisis**, configure un área del análisis.
     b. En la sección **Opciones**, configure el nivel de prioridad de la tarea y la integración con otros componentes del programa.
   - Para configurar una tarea de actualización, establezca los valores de la tarea según sus requisitos:
     a. En la sección **Orígenes de actualizaciones**, configure las opciones del origen de actualizaciones y el servidor proxy.
     b. En la sección **Optimización**, configure la optimización del subsistema de disco.
   - Para configurar la tarea Actualización de módulos del programa, en la sección **Configuración avanzada**, elija una acción para realizar: copiar e instalar actualizaciones críticas de módulos del programa o solo comprobar si existen.
   - Para configurar la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la sección **Configuración de la copia de actualizaciones**.

- Para configurar la tarea Activación de la aplicación, aplique el archivo de clave que desea utilizar para activar la aplicación. Seleccione la casilla de verificación **Usar como clave adicional** si desea agregar un código de activación o archivo de clave para renovar la licencia.

- Para configurar la generación automática de reglas de autorización para el Control de dispositivos, especifique la configuración que se utilizará para crear la lista de reglas de autorización.

4. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).

5. En la pestaña **Configuración** de la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

6. Haga clic en el botón **Guardar**.

Se guardan las opciones de la tarea de grupo recientemente configuradas.

Configuración de la tarea Activación de la aplicación en el Complemento web

Para configurar una activación de la tarea Aplicación:

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

2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.

3. En la sección **Común**, especifique el archivo de clave que desea usar para activar la aplicación. Active la casilla **Usar como clave adicional** si desea agregar una clave para renovar la licencia.

4. Configure la programación de tareas en la sección **Programación**.

5. En la ventana **<Nombre de la tarea>**, haga clic en **Aceptar**.

Configurar tareas de actualización en el Complemento web

Para configurar las tareas Copia de actualizaciones, Actualización de bases de datos o Actualización de módulos del programa:

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

2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.

3. En la sección **Orígenes de actualizaciones**, configure las opciones del origen de actualizaciones:

   - En la sección **Origen de actualizaciones de la base de datos**, especifique el Servidor de administración de Kaspersky Security Center o los servidores de actualizaciones de Kaspersky como origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones:

si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones.

Puede especificar el uso de Servidores de actualizaciones de Kaspersky si los servidores personalizados manualmente no están disponibles.

Para usar una carpeta compartida de SMB como origen de actualizaciones, debe especificar una cuenta de usuario para iniciar una tarea.

Al configurar una tarea de actualización a través de Cloud Console, solo la configuración de los **Puntos de distribución** y los **Servidores de actualizaciones de Kaspersky** está disponible para especificar el origen de actualizaciones.

- En la sección **Configuración de conexión**, configure el uso de un servidor proxy para conectarse a servidores de actualizaciones de Kaspersky y otros servidores.

4. En la sección **Optimización** de la tarea Actualización de bases de datos, puede configurar la función que reduce la carga de trabajo en el subsistema del disco:
   - **Optimización de lectura y escritura en disco**
   - **RAM usada para optimización (400 - 9999 MB)**
5. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
6. En la ventana **<Nombre de la tarea>**, haga clic en **Aceptar**.

Configuración de ajustes de diagnósticos de falla en el Complemento web

Si ocurre un error durante el funcionamiento de Kaspersky Embedded Systems Security para Windows (por ejemplo, la aplicación se detiene), puede diagnosticar el problema. Para tal fin, puede habilitar la creación de archivos de seguimiento y de un archivo de volcado para el proceso de Kaspersky Embedded Systems Security para Windows y enviar estos archivos al Servicio de soporte técnico para que sean analizados.

Kaspersky Embedded Systems Security para Windows no envía ningún archivo de volcado o rastreo automáticamente. Solo el usuario que posea los permisos requeridos podrá enviar datos de diagnóstico.

Kaspersky Embedded Systems Security para Windows escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security para Windows. Puede configurar los permisos de acceso y permitir que solo los usuarios necesarios puedan acceder a los registros, los archivos de rastreo y los archivos de volcado.

Para configurar el diagnóstico de interrupciones en Kaspersky Security Center:

1. En la Consola de administración de Kaspersky Security Center, abra la ventana **Configuración de la aplicación**.
2. Abra la sección **Diagnóstico de mal funcionamiento**.

3. Para registrar información de depuración en un archivo, en la sección **Configuración de resolución de problemas**, active la casilla **Habilitar seguimiento**.

4. En el campo **Carpeta de archivos de seguimiento**, indique la ruta absoluta a la carpeta local donde Kaspersky Embedded Systems Security para Windows guardará los archivos de seguimiento.

   La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. La ruta no puede hacer referencia a una unidad, una carpeta de red o una variable de entorno.

5. Configure el nivel de detalle de la información de depuración.

6. Especifique el **Tamaño máximo de los archivos de seguimiento (MB)**.

   Valores disponibles: de 1 a 4095 MB. De forma predeterminada, el tamaño máximo de los archivos de seguimiento es de 50 MB.

7. Para que los archivos de seguimiento más antiguos se eliminen cuando se alcance el número máximo de archivos, seleccione la casilla **Eliminar los archivos de seguimiento más antiguos**.

8. Especifique el **Cantidad máxima de archivos para un registro de seguimiento**.

   Valores disponibles: de 1 a 999. De manera predeterminada, el número máximo de archivos es 5. Para que este campo esté disponible, la casilla **Eliminar los archivos de seguimiento más antiguos** debe estar seleccionada.

9. Si desea que la aplicación cree un archivo de volcado de memoria, seleccione la casilla de verificación **Crear archivo de volcado**.

10. En el campo **Carpeta de archivos de volcado**, especifique la ruta absoluta a la carpeta local donde Kaspersky Embedded Systems Security para Windows guardará los archivos de volcado.

    La carpeta debe crearse de antemano y es necesario que la cuenta SYSTEM pueda escribir en ella. No puede indicar una carpeta de red, una unidad o una variable de entorno como ruta.

11. Haga clic en el botón **Aceptar**.

La configuración de la aplicación establecida se aplica en el dispositivo protegido.

Administración de programaciones de tareas

Puede configurar la programación de inicio para tareas de Kaspersky Embedded Systems Security para Windows y establecer la configuración para ejecutar tareas en base a una programación.

Tareas de programación

Puede programar las tareas personalizadas y las tareas locales del sistema en la Consola de la aplicación. No puede programar tareas de grupo en la Consola de la aplicación.

Para programar tareas de grupo mediante el Complemento web, realice lo siguiente:

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

2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **<Nombre de la tarea>**.

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

4. En la sección **Programación**, seleccione la casilla de verificación **Ejecutar según programación**.

Los campos con la configuración de programación para las tareas análisis a pedido y actualización no estarán disponibles si una directiva de Kaspersky Security Center bloquea la programación de estas tareas.

5. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:

   a. En la lista **Frecuencia**, seleccione uno de los siguientes valores:

   - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
   - **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
   - **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
   - **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security para Windows.
   - **Tras actualizarse las bases de datos**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

   b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

   c. En el campo **Fecha de inicio**, especifique la fecha de inicio de la programación.

6. En la sección **Configuración de detención de tareas**:

   a. Seleccione la casilla de verificación **Duración** y, en los campos a la derecha, ingrese el número máximo de horas y minutos de la ejecución de la tarea.

   b. Seleccione la casilla de verificación **Pausar tarea** y, en los campos a la derecha, introduzca los valores de inicio y final de un intervalo de tiempo inferior a 24 horas durante el cual se detendrá la ejecución de la tarea.

7. En el bloque **Configuración avanzada de la programación**:

   a. Seleccione la casilla de verificación **Cancelar programación** y especifique la fecha desde la cual la programación dejará de aplicar.

   b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.

   c. Seleccione la casilla de verificación **Aleatorizar la hora de inicio de la tarea con un intervalo** y especifique el valor en minutos.

8. Haga clic en el botón **Guardar** para guardar la configuración de inicio de la tarea.

Cómo habilitar y deshabilitar tareas programadas

Puede habilitar y deshabilitar tareas programadas antes o después de configurar las opciones de programación.

Para habilitar o deshabilitar la programación de inicio de tareas:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.
   Se abre la ventana **<Nombre de la tarea>**.
3. Seleccione la sección **Configuración de la aplicación**.
4. Seleccione la sección **Programación**.
5. Realice una de las siguientes opciones:
   - Seleccione la casilla de verificación **Ejecutar según programación** si desea habilitar el inicio programado de la tarea.
   - Cancele la selección de la casilla de verificación **Ejecutar según programación** si desea deshabilitar el inicio programado de la tarea.

     La programación configurada para la tarea no se eliminará y se aplicará la próxima vez que habilite el inicio de una tarea programada.
6. Haga clic en el botón **Guardar**.

Se guardan las opciones de programación de inicio de tareas configuradas.

Informes en Kaspersky Security Center

Los informes en Kaspersky Security Center contienen información sobre el estado de dispositivos administrados. Los informes se basan en información almacenada en el Servidor de administración.

A partir de Kaspersky Security Center 11, los siguientes tipos de informes están disponibles para Kaspersky Embedded Systems Security para Windows:

- Informe sobre el estado de componentes de la aplicación
- Informe sobre aplicaciones prohibidas
- Informe sobre aplicaciones prohibidas en modo de prueba

Consulte la *Ayuda de Kaspersky Security Center* para obtener información detallada sobre todos los informes de Kaspersky Security Center y cómo configurarlos.

Informe de estado de los componentes de Kaspersky Embedded Systems Security para Windows

Puede supervisar el estado de protección de todos los dispositivos de red y acceder a un panorama estructurado del conjunto de componentes en cada dispositivo.

El informe muestra uno de los siguientes estados para cada componente: *En ejecución*, *En pausa*, *Detenido*, *Mal funcionamiento*, *No instalado*, *Iniciando*.

El estado *No instalado* hace referencia al componente, no a la aplicación. Si la aplicación no se instala, Kaspersky Security Center Web Console asigna el estado N/D (No disponible).

Puede crear selecciones de componentes y utilizar filtros para mostrar dispositivos de red con un conjunto especificado de componentes y su estado.

Consulte la *Ayuda de Kaspersky Security Center* para acceder a información detallada sobre la creación y el uso de selecciones.

Para revisar los estados de los componentes en la configuración de la aplicación, realice lo siguiente:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo protegido.
3. En la pestaña **General**, seleccione la sección **Componentes**.
4. Revise la tabla de estado.

   La información sobre el estado del componente Prevención de exploits no está disponible en esta tabla.

Para revisar un informe estándar de Kaspersky Security Center Web Console:

1. Seleccione **Supervisión e informes** → **Informes**.
2. Seleccione el elemento de lista **Informe sobre el estado de componentes de la aplicación** y haga clic en el botón **Mostrar informe**.

   Se genera un informe.
3. Revise los siguientes detalles del informe:

   - Un diagrama gráfico.
   - Una tabla con un resumen de los componentes y los números sumados de los dispositivos de red donde se instala cada uno de los componentes, y los grupos a los que pertenecen.
   - Una tabla detallada donde se especifica el estado, la versión, el dispositivo y el grupo del componente.

Informes sobre aplicaciones prohibidas en los modos activo y de prueba

En base a los resultados de la tarea Control de inicio de aplicaciones, pueden generarse dos tipos de informes: un informe sobre las aplicaciones prohibidas (si la tarea se inicia en modo Activo) y un informe sobre las aplicaciones prohibidas en modo de prueba (si la tarea se inició en modo Solo estadísticas). Estos informes muestran información sobre las aplicaciones bloqueadas en los dispositivos protegidos de la red. Cada informe se genera para todos los grupos de administración y acumula datos de todas las aplicaciones de Kaspersky instaladas en los dispositivos protegidos.

Para revisar un informe sobre aplicaciones prohibidas en modo Solo estadísticas:

1. Ejecute la tarea Control de inicio de aplicaciones en el modo Solo estadísticas.
2. Seleccione **Supervisión e informes → Informes**.
3. Seleccione el elemento de lista **Informe sobre aplicaciones prohibidas en modo de prueba** y haga clic en el botón **Mostrar informe**.

   Se genera un informe.
4. Revise los siguientes detalles del informe:

   - Diagrama gráfico que muestra las diez primeras aplicaciones con el mayor número de inicios bloqueados.
   - Una tabla que resume los bloqueos de aplicaciones, donde se especifican el nombre del archivo ejecutable, el motivo, el tiempo de bloqueo y el número de dispositivos donde se bloqueó.
   - Una tabla detallada donde se especifican datos sobre el dispositivo, la ruta de acceso del archivo y el criterio para el bloqueo.

Para revisar un informe sobre aplicaciones prohibidas en modo Activo:

1. Ejecute la tarea Control de inicio de aplicaciones en el modo Activo.
2. Seleccione **Supervisión e informes → Informes**.
3. Seleccione el elemento de lista **Informe sobre aplicaciones prohibidas en modo de prueba** y haga clic en el botón **Mostrar informe**.

   Se genera un informe.

Este informe consiste en los mismos datos sobre bloqueos que el informe sobre aplicaciones prohibidas en modo de prueba.

Interfaz de diagnóstico compacto

Esta sección describe cómo usar la Interfaz de diagnóstico compacto para revisar el estado del dispositivo protegido o la actividad actual, y cómo configurar la escritura de archivos de volcado y de rastreo.

Acerca de la Interfaz de diagnóstico compacto

El componente Interfaz de diagnóstico compacto (también denominado "CDI") se instala y se desinstala junto con el componente Icono de la bandeja del sistema, de forma independiente respecto de la Consola de la aplicación, y puede usarse cuando la Consola de la aplicación no está instalada en el dispositivo protegido. Para iniciar la Interfaz de diagnóstico compacto, puede usar el icono de la bandeja del sistema o puede ejecutar el archivo kavfsmui.exe, ubicado en la carpeta de la aplicación en el dispositivo protegido.

La Interfaz de diagnóstico compacto permite hacer lo siguiente:

- Ver información sobre el estado general de la aplicación.
- Ver los incidentes de seguridad que han ocurrido.
- Revisar la actividad actual del dispositivo protegido.
- Iniciar o detener la escritura de los archivos de volcado y de rastreo.
- Abra la Consola de la aplicación.
- Abra la ventana **Acerca de la aplicación** con la lista de actualizaciones instaladas y parches disponibles.

La Interfaz de diagnóstico compacto está disponible incluso si el acceso a las funciones de Kaspersky Embedded Systems Security para Windows está protegido con contraseña. No se requiere contraseña.

El componente Interfaz de diagnóstico compacto no puede configurarse mediante Kaspersky Security Center.

Revisión del estado de Kaspersky Embedded Systems Security para Windows a través de la Interfaz de diagnóstico compacto

Para abrir la Interfaz de diagnóstico compacto, realice las siguientes acciones:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security para Windows, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la **Interfaz de diagnóstico compacto**.

Revise el estado actual de las tareas clave de Protección del equipo en tiempo real y de Actualización en la pestaña **Estado de protección**. Se utilizan diferentes colores para notificar al usuario sobre el estado de protección (consulte la tabla a continuación).

Estado de protección en la Interfaz de diagnóstico compacto

Sección	Estado

Estado de protección en tiempo real	El panel es *verde* para cualquiera de los siguientes escenarios (si se cumple alguna de las condiciones):
	• Configuración recomendada:
	  • Se inicia la tarea Protección de archivos en tiempo real con la configuración predeterminada.
	  • Se inicia la tarea Control de inicio de aplicaciones en modo **Activo**con la configuración predeterminada.
	• Configuración aceptable:
	  • El usuario configura la tarea Protección de archivos en tiempo real.
	  • Se modifica la configuración de la tarea de Control de inicio de aplicaciones.

	El panel es *amarillo* si se cumplen una o varias de las siguientes condiciones: • La tarea Protección de archivos en tiempo real está pausada (p el usuario o por la programación). • La tarea Control de inicio de aplicaciones se inicia en el modo **Solo estadísticas**. • Prevención de exploits y la tarea Control de inicio de aplicaciones se han iniciado en modo **Solo estadísticas**.
	El panel es *rojo* si se cumplen estas dos condiciones: • El componente Protección de archivos en tiempo real no está instalado, o la tarea está detenida o pausada. • El componente Control de inicio de aplicaciones no está instalado, o la tarea se inició en el modo **Solo estadísticas**.
Licencia	El panel es *verde* si la licencia actual es válida.
	Un panel *amarillo* significa que ha ocurrido uno de los siguientes eventos: • *Consultar el estado de la licencia*. • *La licencia caducará en 14 días y no se ha agregado ninguna clave adicional ni código de activación.* • *La clave agregada se ha añadido a la lista de rechazadas y se bloqueará.*
	Un panel *rojo* significa que ha ocurrido uno de los siguientes eventos: • *Aplicación no activada* • *La licencia ha caducado* • *Infracción del Contrato de licencia de usuario final*

	• *La clave está en la lista de rechazadas*
Actualización	El panel es *verde* cuando las bases de datos de la aplicación están actualizadas.
	El panel es *amarillo* cuando las bases de datos de la aplicación están desactualizadas.
	El panel es *rojo* cuando las bases de datos de la aplicación son obsoletas.

Revisión de estadísticas de eventos de seguridad

La pestaña **Estadísticas** muestra todos los eventos de seguridad. Cada estadística de la tarea de protección se muestra en un bloque independiente que especifica el número de incidentes, junto a la fecha y la hora en que ocurrió el último incidente. Cuando se registra un incidente, el color del bloque cambia a rojo.

Para revisar las estadísticas:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security para Windows, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la **Interfaz de diagnóstico compacto**.
3. Abra la pestaña **Estadísticas**.
4. Revise los incidentes de seguridad para las tareas de protección.

Revisión de la actividad de la aplicación actual

En esta pestaña, puede revisar el estado de las tareas y los procesos actuales de la aplicación, y obtener notificaciones rápidas sobre los eventos críticos que ocurren.

Los diferentes colores se usan para indicar el estado de la actividad de la aplicación:

- En la sección **Tareas**:
  - *Verde*. Ninguna condición requiere rojo o amarillo.
  - *Amarillo*. Las áreas críticas no se han analizado durante un periodo prolongado.
  - *Rojo*. Al menos una de las siguientes condiciones es verdadera:
    - No se inicia ninguna tarea, y no hay una programación de inicio configurada para ninguna de las tareas.
    - Los errores de inicio de aplicaciones se registran como eventos críticos.
- En la sección **Kaspersky Security Network**:
  - *Verde*. Se inicia la tarea Uso de KSN.
  - *Amarillo*. Se acepta la Declaración de KSN, pero no se inicia la tarea.

Para revisar la actividad de la aplicación actual en el dispositivo protegido:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security para Windows, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la **Interfaz de diagnóstico compacto**.
3. Abra la pestaña **Actividad actual de la aplicación**.
4. Revise la siguiente información en la sección **Tareas**:
   - **Áreas críticas no analizadas durante mucho tiempo**.

     Este campo solo se muestra si la aplicación devuelve una advertencia correspondiente a un análisis de áreas críticas.
   - **En ejecución**
   - **Error de ejecución**
   - **Próximo inicio definido por programación**
5. Revise la siguiente información en la sección **Kaspersky Security Network**:
   - **KSN activado, servicios de reputación de archivos habilitados** o la **Protección desactivada**.
   - KSN activado, servicios de reputación de archivos habilitados, estadísticas de la aplicación enviadas a KSN.

     La aplicación envía la información sobre malware, incluido el software fraudulento, detectada durante la tarea Protección de archivos en tiempo real y las tareas de análisis a pedido, así como la información de depuración sobre errores ocurridos durante el análisis.

     El campo se muestra si se selecciona la casilla de verificación **Enviar estadísticas de Kaspersky Security Network** en la configuración de la tarea Uso de KSN.
6. Revise la siguiente información en la sección **Integración con Kaspersky Security Center**:
   - **Administración local autorizada**.
   - **Directiva aplicada: <Nombre del servidor de administración>**.

Configuración de la escritura de archivos de rastreo y volcado

Puede configurar la escritura de archivos de seguimiento y de volcado en la Interfaz de diagnóstico compacto.

También puede configurar el diagnóstico de mal funcionamiento a través de la Consola de la aplicación.

Para empezar a escribir archivos de rastreo y de volcado, realice las siguientes acciones:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security para Windows, en el área de notificación de la barra de herramientas.

2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la **Interfaz de diagnóstico compacto**.

3. Abra la pestaña **Solución de problemas**.

4. Cambie las siguientes opciones de rastreo, si es necesario:

   a. Seleccione la casilla de verificación **Escribir información de depuración en el archivo de seguimiento**.

   b. Haga clic en el botón **Examinar** para especificar la carpeta donde Kaspersky Embedded Systems Security para Windows guardará los archivos de rastreo.

      El seguimiento se habilitará para todos los componentes con los parámetros predeterminados: se utilizará el nivel de detalle *Depuración* y el tamaño máximo del registro será de 50 MB.

5. Cambie las siguientes opciones del archivo de volcado, si es necesario:

   a. Seleccione la casilla de verificación **Crear archivo de volcado por mal funcionamiento en esta carpeta**.

   b. Haga clic en el botón **Examinar** para especificar la carpeta donde Kaspersky Embedded Systems Security para Windows guardará el archivo de volcado.

6. Haga clic en el botón **Aplicar**.

   Se aplicará la nueva configuración.

Base de datos y actualización de módulos del programa de Kaspersky Embedded Systems Security para Windows

Esta sección brinda información sobre las tareas de actualización de los módulos del programa y las bases de datos de Kaspersky Embedded Systems Security para Windows, la copia de actualizaciones y las reversiones de actualizaciones de bases de datos de Kaspersky Embedded Systems Security para Windows, además de instrucciones sobre cómo configurar las tareas de actualización de las bases de datos y los módulos del programa.

Acerca de las tareas de Actualización

Kaspersky Embedded Systems Security para Windows proporciona cuatro tareas de actualización del sistema: Actualización de bases de datos, Actualización de módulos del programa, Copia de actualizaciones y Reversión de la actualización de bases de datos.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows se conecta con el origen de actualizaciones (uno de los servidores de actualizaciones de Kaspersky) una vez por hora. Puede configurar todas las tareas de actualización, excepto la tarea Reversión de la actualización de bases de datos. Cuando se modifica la configuración de una tarea, Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores en el próximo inicio de la tarea.

No puede pausar y reanudar tareas de Actualización.

Actualización de bases de datos

De forma predeterminada, Kaspersky Embedded Systems Security para Windows copia las bases de datos del origen de actualizaciones al dispositivo protegido e inmediatamente comienza a usarlas ejecutando la tarea de Protección del equipo en tiempo real. Las tareas de Análisis a pedido empiezan a usar la base de datos actualizada en el siguiente inicio.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows ejecuta la tarea de Actualización de bases de datos cada hora.

Actualización de módulos del programa

De forma predeterminada, Kaspersky Embedded Systems Security para Windows comprueba si las actualizaciones de módulos del programa están disponibles en el origen de actualizaciones. Para empezar a utilizar los módulos del programa instalados, se requiere un reinicio del dispositivo protegido o un reinicio de Kaspersky Embedded Systems Security para Windows.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows ejecuta la tarea de Actualización de módulos del programa cada semana los viernes a las 04:00 p. m. (según la configuración regional de la hora en el dispositivo protegido). Durante la ejecución de la tarea, la aplicación examina la disponibilidad de las actualizaciones importantes y programadas de módulos de Kaspersky Embedded Systems Security para Windows sin distribuirlos.

Copia de actualizaciones

De forma predeterminada, durante la ejecución de la tarea, Kaspersky Embedded Systems Security para Windows descarga los archivos de la actualización de bases de datos y los guarda en la red especificada o en la carpeta local sin aplicarlos.

La tarea de Copia de actualizaciones está deshabilitada de forma predeterminada.

Reversión de la actualización de bases de datos

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security para Windows vuelve a utilizar bases de datos de las actualizaciones instaladas anteriormente.

La tarea de Reversión de la Actualización de bases de datos está deshabilitada de forma predeterminada.

Acerca de la actualización de módulos del programa

Kaspersky puede emitir paquetes de actualización para los módulos de Kaspersky Embedded Systems Security para Windows. Los paquetes de actualización pueden ser *urgentes* (o *críticos*) o planificados. Los paquetes de actualización críticos reparan vulnerabilidades y errores; los paquetes planificados agregan nuevas funciones o mejoran las funciones existentes.

Los paquetes de actualización urgentes (críticos) se cargan en los servidores de actualizaciones de Kaspersky. Su instalación automática puede configurarse usando la tarea de Actualización de módulos del programa. De forma predeterminada, Kaspersky Embedded Systems Security para Windows ejecuta la tarea de Actualización de módulos del programa cada semana los viernes a las 04:00 p. m. (según la configuración regional de la hora en el dispositivo protegido).

Kaspersky no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la actualización automática; estos se deben descargar manualmente desde el sitio web de Kaspersky. La tarea de Actualización de módulos del programa puede utilizarse para recibir información sobre la publicación de actualizaciones planificadas de Kaspersky Embedded Systems Security para Windows.

Puede descargar actualizaciones críticas de Internet a cada dispositivo protegido o, si lo prefiere, puede copiar todas las actualizaciones a un único dispositivo y, usándolo como intermediario, distribuir desde allí las actualizaciones a los demás dispositivos protegidos de la red. Para copiar y guardar actualizaciones sin instalarlas, utilice la tarea de Copia de actualizaciones.

Antes de instalar las actualizaciones de los módulos, Kaspersky Embedded Systems Security para Windows crea copias de seguridad de los módulos instalados anteriormente. Si el proceso de actualización de los módulos del programa se interrumpe o genera un error, Kaspersky Embedded Systems Security para Windows volverá a usar automáticamente los módulos del programa instalados anteriormente. Los módulos del programa se pueden revertir manualmente a las actualizaciones anteriormente instaladas.

Durante la instalación de las actualizaciones descargadas, el servicio de Kaspersky Security se detiene y luego se inicia automáticamente.

Acerca de la actualización de bases de datos

Las bases de datos de Kaspersky Embedded Systems Security para Windows almacenadas en el dispositivo protegido se desactualizan rápidamente. Los analistas de virus de Kaspersky detectan cientos de nuevas amenazas diariamente, crean registros de identificación para ellas y las incluyen en las actualizaciones de las bases de datos de la aplicación. Las actualizaciones de las bases de datos son un archivo o un conjunto de archivos que contienen registros que identifican las amenazas descubiertas durante el tiempo desde que se creó la última actualización. Para mantener el nivel requerido de protección del dispositivo, se recomienda que las actualizaciones de las bases de datos se reciban en forma regular.

De forma predeterminada, si las bases de datos de Kaspersky Embedded Systems Security para Windows no se actualizan en un plazo de una semana a partir de la creación de las actualizaciones de las bases de datos instaladas, ocurre el evento *Las bases de datos de la aplicación están desactualizadas*. Si las bases de datos no se actualizan durante un periodo de dos semanas, ocurre el evento *Las bases de datos de la aplicación son obsoletas*. Aparece información sobre el estado de actualización de las bases de datos en el panel de resultados del nodo **Kaspersky Embedded Systems Security para Windows** del árbol de la Consola de la aplicación. Puede usar la configuración general de Kaspersky Embedded Systems Security para Windows para indicar un número diferente de días antes de que estos eventos ocurran. También puede configurar las notificaciones del administrador sobre estos eventos.

Kaspersky Embedded Systems Security para Windows descarga las actualizaciones de las bases de datos y los módulos de la aplicación desde los servidores de actualizaciones FTP o HTTP de Kaspersky, el servidor de administración de Kaspersky Security Center u otros orígenes de actualizaciones.

Puede descargar las actualizaciones a cada dispositivo protegido o puede usar un dispositivo protegido como intermediario. Las actualizaciones se copiarán al dispositivo que actúe como intermediario y luego se distribuirán a los dispositivos protegidos restantes. Si utiliza Kaspersky Security Center para la administración centralizada de la protección de los dispositivos de una organización, puede utilizar el servidor de administración de Kaspersky Security Center como intermediario para descargar las actualizaciones.

Las tareas de actualización de bases de datos pueden iniciarse manualmente o según una programación. De forma predeterminada, Kaspersky Embedded Systems Security para Windows ejecuta la tarea de Actualización de bases de datos cada hora.

Si el proceso de descarga de las actualizaciones se interrumpe o provoca un error, Kaspersky Embedded Systems Security para Windows volverá automáticamente a utilizar las bases de datos de las últimas actualizaciones instaladas. Si las bases de datos de Kaspersky Embedded Systems Security para Windows se dañan, se pueden revertir manualmente a las actualizaciones anteriormente instaladas.

Esquemas para actualizar las bases de datos y los módulos de las aplicaciones antivirus utilizadas en una organización

La selección de un origen de actualizaciones en las tareas de actualización depende del esquema utilizado para actualizar las bases de datos y los módulos del programa en la organización.

Los módulos y bases de datos de Kaspersky Embedded Systems Security para Windows se pueden actualizar en los dispositivos protegidos mediante los esquemas siguientes:

- Descargar actualizaciones directamente de Internet a cada dispositivo protegido (Esquema 1).
- Descargar actualizaciones de Internet a un dispositivo intermediario y distribuirlas a dispositivos protegidos desde ese dispositivo.

  Cualquier dispositivo con los elementos de software enumerados a continuación instalados puede utilizarse como un dispositivo intermediario:

  - Kaspersky Embedded Systems Security para Windows (Esquema 2).
  - Servidor de administración de Kaspersky Security Center (Esquema 3).

La actualización mediante un dispositivo intermediario no solo reduce el tráfico de Internet, sino que también proporciona seguridad adicional para los dispositivos protegidos de la red.

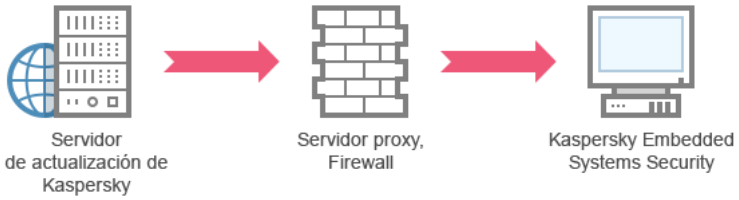
Los esquemas de actualización enumerados se describen a continuación.

Esquema 1. Actualización de bases de datos y módulos directamente desde Internet.

Para configurar actualizaciones de Kaspersky Embedded Systems Security para Windows directamente desde Internet:

en cada dispositivo protegido, en la configuración de la tarea de Actualización de bases de datos y la tarea de Actualización de módulos del programa, especifique los servidores de actualizaciones de Kaspersky como el origen de actualizaciones.

Se pueden configurar otros servidores HTTP o FTP que tengan una carpeta de actualización como el origen de actualizaciones.



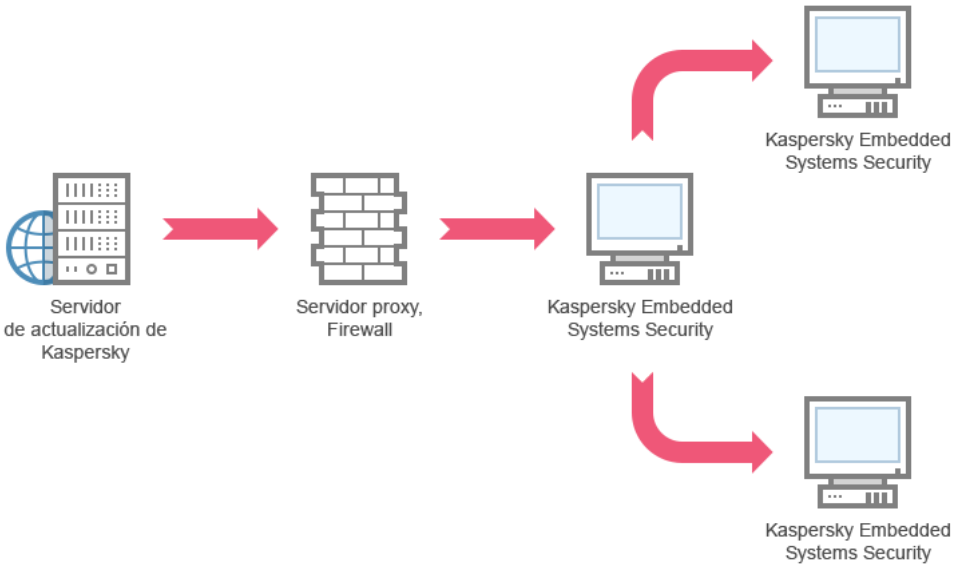
Esquema 1: Actualización de bases de datos y módulos directamente desde Internet

Esquema 2. Actualización de bases de datos y módulos a través de uno de los dispositivos protegidos

Para configurar actualizaciones de Kaspersky Embedded Systems Security para Windows mediante uno de los dispositivos protegidos:

1. Copie las actualizaciones en el dispositivo protegido seleccionado. Para ello, realice las siguientes acciones:
   - Configure la tarea de Copia de actualizaciones en el dispositivo protegido seleccionado:
     a. Especifique el servidor de actualizaciones de Kaspersky como el origen de actualizaciones.
     b. Especifique una carpeta compartida para utilizar como la carpeta donde se guardan las actualizaciones.
2. Distribuya las actualizaciones a otros dispositivos protegidos. Para ello, realice las siguientes acciones:
   - En cada dispositivo protegido, configure la tarea Actualización de bases de datos y la tarea Actualización de módulos del programa (vea la imagen a continuación):
     a. Como origen de actualizaciones, especifique la carpeta en la unidad del dispositivo intermediario en la cual se descargarán las actualizaciones.

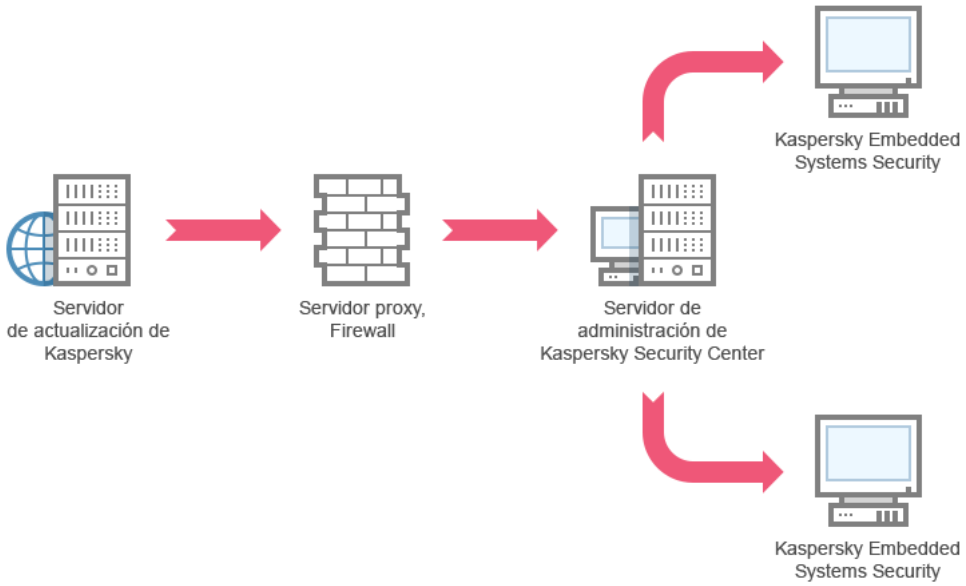
Kaspersky Embedded Systems Security para Windows obtendrá actualizaciones mediante uno de los dispositivos protegidos.



Esquema 2: Actualización de bases de datos y módulos a través de uno de los dispositivos protegidos

Esquema 3. Actualización de bases de datos y módulos a través del Servidor de administración de Kaspersky Security Center

Si se utiliza Kaspersky Security Center para la administración centralizada de la protección del dispositivo del antivirus, se pueden descargar las actualizaciones mediante el servidor de administración de Kaspersky Security Center instalado en la red de área local (consulte la figura a continuación).



Esquema 3: Actualización de bases de datos y módulos a través del Servidor de administración de Kaspersky Security Center

Para configurar actualizaciones de Kaspersky Embedded Systems Security para Windows mediante el Servidor de administración de Kaspersky Security Center:

1. Descargue las actualizaciones de los servidores de actualizaciones de Kaspersky en el servidor de administración de Kaspersky Security Center. Para ello, realice las siguientes acciones:

   - Configure la tarea de Recuperar actualizaciones por el servidor de administración para el conjunto especificado de dispositivos protegidos:

     a. Especifique el servidor de actualizaciones de Kaspersky como el origen de actualizaciones.

2. Distribuir actualizaciones a los dispositivos protegidos. Para esto, realice una de las siguientes acciones:

- En Kaspersky Security Center, configure una tarea de grupo de Actualización de bases de datos (módulo de aplicación) del antivirus para distribuir las actualizaciones en los dispositivos protegidos:

  a. En la programación de la tarea, especifique **Después de que el Servidor de administración obtenga las actualizaciones** como la frecuencia de inicio.

  El servidor de administración iniciará la tarea cada vez que reciba actualizaciones (método recomendado).

  La frecuencia de inicio **Después de que el Servidor de administración obtenga las actualizaciones** no se puede especificar en la Consola de la aplicación.

- En cada dispositivo protegido, configure la tarea de Actualización de bases de datos y de Actualización de módulos del programa:

  a. Especifique el servidor de administración de Kaspersky Security Center como origen de actualizaciones.

  b. Configure la programación de la tarea de ser necesario.

  Si la base de datos antivirus de Kaspersky Embedded Systems Security para Windows se actualiza con poca frecuencia (entre una vez al mes y una vez al año), la probabilidad de descubrir amenazas se reducirá y la frecuencia de falsas alarmas que surjan debido a los componentes de la aplicación aumentará.

Kaspersky Embedded Systems Security para Windows obtendrá actualizaciones mediante el Servidor de administración de Kaspersky Security Center.

Si planea utilizar el Servidor de administración de Kaspersky Security Center para distribuir actualizaciones, instale el Agente de red (un componente de aplicación incluido en el kit de distribución de Kaspersky Security Center) en cada uno de los dispositivos protegidos. Esto garantiza la interacción entre el Servidor de administración y Kaspersky Embedded Systems Security para Windows en el dispositivo protegido. Se proporciona información detallada sobre el Agente de red y su configuración con Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Configuración de tareas de Actualización

Esta sección proporciona instrucciones sobre cómo configurar tareas de Actualización de Kaspersky Embedded Systems Security para Windows.

Configuración de las opciones para trabajar con orígenes de actualizaciones de Kaspersky Embedded Systems Security para Windows

Para cada tarea de actualización excepto la tarea de Reversión de la actualización de bases de datos, puede especificar uno o más orígenes de actualizaciones, agregar orígenes de actualizaciones definidas por los usuarios y configurar las opciones para conectar con los orígenes especificados.

Después de que la configuración de la tarea de actualización se modifica, la nueva configuración no se aplicará inmediatamente en las tareas de actualización en ejecución. La configuración solo se aplicará cuando la tarea se reinicie.

Para especificar el tipo de origen de actualizaciones:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario correspondiente a la tarea de actualización que desea configurar.
3. Haga clic en el vínculo **Propiedades** en el panel de resultados del nodo seleccionado.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. En la sección **Origen de actualizaciones**, seleccione el tipo de origen de actualizaciones de Kaspersky Embedded Systems Security para Windows:
   - **Servidor de administración de Kaspersky Security Center**
   - **Servidores de actualizaciones de Kaspersky**
   - **Servidores FTP o HTTP personalizados o carpetas de red**
5. Si es necesario, establezca la configuración avanzada para los orígenes de actualizaciones definidas por los usuarios:
   a. Haga clic en el vínculo **Servidores FTP o HTTP personalizados o carpetas de red**.
      1. En la ventana **Servidores de actualizaciones** que se abre, seleccione o desactive las casillas de verificación al lado de los orígenes de actualizaciones definidas por los usuarios para iniciar o detener su uso.
      2. Haga clic en el botón **Aceptar**.
   b. En la sección **Origen de actualizaciones**, en la pestaña **General**, seleccione o desactive la casilla **Usar los servidores de actualizaciones de Kaspersky si no están disponibles los servidores especificados**.
6. En la ventana **Configuración de tareas**, seleccione la pestaña **Configuración de conexión** para establecer la configuración y conectarse con los orígenes de actualizaciones:
   - Desactive o seleccione la casilla de verificación **Usar la configuración del servidor proxy para conectarse a los servidores de actualizaciones de Kaspersky**.
   - Desactive o seleccione la casilla de verificación **Usar servidor proxy para otros servidores**.

   Para obtener información sobre cómo establecer la configuración del servidor proxy opcional y la configuración de autenticación para acceder al servidor proxy, consulte la sección Inicio y configuración de la tarea Actualización de bases de datos de Kaspersky Embedded Systems Security para Windows.
7. Haga clic en el botón **Aceptar**.

La configuración establecida para el origen de actualizaciones de Kaspersky Embedded Systems Security para Windows se guardará y se aplicará en el siguiente inicio de la tarea.

Puede administrar la lista de orígenes de actualizaciones definidas por los usuarios de Kaspersky Embedded Systems Security para Windows.

Para modificar la lista de orígenes de actualizaciones de aplicación definidas por los usuarios:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario correspondiente a la tarea de actualización que desea configurar.
3. Haga clic en el vínculo **Propiedades** en el panel de resultados del nodo seleccionado.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. Haga clic en el vínculo **Servidores FTP o HTTP personalizados o carpetas de red**.

   Se abre la ventana **Servidores de actualizaciones**.
5. Haga lo siguiente:

   - Para añadir un nuevo origen de actualizaciones definido por el usuario, haga clic en **Agregar** y, en el campo de entrada, especifique la dirección de la carpeta que contiene los archivos de actualización en el servidor FTP o HTTP. Especifique una carpeta local o de red en el formato UNC (convención de nomenclatura universal). Presione la tecla **INTRO**.

     De forma predeterminada, la carpeta agregada se utiliza como origen de actualizaciones.
   - Para deshabilitar el uso de un origen definido por el usuario, desactive la casilla de verificación al lado del origen en la lista.
   - Para habilitar el uso de un origen definido por el usuario, seleccione la casilla de verificación al lado del origen en la lista.
   - Para cambiar el orden en el que Kaspersky Embedded Systems Security para Windows accede a los orígenes de actualizaciones definidos por el usuario, utilice los botones **Subir** y **Bajar** para mover el origen seleccionado hacia el comienzo o final de la lista, según si se debe usar antes o después de otros orígenes.
   - Para cambiar la ruta de un origen, seleccione el origen en la lista y haga clic en el botón **Editar**, realice los cambios necesarios en el campo de entrada y presione la tecla **INTRO**.
   - Para eliminar un origen definido por el usuario, selecciónelo en la lista y haga clic en el botón **Eliminar**.

     No es posible eliminar el único origen definido por el usuario restante de la lista.
6. Haga clic en el botón **Aceptar**.

Se guardarán los cambios en la lista de orígenes de actualizaciones de la aplicación definidas por los usuarios.

Optimización de la lectura y escritura en disco al ejecutar la tarea de Actualización de bases de datos

Al ejecutar la tarea de Actualización de bases de datos, Kaspersky Embedded Systems Security para Windows almacena archivos de actualización en el disco local del dispositivo protegido. Puede reducir la carga de trabajo en el subsistema de lectura y escritura en disco del dispositivo protegido mediante el almacenamiento de archivos de actualización en una unidad virtual en RAM al ejecutar la tarea de actualización.

Esta función está disponible para los sistemas operativos Microsoft Windows 7 y superiores.

Cuando se usa esta función mientras se ejecuta la tarea Actualización de bases de datos, es posible que aparezca una unidad lógica adicional en el sistema. Esta unidad lógica se eliminará del sistema operativo después de que la tarea se complete.

Para reducir la carga de trabajo en el subsistema de lectura y escritura en disco de su dispositivo protegido durante la tarea Actualización de bases de datos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario **Actualización de bases de datos**.
3. Haga clic en el vínculo **Actualización de bases de datos** en el panel de resultados del nodo **Propiedades**.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. En la sección **Optimización de lectura y escritura en disco**, defina la siguiente configuración:
   - Desactive o seleccione la casilla de verificación **Reducir la carga de lectura y escritura en disco**.
   - En el campo **RAM usada para la optimización, MB**, especifique el volumen de RAM (en MB). El sistema operativo asigna temporalmente el volumen de RAM especificado para almacenar archivos de actualización al ejecutar la tarea. El tamaño de RAM predeterminado es 512 MB. El tamaño de RAM mínimo es 400 MB.

     Al ejecutar la tarea de Actualización de bases de datos con la función de optimización del subsistema del disco habilitada, puede producirse una de las siguientes situaciones, según la cantidad de memoria RAM asignada para la función:

     - Si el valor es demasiado pequeño, la cantidad de memoria RAM asignada podría ser insuficiente para completar la tarea de actualización de bases de datos (por ejemplo, durante la primera actualización); lo que conducirá a la finalización de la tarea con un error.

       En este caso, se recomienda asignar más memoria RAM para la función de optimización del subsistema del disco.

     - Si el valor es demasiado grande, al comienzo de la tarea de Actualización de bases de datos, podría ser imposible crear una unidad virtual de un tamaño seleccionado en la memoria RAM. Como consecuencia, la función de optimización del subsistema del disco se deshabilita automáticamente y la tarea de Actualización de bases de datos se ejecuta sin la función de optimización.

       En este caso, se recomienda asignar menos memoria RAM para la función de optimización del subsistema del disco.
5. Haga clic en el botón **Aceptar**.

Las opciones configuradas se guardarán y se aplicarán en el siguiente inicio de la tarea.

Configuración de parámetros de la tarea Copia de actualizaciones

Para configurar la tarea Copia de actualizaciones:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario **Copia de actualizaciones**.

3. Haga clic en el vínculo **Copia de actualizaciones** en el panel de resultados del nodo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

4. En las pestañas **General** y **Configuración de conexión**, configure las opciones para trabajar con orígenes de actualizaciones.

5. En la pestaña **General** en la sección **Configuración de la copia de actualizaciones**:

   - Especifique las condiciones para la copia de actualizaciones:
     - **Copiar actualizaciones de las bases de datos**.
     - **Copiar actualizaciones críticas de módulos del programa**.
     - **Copiar actualizaciones de bases de datos y actualizaciones críticas de módulos del programa**.
   - Especifique la carpeta local o de red a la cual Kaspersky Embedded Systems Security para Windows distribuirá las actualizaciones descargadas.

6. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas.

7. En la pestaña **Ejecutar como**, configure los ajustes para que la tarea se inicie utilizando una cuenta de usuario específica.

8. Haga clic en el botón **Aceptar**.

Las opciones configuradas se guardarán y se aplicarán en el siguiente inicio de la tarea.

Configuración de tareas de Actualización de módulos del programa

Para configurar la tarea de Actualización de módulos del programa:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.

2. Seleccione el nodo secundario **Actualización de módulos del programa**.

3. Haga clic en el vínculo **Actualización de módulos del programa** en el panel de resultados del nodo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

4. En las pestañas **General** y **Configuración de conexión**, configure las opciones para trabajar con orígenes de actualizaciones.

5. En la pestaña **General** de la sección **Configuración de actualización**, configure las opciones para actualizar módulos de la aplicación:

   - **Buscar solo actualizaciones críticas de módulos del programa**
   - **Copiar e instalar actualizaciones críticas de módulos del programa**
   - **Permitir el reinicio del sistema operativo**
   - **Informarme de las actualizaciones programadas que estén disponibles para los módulos del programa**

6. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas. De forma predeterminada, Kaspersky Embedded Systems Security para Windows ejecuta la tarea de Actualización de módulos del programa cada semana los viernes a las 04:00 p. m. (según la configuración regional de la hora en el dispositivo protegido).

7. En la pestaña **Ejecutar como**, configure los ajustes para que la tarea se inicie utilizando una cuenta de usuario específica.

8. Haga clic en el botón **Aceptar**.

Las opciones configuradas se guardarán y se aplicarán en el siguiente inicio de la tarea.

Kaspersky no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la instalación automática; se deben descargar manualmente desde el sitio web de Kaspersky. Puede configurar la notificación del administrador sobre el evento *Hay nuevas actualizaciones críticas y programadas disponibles*. La notificación incluirá la URL del sitio web donde se pueden descargar las actualizaciones programadas.

Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security para Windows

Antes de que se realicen las actualizaciones de las bases de datos, Kaspersky Embedded Systems Security crea copias de seguridad de las bases de datos anteriormente usadas. Si una actualización se interrumpió o arrojó un error, Kaspersky Embedded Systems Security para Windows volverá automáticamente a usar las bases de datos anteriormente instaladas.

Si se produce algún problema después de la actualización de bases de datos, puede regresar a las actualizaciones instaladas anteriormente mediante la tarea Reversión de la actualización de bases de datos.

Para iniciar la tarea Reversión de la actualización de bases de datos:

En el panel de resultados del nodo **Reversión de la actualización de bases de datos de la aplicación**, haga clic en el vínculo **Iniciar**.

Reversión de actualizaciones del módulo de aplicación

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Antes de aplicar actualizaciones de módulos del programa, Kaspersky Embedded Systems Security para Windows crea copias de seguridad de los módulos actualmente en uso. Si el proceso de actualización de los módulos se interrumpió o arrojó un error, Kaspersky Embedded Systems Security para Windows volverá automáticamente a usar los módulos de las últimas actualizaciones instaladas.

Para revertir los módulos del programa, utilice la función **Instalar y eliminar aplicaciones** en Microsoft Windows.

Estadísticas de las tareas de actualización

Mientras se ejecuta la tarea de actualización, se muestra la información en tiempo real sobre la cantidad de datos descargados desde que se inició la tarea, así como otras estadísticas de ejecución de la tarea.

Cuando la tarea finaliza o se detiene, la información está disponible en el registro de tareas.

Para ver las estadísticas de las tareas de actualización:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario que corresponda a la tarea cuyas estadísticas desea ver.

   Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de resultados del nodo seleccionado.

Si está viendo la tarea Actualización de bases de datos o la tarea Copia de actualizaciones, la sección **Estadísticas** muestra el volumen de datos descargados por Kaspersky Embedded Systems Security en el momento actual (**Datos recibidos**).

La siguiente tabla contiene los detalles de la tarea de Actualización de módulos del programa.

Información sobre la tarea de Actualización de módulos del programa

Campo	Descripción
Datos recibidos	Cantidad total de datos descargados.
Actualizaciones críticas disponibles	Cantidad de actualizaciones críticas disponibles para instalar.
Actualizaciones programadas disponibles	Cantidad de actualizaciones planificadas disponibles para la instalación.
Errores al aplicar las actualizaciones	Si el valor de este campo no es cero, la actualización no se aplicó. Se puede ver el nombre de la actualización que causó un error en el registro de tareas.

Aislamiento de objetos y copia de copias de seguridad

Esta sección proporciona información sobre las copias de seguridad de objetos maliciosos detectados antes de su desinfección o eliminación, y sobre poner en cuarentena a los objetos probablemente infectados.

Cómo aislar objetos probablemente infectados. Cuarentena

En esta sección se describe cómo aislar objetos probablemente infectados poniéndolos en cuarentena y cómo configurar las opciones de Cuarentena.

Acerca de la puesta en cuarentena de objetos probablemente infectados

Kaspersky Embedded Systems Security para Windows pone en cuarentena los objetos probablemente infectados al pasarlos de su ubicación original a la carpeta de *Cuarentena*. Por motivos de seguridad, los objetos en la carpeta Cuarentena se almacenan en forma cifrada.

Visualización de los objetos en cuarentena

Los objetos en cuarentena se pueden visualizar en el nodo **Cuarentena** de la consola de la aplicación.

Para visualizar los objetos en cuarentena:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.

   La información sobre los objetos en Cuarentena se muestra en el panel de resultados del nodo seleccionado.

Para encontrar el objeto requerido en la lista de objetos en cuarentena,

ordene los objetos o filtre los objetos.

Cómo ordenar los objetos en Cuarentena

De manera predeterminada, los objetos en la lista de objetos en cuarentena se ordenan por la fecha de cuarentena en orden cronológico inverso. Para encontrar el objeto requerido, puede ordenar los objetos por las columnas con la información del objeto. El resultado de la clasificación se guardará si cierra y vuelve a abrir el nodo **Cuarentena**, o si cierra la Consola de la aplicación, guarda el archivo msc y vuelve a abrirla desde este archivo.

Para ordenar objetos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.

3. En el panel de resultados del nodo **Cuarentena**, seleccione el encabezado de columna que desee usar para ordenar los objetos en la lista.

Los objetos en la lista se ordenarán según el parámetro seleccionado.

Filtrado de objetos en cuarentena

Para buscar el objeto en cuarentena requerido, puede filtrar los objetos de la lista, es decir, mostrar solo los objetos que satisfagan los criterios de filtrado (filtros) que especifique. Los resultados filtrados se guardarán si cierra y vuelve a abrir el nodo **Cuarentena** o si cierra la consola de la aplicación, guarda el archivo msc y vuelve a abrirlo desde este archivo.

Para especificar uno o más filtros:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.
3. Seleccione **Filtrar** en el menú contextual del nombre del nodo.

   Se abre la ventana **Configuración de filtro**.
4. Para agregar un filtro, siga estos pasos:
   a. En la lista **Nombre del campo**, seleccione el campo que formará la base del filtro.
   b. En la lista **Operador**, seleccione la condición de filtrado. Las condiciones de filtrado en la lista pueden diferir según el valor seleccionado en la lista **Nombre del campo**.
   c. Introduzca el valor de filtro en el campo **Valor del campo** o seleccione el valor del filtro.
   d. Haga clic en el botón **Agregar**.

   El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**. Repita los pasos a-d para cada filtro que agregue. Siga estas pautas para utilizar los filtros:
   - Para combinar varios filtros mediante el operador lógico "AND", seleccione **Si se cumplen todas las condiciones**.
   - Para combinar varios filtros mediante el operador lógico "OR", seleccione **Si se cumple alguna condición**.
   - Para eliminar un filtro, seleccione el filtro que desea eliminar en la lista de filtros y haga clic en el botón **Eliminar**.
   - Para editar un filtro, seleccione el filtro de la lista en la ventana **Configuración de filtro**. Luego, cambie los valores requeridos en el campo **Nombre del campo**, **Operador** o **Valor del campo** y haga clic en el botón **Reemplazar**.
5. Después de haber agregado todos los filtros, haga clic en el botón **Aplicar**.

Se guardarán los filtros creados.

Para volver a mostrar todos los objetos en cuarentena,

seleccione **Cuarentena** en el menú contextual del nodo **Eliminar filtro**.

Análisis de archivos en cuarentena

De forma predeterminada, después de cada actualización de bases de datos, Kaspersky Embedded Systems Security para Windows realiza la tarea local del sistema Análisis de archivos en cuarentena. La configuración de la tarea se describe en la tabla a continuación. La configuración de la tarea de Análisis de archivos en cuarentena no se puede modificar.

Puede configurar el inicio programado de la tarea, iniciar la tarea manualmente y modificar los permisos de la cuenta con la que se inicia la tarea.

Después de analizar los objetos en cuarentena luego de actualizar las bases de datos, es posible que Kaspersky Embedded Systems Security para Windows vuelva a clasificar algunos objetos como no infectados: el estado de dichos objetos cambiará a **Falsa alarma**. Es posible que otros objetos vuelvan a clasificarse como infectados, en cuyo caso Kaspersky Embedded Systems Security para Windows gestiona tales objetos según lo especificado por la configuración de la tarea de Análisis de archivos en cuarentena: desinfectar, o eliminar si la desinfección produjera un error.

Configuración de la tarea de Análisis de archivos en cuarentena

Configuración de la tarea de Análisis de archivos en cuarentena	Valor
Área del análisis	Carpeta de cuarentena
Configuración de seguridad	Lo mismo para toda el área del análisis; los valores se proporcionan en la tabla a continuación

Configuración del análisis en la tarea de Análisis de archivos en cuarentena

Configuración de seguridad	Valor
Analizar objetos	Todos los objetos incluidos en el área del análisis
Rendimiento	Deshabilitado
Acción que se realizará con los objetos infectados y otros objetos	Desinfectar. Si la desinfección es imposible, eliminar
Acción que se realizará con los objetos probablemente infectados	Omitir
Excluir archivos	No
No detectar	No
Detener el análisis si demora más de (s)	No definido
No analizar objetos de más de (MB)	No definido
Analizar secuencias alternativas de NTFS	Habilitado
Analizar sectores de inicio del disco y MBR	Deshabilitado
Usar la tecnología iChecker	Deshabilitado
Usar la tecnología iSwift	Deshabilitado
Analizar objetos compuestos	• **Archivos comprimidos*** • **Archivos SFX*** • **Objetos empaquetados***

	• **Objetos OLE incorporados*** * La opción **Analizar solo los archivos nuevos y modificados** está deshabilitada.
Comprobar si el archivo está firmado por Microsoft	No se realizó
Usar el analizador heurístico	Habilitado con nivel de análisis **Profundo**
Zona de confianza	No aplicado

Restauración de objetos en cuarentena

Kaspersky Embedded Systems Security para Windows coloca los objetos probablemente infectados en la carpeta de Cuarentena en forma cifrada para proteger al dispositivo protegido contra cualquier posible efecto perjudicial.

Puede restaurar cualquier objeto de Cuarentena. Esto puede resultar necesario en los siguientes casos:

- Después de realizar el Análisis de archivos en cuarentena mediante el uso de una base de datos actualizada, el estado del objeto cambió a **Falsa alarma** o **Desinfectado**.
- Usted considera que el objeto no es peligroso para el dispositivo protegido y desea utilizarlo. Si no desea que Kaspersky Embedded Systems Security para Windows aísle el objeto durante los análisis sucesivos, puede excluir el objeto del procesamiento en la tarea de Protección de archivos en tiempo real y las tareas de Análisis a pedido. Para ello, especifique el objeto en la configuración de seguridad **Excluir archivos** (por nombre de archivo) o **No detectar** en esas tareas, o bien agréguelo a la Zona de confianza.

Al restaurar un objeto, puede seleccionar dónde se guardará el objeto restaurado: en su ubicación original (opción predeterminada), en una carpeta utilizada especialmente para colocar los objetos restaurados en el dispositivo protegido o en una carpeta personalizada que se encuentre, bien en el dispositivo protegido en el que esté instalada la Consola de la aplicación, bien en otro dispositivo de la red.

Puede especificar la carpeta para almacenar objetos restaurados en el dispositivo protegido. Puede configurar los valores de seguridad especiales para que se realice su análisis. La ruta a esta carpeta está definida por la configuración de Cuarentena.

Restaurar archivos de Cuarentena puede dar lugar a una infección en el dispositivo protegido.

Puede restaurar el objeto y guardar su copia en la carpeta de Cuarentena para usarla después, por ejemplo, para volver a analizar el objeto después de que se haya actualizado la base de datos.

Si un objeto en cuarentena estaba contenido en un objeto compuesto (por ejemplo, en un archivo de almacenamiento), Kaspersky Embedded Systems Security para Windows no incluirá el objeto en cuarentena cuando se restaure el objeto compuesto. El objeto en cuarentena se guardará por separado en la carpeta seleccionada.

Puede restaurar uno o más objetos.

Para restaurar objetos en cuarentena, siga estos pasos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.

2. Seleccione el nodo secundario **Cuarentena**.

3. En el panel de detalles del nodo **Cuarentena**, realice una de las siguientes acciones:

   - Para restaurar un objeto, seleccione **Restaurar** desde el menú contextual del objeto que desea restaurar.

   - Para restaurar varios objetos, seleccione los objetos que desea restaurar mediante la tecla **CTRL** o **MAYÚS**, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione Restaurar en el menú contextual.

   Se abre la ventana **Restaurar objeto**.

4. En la ventana **Restaurar objeto**, especifique la carpeta en la que se guardará el objeto restaurado para cada objeto seleccionado.

   El nombre del objeto restaurado se muestra en el campo **Objeto** en la parte superior de la ventana. Si selecciona varios objetos, se mostrará el nombre del primer objeto en la lista de objetos seleccionados.

5. Realice una de las siguientes opciones:

   - Para restaurar un objeto a su ubicación original, seleccione **Restaurar a la carpeta de origen**.

   - Para restaurar un objeto a la carpeta especificada como la ubicación para los objetos restaurados en la configuración, seleccione **Restaurar a la carpeta de restauración predeterminada**.

   - Para guardar un objeto en una carpeta diferente del dispositivo protegido en el que esté instalada la Consola de la aplicación, seleccione **Restaurar a una carpeta del equipo local** y seleccione la carpeta en cuestión (o especifique la ruta a dicha carpeta).

6. Si desea guardar una copia del objeto en la carpeta de *Cuarentena* después de restaurarlo, desactive la casilla de verificación **Eliminar objetos del depósito una vez restaurados**.

7. Para aplicar las condiciones de restauración especificadas en los restantes objetos seleccionados, active la casilla de verificación **Aplicar a todos los objetos seleccionados**.

   Todos los objetos seleccionados se restaurarán y se guardarán en la ubicación especificada. Si seleccionó **Restaurar a la carpeta de origen**, cada uno de los objetos se guardará en su ubicación original; si seleccionó **Restaurar a la carpeta de restauración predeterminada** o **Restaurar a una carpeta del equipo local**, todos los objetos se guardarán en la carpeta especificada.

8. Haga clic en el botón **Aceptar**.

   Kaspersky Embedded Systems Security para Windows iniciará la restauración del primero de los objetos seleccionados.

9. Si ya existe un objeto con este nombre en la ubicación especificada, se abrirá la ventana **Ya existe un objeto con este nombre**.

   a. Seleccione una de las siguientes acciones de Kaspersky Embedded Systems Security para Windows:

      - **Reemplazar**, para sustituir el objeto existente con el objeto restaurado.

      - **Cambiar el nombre**, para guardar un objeto restaurado con otro nombre. En el campo de entrada, introduzca el nombre de archivo del nuevo objeto restaurado y la ruta completa.

      - **Agregar un sufijo al nombre**, para cambiar el nombre del objeto restaurado al agregar un sufijo a su nombre de archivo. Escriba el sufijo en el campo de entrada.

b. Si eligió varios objetos para restaurar, seleccione la casilla de verificación **Cambiar el nombre** para aplicar la acción seleccionada (**Aplicar a todos los objetos seleccionados** o **Reemplazar**) al resto de los objetos seleccionados. Si seleccionó **Cambiar el nombre**, la casilla de verificación **Aplicar a todos los objetos seleccionados** no estará disponible.

c. Haga clic en el botón **Aceptar**.

Se restaurará el objeto. En el registro de auditoría del sistema se incluirá la información sobre la operación de restauración.

Si no seleccionó **Aplicar a todos los objetos seleccionados** en la ventana **Restaurar objeto**, la ventana **Restaurar objeto** puede abrirse de nuevo. Utilice esta ventana para especificar la ubicación donde se guardará el objeto seleccionado (vea el paso 4 de este procedimiento).

Cómo mover objetos a Cuarentena

Puede enviar archivos a Cuarentena de forma manual.

Para poner en cuarentena un archivo:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Cuarentena**.
2. Seleccione **Agregar**.
3. En la ventana **Abrir**, seleccione el archivo del disco que desea poner en cuarentena.
4. Haga clic en el botón **Aceptar**.

Kaspersky Embedded Systems Security para Windows pondrá en cuarentena el archivo seleccionado.

Eliminación de objetos de la cuarentena

Según la configuración de la tarea de Análisis de archivos en cuarentena, Kaspersky Embedded Systems Security para Windows elimina automáticamente de la carpeta de Cuarentena los objetos cuyo estado cambió a *Infectado* durante un Análisis de archivos en cuarentena con las bases de datos actualizadas y si Kaspersky Embedded Systems Security para Windows no pudo desinfectarlos. Kaspersky Embedded Systems Security para Windows no elimina otros objetos de la Cuarentena.

Es posible eliminar uno o más objetos de la Cuarentena.

Para eliminar uno o más objetos de la Cuarentena:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.
3. Realice una de las siguientes opciones:

   - Para eliminar un objeto, seleccione **Eliminar** en el menú contextual del nombre del objeto.
   - Para eliminar varios objetos, seleccione los objetos que desea eliminar con las teclas **Ctrl** o **Shift**, abra el menú contextual en cualquiera de los objetos seleccionados y seleccione **Eliminar**.

4. En la ventana de confirmación, haga clic en el botón **Sí** para confirmar la operación.

Los objetos seleccionados se eliminarán de la Cuarentena.

Envío de objetos probablemente infectados a Kaspersky para su análisis

Si el comportamiento de un archivo le da motivos para sospechar que contiene una amenaza y Kaspersky Embedded Systems Security para Windows considera que el archivo está limpio, es posible que se trate de una amenaza desconocida, cuya firma aún no se agregó a las bases de datos. Puede enviar este archivo a Kaspersky para análisis. Los analistas de antivirus de Kaspersky lo analizarán y si detectan una amenaza nueva, la agregarán a un registro que la identificará en las bases de datos. Cuando vuelva a analizar el objeto después de que la base de datos se haya actualizado, es probable que Kaspersky Embedded Systems Security para Windows identifique el objeto como infectado y pueda desinfectarlo. No solo podrá conservar el objeto, sino que también evitará un ataque de virus.

Sólo los archivos en cuarentena se pueden enviar para análisis. Los archivos en cuarentena se almacenan en forma cifrada y la aplicación antivirus instalada en el servidor de correo no los elimina cuando se envían.

Un objeto en cuarentena no puede enviarse a Kaspersky para su análisis después de que caduque la licencia.

Para enviar un archivo para su análisis a Kaspersky:

1. Si el archivo no se colocó en cuarentena, en primer lugar, muévalo a **Cuarentena**.

2. En el nodo **Cuarentena**, abra el menú contextual del archivo que desea enviar para análisis y seleccione **Enviar objeto a analizar** en el menú contextual.

3. En la ventana de confirmación que se abre, haga clic en **Sí** si está seguro de que desea enviar el objeto seleccionado a análisis.

4. Si un cliente de correo está configurado en el dispositivo protegido en que está instalada la consola de la aplicación, se crea un nuevo mensaje de correo electrónico. Revíselo y haga clic en el botón **Enviar**.

   El campo **Destinatario** contiene la dirección de correo electrónico de Kaspersky newvirus@kaspersky.com. El campo Asunto contendrá el texto "Objeto en cuarentena".

   El cuerpo del mensaje contendrá el texto "El objeto se enviará a analizar a Kaspersky". Cualquier información adicional sobre el archivo, por qué se consideró probablemente infectado o peligroso, cómo se comporta o cómo afecta el sistema puede incluirse en el cuerpo del mensaje.

   Un archivo de almacenamiento <nombre de objeto>.cab se adjuntará al mensaje. Dentro de este archivo, se incluirá un archivo <uuid>.klq con el objeto en formato cifrado, un archivo <uuid>.txt con información sobre el objeto recibida de Kaspersky Embedded Systems Security para Windows y un archivo Sysinfo.txt con la siguiente información sobre Kaspersky Embedded Systems Security para Windows y el sistema operativo instalado en el dispositivo protegido:

   - Nombre y versión del sistema operativo.
   - Nombre y versión de Kaspersky Embedded Systems Security para Windows.
   - Fecha de lanzamiento de la última actualización de bases de datos instalada.
   - Clave activa.

Los analistas de antivirus de Kaspersky necesitan esta información para analizar su archivo de manera más rápida y eficaz. Sin embargo, si no desea enviar esta información, puede eliminar el archivo Sysinfo.txt del archivo de almacenamiento.

Si un cliente de correo no está instalado en el dispositivo protegido con la Consola de la aplicación, la aplicación le solicita guardar el objeto cifrado seleccionado en el archivo. Este archivo se puede enviar a Kaspersky en forma manual.

Para guardar un objeto cifrado en un archivo:

1. En la ventana que se abre con una solicitud para guardar el objeto, haga clic en **Aceptar**.
2. Seleccione la carpeta en la que desee guardar el archivo que contiene el objeto. Puede seleccionar una carpeta del dispositivo protegido o una carpeta de red.

El objeto se guardará en un archivo CAB.

Configuración de las opciones de la Cuarentena

Puede configurar las opciones de la Cuarentena. La nueva configuración de la Cuarentena se aplica inmediatamente después de guardar las opciones.

Para configurar las opciones de la Cuarentena:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Abra el menú contextual en el nodo secundario **Cuarentena**.
3. Seleccione **Propiedades**.
4. En la ventana de propiedades de **Cuarentena**, configure los ajustes de Cuarentena según sus necesidades:
   - En la sección **Configuración de Cuarentena**:
     - Carpeta de Cuarentena
     - Tamaño máximo de cuarentena (MB)
     - Valor umbral de espacio disponible (MB)

     Si el tamaño de los objetos en la Cuarentena supera el tamaño máximo de Cuarentena o supera el umbral del espacio disponible, Kaspersky Embedded Systems Security para Windows le notificará sobre esto y, al mismo tiempo, continuará colocando objetos en la Cuarentena.
   - En la sección **Configuración de restauración**:
     - Carpeta de destino para restaurar objetos
5. Haga clic en el botón **Aceptar**.

Se guardarán las opciones de Cuarentena configuradas recientemente.

Estadísticas de cuarentena

Se puede visualizar información sobre la cantidad de objetos en cuarentena, es decir, estadísticas de cuarentena.

Para ver las estadísticas de Cuarentena,

abra el menú contextual en el nodo **Cuarentena** en el árbol de la Consola de la aplicación y seleccione **Estadísticas**.

La ventana **Estadísticas de Cuarentena** muestra información sobre la cantidad de objetos almacenados en Cuarentena (consulte la tabla a continuación):

Campo	Descripción
Objetos probablemente infectados	Cantidad de objetos probablemente infectados encontrados por Kaspersky Embedded Systems Security para Windows.
Espacio de Cuarentena utilizado	Cantidad total de datos en la carpeta de Cuarentena.
Falsos positivos	La cantidad de objetos que recibieron el estado *Falsa alarma* debido a que se clasificaron como no infectados durante un Análisis de archivos en cuarentena con las bases de datos actualizadas.
Objetos desinfectados	La cantidad de objetos que recibieron el estado *Desinfectado* después del Análisis de archivos en cuarentena.
Número total de objetos	Cantidad total de objetos en cuarentena.

Creación de copias de seguridad de los objetos. Copia de seguridad

Esta sección brinda información sobre las copias de seguridad de los objetos maliciosos detectados antes de la desinfección o la eliminación, así como instrucciones para configurar las Copia de seguridad.

Acerca de la copia de seguridad de objetos antes de la desinfección o eliminación

Kaspersky Embedded Systems Security para Windows almacena copias cifradas de los objetos clasificados como *Infectados* en *Copia de seguridad* antes de desinfectarlos o eliminarlos.

Si el objeto forma parte de un objeto compuesto (por ejemplo, parte de un archivo de almacenamiento), Kaspersky Embedded Systems Security para Windows guardará el objeto compuesto en su totalidad en Copia de seguridad. Por ejemplo, si Kaspersky Embedded Systems Security para Windows ha detectado que uno de los objetos de una base de datos de correo está infectado, hará una copia de seguridad de toda la base de datos de correo.

Los objetos grandes ubicados en Copia de seguridad por Kaspersky Embedded Systems Security para Windows pueden ralentizar el sistema y reducir el espacio disponible en el disco duro.

Los archivos se pueden restaurar de la Copia de seguridad a su carpeta original o a una carpeta diferente en el dispositivo protegido o en otro dispositivo de la red de área local. Un archivo se puede restaurar de la Copia de seguridad, por ejemplo, si un archivo infectado contiene información importante. Sin embargo, Kaspersky Embedded Systems Security para Windows no puede desinfectarlo sin dañar su integridad y perder la información.

Restaurar archivos de Copia de seguridad puede dar lugar a una infección en el dispositivo protegido.

Visualización de objetos almacenados en Copia de seguridad

Los objetos se pueden visualizar en la carpeta de Copia de seguridad solo mediante la Consola de la aplicación en el nodo **Copia de seguridad**. No se pueden visualizar mediante los administradores de archivos de Microsoft Windows.

Para ver los objetos en la Copia de seguridad,

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Copia de seguridad**.

   La información sobre los objetos colocados en Copia de seguridad se muestra en el panel de resultados del nodo seleccionado.

Para encontrar el objeto necesario en la lista de Objetos en Copia de seguridad,

ordene los objetos o filtre los objetos.

Cómo ordenar archivos en Copia de seguridad

De manera predeterminada, los archivos en Copia de seguridad se ordenan por la fecha de copia de seguridad en orden cronológico inverso. Para buscar el archivo requerido, puede ordenarlos de acuerdo con el contenido de cualquiera de las columnas en el panel de resultados.

El resultado de la clasificación se guardará si usted cierra y vuelve a abrir el nodo **Copia de seguridad** o si cierra la Consola de la aplicación, guarda el archivo msc y vuelve a abrirla desde este archivo.

Para ordenar archivos en Copia de seguridad:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Copia de seguridad**.
3. En la lista de archivos del nodo **Copia de seguridad**, seleccione el encabezado de la columna que desea usar para ordenar los objetos.

Los archivos en Copia de seguridad se ordenarán según el criterio seleccionado.

Filtrado de archivos en Copia de seguridad

Para buscar el archivo requerido en Copia de seguridad, puede filtrar los archivos: mostrar en el nodo **Copia de seguridad** solo los archivos que satisfagan los criterios de filtrado (filtros) que haya especificado.

El resultado de la clasificación se guardará si usted cierra y vuelve a abrir el nodo **Copia de seguridad** o si cierra la Consola de la aplicación, guarda el archivo msc y vuelve a abrirla desde este archivo.

Para filtrar archivos en Copia de seguridad:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Copia de seguridad** y seleccione **Filtrar**.

   Se abre la ventana **Configuración de filtro**.

2. Para agregar un filtro, siga estos pasos:

   a. En la lista **Nombre del campo**, seleccione el campo que formará la base del filtro.

   b. En la lista **Operador**, seleccione la condición de filtrado. Las condiciones de filtrado en la lista pueden diferir según el valor seleccionado en el campo **Nombre del campo**.

   c. Introduzca el valor de filtro en el campo **Valor del campo** o seleccione el valor del filtro.

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

   El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**. Repita estos pasos para cada filtro que agregue. Siga estas pautas para utilizar los filtros:

   - Para combinar varios filtros mediante el operador lógico "AND", seleccione **Si se cumplen todas las condiciones**.
   - Para combinar varios filtros mediante el operador lógico "OR", seleccione **Si se cumple alguna condición**.
   - Para eliminar un filtro, seleccione el filtro que desea eliminar en la lista de filtros y haga clic en el botón **Eliminar**.
   - Para editar un filtro, selecciónelo en la lista de filtros de la ventana **Configuración de filtro**, modifique los valores necesarios en los campos **Nombre del campo**, **Operador** y **Valor del campo**, y haga clic en el botón **Reemplazar**.

   Una vez agregados todos los filtros, haga clic en el botón **Aplicar**. Solo los archivos que coinciden con los filtros especificados se mostrarán en la lista.

Para mostrar todos los archivos incluidos en la lista de objetos almacenados en Copia de seguridad,

seleccione **Copia de seguridad** en el menú contextual del nodo **Eliminar filtro**.

Restauración de archivos de Copia de seguridad

Kaspersky Embedded Systems Security para Windows almacena archivos en la carpeta Copia de seguridad en forma cifrada para proteger el dispositivo protegido contra cualquier posible efecto peligroso.

Se puede restaurar cualquier archivo de la copia de seguridad.

Es posible que se deba restaurar un archivo en los casos siguientes:

- El archivo original infectado contenía información importante y Kaspersky Embedded Systems Security para Windows no pudo mantener su integridad. Como resultado, la información contenida en el archivo dejó de estar disponible.

- Usted considera que el archivo no es peligroso para el dispositivo protegido y desea utilizarlo. Si no desea que Kaspersky Embedded Systems Security para Windows considere a este archivo infectado o probablemente infectado durante los análisis subsiguientes, puede excluirlo del procesamiento en la tarea de Protección de archivos en tiempo real y las tareas de Análisis a pedido. Para ello, especifique el archivo en la configuración **Excluir archivos** o en la configuración **No detectar** en las tareas correspondientes.

  Restaurar archivos de Copia de seguridad puede dar lugar a una infección en el dispositivo protegido.

Al restaurar un archivo, puede seleccionar dónde guardarlo: en su ubicación original (opción predeterminada), en una carpeta utilizada especialmente para colocar los objetos restaurados en el dispositivo protegido o en una carpeta personalizada que se encuentre, bien en el dispositivo protegido en el que esté instalada la Consola de la aplicación, bien en otro dispositivo de la red.

Puede especificar la carpeta para almacenar objetos restaurados en el dispositivo protegido. Puede configurar los valores de seguridad especiales para que se realice su análisis. La ruta de acceso a esta carpeta se define en la configuración de Copia de seguridad.

De manera predeterminada, cuando Kaspersky Embedded Systems Security para Windows restaura un archivo, hace una copia de él en Copia de seguridad. La copia del archivo se puede eliminar de la copia de seguridad una vez restaurado.

Para restaurar archivos de Copia de seguridad:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.

2. Seleccione el nodo secundario **Copia de seguridad**.

3. En el panel de detalles del nodo **Copia de seguridad**, realice una de las siguientes acciones:

   - Para restaurar un objeto, seleccione **Restaurar** desde el menú contextual del objeto que desea restaurar.

   - Para restaurar varios objetos, seleccione los objetos que desea restaurar mediante la tecla **CTRL** o **MAYÚS**, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione Restaurar en el menú contextual.

   Se abre la ventana **Restaurar objeto**.

4. En la ventana **Restaurar objeto**, especifique la carpeta en la que se guardará el objeto restaurado para cada objeto seleccionado.

   El nombre del objeto restaurado se muestra en el campo **Objeto** en la parte superior de la ventana. Si selecciona varios objetos, se mostrará el nombre del primer objeto en la lista de objetos seleccionados.

5. Realice una de las siguientes opciones:

   - Para restaurar un objeto a su ubicación original, seleccione **Restaurar a la carpeta de origen**.

- Para restaurar un objeto a la carpeta especificada como la ubicación para los objetos restaurados en la configuración, seleccione **Restaurar a la carpeta de restauración predeterminada**.

- Para guardar un objeto en una carpeta diferente del dispositivo protegido en el que esté instalada la Consola de la aplicación, seleccione **Restaurar a una carpeta del equipo local** y seleccione la carpeta en cuestión (o especifique la ruta a dicha carpeta).

6. Si no desea guardar una copia del archivo en la carpeta Copia de seguridad después de restaurarlo, seleccione la casilla de verificación **Eliminar objetos del depósito una vez restaurados** (de manera predeterminada, esta casilla de verificación está desactivada).

7. Para aplicar las condiciones de restauración especificadas en los restantes objetos seleccionados, active la casilla de verificación **Aplicar a todos los objetos seleccionados**.

   Todos los objetos seleccionados se restaurarán y se guardarán en la ubicación especificada. Si seleccionó **Restaurar a la carpeta de origen**, cada uno de los objetos se guardará en su ubicación original; si seleccionó **Restaurar a la carpeta de restauración predeterminada** o **Restaurar a una carpeta del equipo local**, todos los objetos se guardarán en la carpeta especificada.

8. Haga clic en el botón **Aceptar**.

   Kaspersky Embedded Systems Security para Windows iniciará la restauración del primero de los objetos seleccionados.

9. Si ya existe un objeto con este nombre en la ubicación especificada, se abrirá la ventana **Ya existe un objeto con este nombre**.

   a. Seleccione una de las siguientes acciones de Kaspersky Embedded Systems Security para Windows:

      - **Reemplazar**, para sustituir el objeto existente con el objeto restaurado.

      - **Cambiar el nombre**, para guardar un objeto restaurado con otro nombre. En el campo de entrada, introduzca el nombre de archivo del nuevo objeto restaurado y la ruta completa.

      - **Agregar un sufijo al nombre**, para cambiar el nombre del objeto restaurado al agregar un sufijo a su nombre de archivo. Escriba el sufijo en el campo de entrada.

   b. Si eligió varios objetos para restaurar, seleccione la casilla de verificación **Cambiar el nombre** para aplicar la acción seleccionada (**Aplicar a todos los objetos seleccionados** o **Reemplazar**) al resto de los objetos seleccionados. Si seleccionó **Cambiar el nombre**, la casilla de verificación **Aplicar a todos los objetos seleccionados** no estará disponible.

   c. Haga clic en el botón **Aceptar**.

   Se restaurará el objeto. En el registro de auditoría del sistema se incluirá la información sobre la operación de restauración.

Si no seleccionó **Aplicar a todos los objetos seleccionados** en la ventana **Restaurar objeto**, la ventana **Restaurar objeto** puede abrirse de nuevo. Utilice esta ventana para especificar la ubicación donde se guardará el objeto seleccionado (vea el paso 4 de este procedimiento).

Eliminación de archivos de Copia de seguridad

Para eliminar uno o más archivos de Copia de seguridad:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.

2. Seleccione el nodo secundario **Copia de seguridad**.

3. Realice una de las siguientes opciones:

   - Para eliminar un objeto, seleccione **Eliminar** en el menú contextual del nombre del objeto.

   - Para eliminar varios objetos, seleccione los objetos que desea eliminar con las teclas **Ctrl** o **Shift**, abra el menú contextual en cualquiera de los objetos seleccionados y seleccione **Eliminar**.

4. En la ventana de confirmación, haga clic en el botón **Sí** para confirmar la operación.

Los archivos seleccionados se eliminarán de las Copia de seguridad.

Configuración de Copia de seguridad

Para configurar las opciones de Copia de seguridad:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.

2. Abra el menú contextual en el nodo **Copia de seguridad**.

3. Seleccione **Propiedades**.

4. En la ventana de propiedades de **Copia de seguridad**, configure los ajustes de Copia de seguridad según sus necesidades:

   En la sección **Configuración de Copia de seguridad**:

   - Carpeta de Copia de seguridad

   - Tamaño máx. de Copia de seguridad (MB)

   - Valor umbral de espacio disponible (MB)

     > Si el tamaño de los objetos en Copia de seguridad supera el tamaño máximo de Copia de seguridad o supera el umbral del espacio disponible, Kaspersky Embedded Systems Security para Windows le notificará sobre esto y, al mismo tiempo, continuará colocando objetos en Copia de seguridad.

   En la sección **Configuración de restauración**:

   - Carpeta de destino para restaurar objetos

5. Haga clic en el botón **Aceptar**.

Se guarda la configuración de Copia de seguridad.

Estadísticas de Copia de seguridad

Puede visualizar la información sobre el estado actual de la Copia de seguridad, es decir, estadísticas de Copia de seguridad.

Para ver las estadísticas de Copia de seguridad,

abra el menú contextual en el nodo **Copia de seguridad** en el árbol de la Consola de la aplicación y seleccione **Estadísticas**. Se abre la ventana **Estadísticas de Copia de seguridad**.

La ventana **Estadísticas de Copia de seguridad** muestra información sobre el estado actual de Copia de seguridad (consulte la tabla siguiente).

Información sobre el estado actual de la Copia de seguridad

Campo	Descripción
Tamaño actual de Copia de seguridad	Cantidad de datos en la carpeta Copia de seguridad; la aplicación calcula el tamaño del archivo en forma cifrada
Número total de objetos	Cantidad total actual de objetos en la copia de seguridad

Bloqueo de acceso a los recursos de red. Sesiones en la red bloqueadas

En esta sección se describe cómo bloquear dispositivos remotos y configurar las opciones de la Lista de sesiones en la red bloqueadas.

Lista de sesiones de red bloqueadas

De manera predeterminada, la lista de sesiones en la red bloqueadas está disponible para su uso si alguno de los siguientes componentes está instalado: Protección de archivos en tiempo real, Protección contra amenazas de red. Estos componentes descubren intentos remotos de cifrar, abrir o ejecutar objetos en el dispositivo protegido o en las carpetas compartidas de almacenamiento conectado a la red de acuerdo con la lista de sesiones en la red bloqueadas. La información sobre las sesiones en la red bloqueadas de todos los dispositivos protegidos se envía a Kaspersky Security Center. Kaspersky Embedded Systems Security bloquea la sesión actual y, en términos de la sesión actual, provoca que las carpetas compartidas o las carpetas de almacenamiento conectadas a la red no estén disponibles.

La lista de sesiones en la red bloqueadas se completa cuando al menos una de las siguientes tareas se inicia en modo activo (en condiciones específicas):

- Para la tarea Protección de archivos en tiempo real: se detecta actividad maliciosa por parte de un dispositivo que accede a los recursos de archivos en red y, en la configuración de la tarea Protección de archivos en tiempo real, se ha activado la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa**.

- Para la tarea Protección contra amenazas de red: se detecta la actividad típica de los ataques de red.

Una vez que se detecta una actividad malintencionada o un intento de cifrado, la tarea envía información sobre la sesión en la red atacante a la lista de sesiones en la red bloqueadas y la aplicación crea un evento de *advertencia* para la sesión actual del host atacante. Se bloqueará cualquier intento de esta sesión de acceder a las carpetas de red compartidas protegidas.

Si el identificador único local (LUID) de un host que inició la sesión en la red atacante se agrega a la lista de sesiones en la red bloqueadas, Kaspersky Embedded Systems Security determina la dirección IP de este host y la agrega a la lista de sesiones en la red bloqueadas en lugar del LUID del host atacante.

De manera predeterminada, Kaspersky Embedded Systems Security elimina las sesiones en la red bloqueadas de la lista 30 minutos después de que se agregaron a la lista. El acceso a los recursos de archivos en red se restaura automáticamente después de que se eliminan las sesiones en la red de la lista de sesiones en la red bloqueadas. Puede especificar el periodo de tiempo después del cual las sesiones de red bloqueadas se desbloquean automáticamente.

Tenga en cuenta que cuando restringe el acceso a la administración de almacenamiento de cualquier cuenta de usuario, la lista de sesiones en la red seguirá estando disponible. La configuración de las sesiones en la red bloqueadas no se puede cambiar a menos que la cuenta de usuario seleccionada tenga **Permisos de edición** para administrar Kaspersky Embedded Systems Security.

Cómo administrar la lista de sesiones en la red bloqueadas a través del Complemento de administración

En esta sección, aprenderá a configurar las opciones de la lista de sesiones en la red bloqueadas a través de la interfaz del Complemento de administración.

Habilitar el bloqueo de hosts no confiables

Para agregar sesiones de red que muestren cualquier actividad maliciosa o de cifrado a la **Lista de sesiones en la red bloqueadas** y bloquear el acceso a los recursos de archivos en red, al menos una de las siguientes tareas debe ejecutarse en el modo activo:

- Protección de archivos en tiempo real
- Protección contra amenazas de red

Configure la tarea Protección de archivos en tiempo real:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Seleccione la pestaña **Directivas** y abra **<Nombre de la directiva>** > **Protección del equipo en tiempo real** > **Configuración** en el bloque **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección del equipo en tiempo real**.
3. En la sección **Integración con otros componentes**, seleccione la casilla **Listar hosts que muestren actividad maliciosa como no confiables** si desea que Kaspersky Embedded Systems Security para Windows bloquee el acceso a los recursos de archivos en red para hosts en los que se detecta actividad maliciosa mientras se ejecuta la tarea Protección de archivos en tiempo real.
4. Si la tarea no se ha iniciado, abra la pestaña **Administración de tareas**:
   a. Seleccione la casilla de verificación **Ejecutar según programación**.
   b. Seleccione la frecuencia de **Al inicio de la aplicación** en la lista desplegable.
5. En la ventana **Protección del equipo en tiempo real**, haga clic en **Aceptar**.

Se guardan las opciones configuradas recientemente.

Configure la tarea Protección contra amenazas de red

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección.
6. Haga clic en el botón **Configuración** en la subsección **Protección contra amenazas de red**.

   Se abre la ventana **Protección contra amenazas de red**.
7. Abra la pestaña **General**.
8. En la sección **Modo de procesamiento**, seleccione **Bloquear las conexiones al detectar un ataque** en el modo de procesamiento.

   La casilla de verificación habilita o deshabilita la adición de hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

   Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada y agrega las direcciones IP de los hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

   Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

   Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.

   Este modo está seleccionado en forma predeterminada.
9. Si la tarea no se ha iniciado, abra la pestaña **Administración de tareas**:
   a. Seleccione la casilla de verificación **Ejecutar según programación**.
   b. Seleccione la frecuencia de **Al inicio de la aplicación** en la lista desplegable.
10. En la ventana, haga clic en **Aceptar**.
11. Se guardan las opciones configuradas recientemente.

Configuración de las opciones de la lista de sesiones en la red bloqueadas

Para configurar la lista de sesiones en la red bloqueadas, realice lo siguiente:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Adicional**, haga clic en el botón **Configuración** de la subsección **Depósitos**.

   Se muestra la ventana de **Configuración de depósitos**.

5. En la sección **Plazos de bloqueo de la sesión de red** de la pestaña **Sesiones de red bloqueadas**, especifique la cantidad de días, horas y minutos que se dejarán transcurrir desde el momento del bloqueo hasta que las sesiones de red bloqueadas puedan acceder nuevamente a los recursos de archivos en red.

6. Haga clic en el botón **Aceptar**.

Cómo administrar la lista de sesiones en la red bloqueadas a través de la Consola de la aplicación

En esta sección, aprenderá a configurar las opciones de la Lista de sesiones en la red bloqueadas a través de la interfaz de la Consola de aplicaciones.

Habilitar el bloqueo de hosts no confiables

Para agregar sesiones de red que muestren cualquier actividad maliciosa o de cifrado a la **Lista de sesiones en la red bloqueadas** y bloquear el acceso a los recursos de archivos en red, al menos una de las siguientes tareas debe ejecutarse en el modo activo:

- Protección de archivos en tiempo real
- Protección contra amenazas de red

Configure la tarea Protección de archivos en tiempo real:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.

2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.

3. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Aparece la ventana **Configuración de tareas**.

4. En la sección **Profundo**, seleccione la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa** si desea que Kaspersky Embedded Systems Security bloquee las sesiones en la red en las que se detecta actividad maliciosa mientras se ejecuta la tarea Protección de archivos en tiempo real.

5. Si la tarea no se ha iniciado, abra la pestaña **Programación**:

a. Seleccione la casilla de verificación **Ejecutar según programación**.

b. Seleccione la frecuencia de **Al inicio de la aplicación** en la lista desplegable.

6. En la ventana **Configuración de tareas**, haga clic en **Aceptar**.

Se guardan las opciones configuradas recientemente.

Configure la tarea Protección contra amenazas de red

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario de **Protección contra amenazas de red**.
3. Haga clic en el vínculo **Protección contra amenazas de red**, en el panel de detalles del nodo **Propiedades**.
4. Aparece la ventana **Configuración de tareas**.
5. Abra la pestaña **General**.
6. En la sección **Modo de procesamiento**, seleccione **Bloquear las conexiones al detectar un ataque** en el modo de procesamiento.

   La casilla de verificación habilita o deshabilita la adición de hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

   Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada y agrega las direcciones IP de los hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

   Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

   Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.

   Este modo está seleccionado en forma predeterminada.

7. Seleccione o desactive la casilla de verificación **No detener el análisis de tráfico cuando la tarea no está en ejecución**.

   Si esta casilla está activada, incluso cuando la tarea Protección contra amenazas de red está detenida, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividades típicas de los ataques de red y bloquea la actividad de red de los equipos atacantes si así lo exige el modo seleccionado para la tarea.

   Si esta casilla está desactivada, cuando se detiene la tarea Protección contra amenazas de red, Kaspersky Embedded Systems Security para Windows deja de analizar el tráfico de red entrante en busca de actividades típicas de los ataques de red.

   De forma predeterminada, la casilla no está activada.

8. Si la tarea no se ha iniciado, abra la pestaña **Programación**:

   a. Seleccione la casilla de verificación **Ejecutar según programación**.

   b. Seleccione la frecuencia de **Al inicio de la aplicación** en la lista desplegable.

9. En la ventana **Configuración de tareas**, haga clic en **Aceptar**.

Se guardan las opciones configuradas recientemente.

Configuración de las opciones de la lista de sesiones en la red bloqueadas

Para configurar la lista de sesiones en la red bloqueadas, realice lo siguiente:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Abra el menú contextual del nodo secundario **Sesiones de red bloqueadas**.
3. Seleccione la opción del menú **Propiedades**.

   Se muestra la ventana **Configuración de la lista de sesiones de red bloqueadas**.
4. En la sección **Plazo de bloqueo de sesiones de red**, especifique la cantidad de días, horas y minutos que se dejarán transcurrir, desde el momento del bloqueo hasta que las sesiones de red bloqueadas puedan acceder nuevamente a los recursos de archivos en red.
5. Haga clic en el botón **Aceptar**.
6. Para restaurar el acceso para todas las sesiones de red bloqueadas:
   a. Abra el menú contextual del nodo secundario **Sesiones de red bloqueadas**.
   b. Seleccione la opción **Desbloquear todo**.

      Se eliminarán y desbloquearán todas las sesiones en la red.
7. Para eliminar varias sesiones de la lista de sesiones de red bloqueadas:
   a. En la lista de sesiones en la red bloqueadas, que se muestra en el panel de resultados, seleccione una o más sesiones.
   b. Abra el menú contextual del nodo secundario **Sesiones de red bloqueadas**.
   c. Seleccione la opción **Desbloquear seleccionado**.

      Las sesiones en la red seleccionadas se desbloquean.

Cómo administrar la lista de sesiones en la red bloqueadas a través del Complemento web

En esta sección, aprenderá cómo configurar la lista de sesiones en la red bloqueadas mediante la interfaz del Complemento web.

Cómo habilitar el bloqueo de sesiones en la red

Para agregar sesiones en la red que muestren cualquier actividad maliciosa o de cifrado a la **Sesiones de red bloqueadas** y bloquear el acceso a los recursos de archivos en red para esas sesiones, al menos una de las siguientes tareas debe ejecutarse en el modo activo:

- Protección de archivos en tiempo real
- Protección contra amenazas de red

Configure la tarea Protección de archivos en tiempo real:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Protección del equipo en tiempo real**.
5. Haga clic en **Configuración** en la subsección **Protección de archivos en tiempo real**.
6. En la sección **Integración con otros componentes**, seleccione la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa** si desea que Kaspersky Embedded Systems Security bloquee la sesión actual y haga que los recursos compartidos de red no estén disponibles para las sesiones en la red hacia las cuales se detectó la actividad maliciosa.
7. Si la tarea no se ha iniciado, abra la pestaña **Administración de tareas**:
   a. Seleccione la casilla de verificación **Ejecutar según programación**.
   b. Seleccione la frecuencia de **Al inicio de la aplicación** en la lista desplegable.
8. Haga clic en el botón **Guardar**.

Se guardan las opciones configuradas recientemente.

Configuración de las opciones de la lista de sesiones en la red bloqueadas

Para configurar la lista de sesiones en la red bloqueadas, realice lo siguiente:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Adicional**.
5. Haga clic en el botón **Configuración** de la subsección **Depósitos**.
6. En la sección **Adicional**, haga clic en el botón **Configuración** de la subsección **Depósitos**.
   Se muestra la ventana **Depósitos**.
7. En la sección **Plazo de bloqueo de sesiones de red** de la pestaña **Sesiones de red bloqueadas**, especifique la cantidad de días, horas y minutos que se dejarán transcurrir desde el momento del bloqueo hasta que las

sesiones de red bloqueadas puedan acceder nuevamente a los recursos de archivos en red.

8. Haga clic en el botón **Aceptar**.

Registro de eventos. Registros de Kaspersky Embedded Systems Security para Windows

Esta sección proporciona información sobre cómo trabajar con los registros de Kaspersky Embedded Systems Security.

Modos de registrar eventos de Kaspersky Embedded Systems Security para Windows

Los eventos de Kaspersky Embedded Systems Security para Windows se dividen en dos grupos:

- Eventos relacionados con el procesamiento de objetos en las tareas de Kaspersky Embedded Systems Security para Windows.
- Eventos relacionados con la administración de Kaspersky Embedded Systems Security para Windows, como el inicio de la aplicación, la creación o la eliminación de tareas, o la edición de la configuración de tareas.

Kaspersky Embedded Systems Security para Windows utiliza los siguientes métodos para registrar eventos:

- **Registros de tareas**. Un registro de tareas contiene información sobre el estado actual de las tareas y los eventos que ocurrieron durante la ejecución de tareas.
- **Registro de auditoría del sistema**. El registro de auditoría del sistema contiene información sobre los eventos relacionados con la administración de Kaspersky Embedded Systems Security para Windows.
- **Registro de eventos**. El registro de eventos contiene información sobre los eventos requeridos para diagnosticar fallas en el funcionamiento de Kaspersky Embedded Systems Security para Windows. El registro de eventos está disponible en el Visor de eventos de Microsoft Windows.
- **Registro de seguridad**. El registro de seguridad contiene información sobre eventos asociados con la violación de la seguridad o intentaron hacerlo en el dispositivo protegido.

Si ocurre un problema durante el funcionamiento de Kaspersky Embedded Systems Security para Windows (por ejemplo, Kaspersky Embedded Systems Security para Windows o una tarea individual se interrumpe de manera anormal o no se inicia), puede crear un archivo de rastreo y uno de volcado de los procesos de Kaspersky Embedded Systems Security para Windows y enviar los archivos con esta información al soporte técnico de Kaspersky para su análisis, con el fin de diagnosticar el problema.

Kaspersky Embedded Systems Security para Windows no envía ningún archivo de volcado o rastreo automáticamente. Solo el usuario que posea los permisos requeridos podrá enviar datos de diagnóstico.

Kaspersky Embedded Systems Security para Windows escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security para Windows. Puede configurar los permisos de acceso y permitir que solo los usuarios necesarios puedan acceder a los registros, los archivos de rastreo y los archivos de volcado.

Los archivos que se pueden descargar mediante los siguientes vínculos contienen tablas con las listas completas de los eventos de Kaspersky Embedded Systems Security para Windows de las siguientes categorías:

- Eventos que Kaspersky Embedded Systems Security para Windows escribe en el registro de eventos.

  DESCARGAR KESS-WEL-EVENTS.ZIP

- Eventos que Kaspersky Embedded Systems Security para Windows envía al Servidor de administración.

  DESCARGAR KESS-KSC-EVENTS.ZIP

Registro de auditoría del sistema

Kaspersky Embedded Systems Security para Windows realiza una auditoría del sistema de los eventos relacionados con la administración de Kaspersky Embedded Systems Security para Windows. La aplicación registra información sobre el inicio de la aplicación, los inicios y las detenciones de las tareas de Kaspersky Embedded Systems Security, los cambios en la configuración de tareas y la creación y eliminación de las tareas Análisis a pedido. Los registros de todos esos eventos se muestran en el panel de resultados cuando se selecciona el nodo **Registro de auditoría del sistema** en la Consola de la aplicación.

De manera predeterminada, Kaspersky Embedded Systems Security para Windows almacena registros en el registro de auditoría del sistema durante un periodo indeterminado. Puede especificar el periodo de almacenamiento para los registros del registro de auditoría del sistema.

Puede especificar una carpeta que Kaspersky Embedded Systems Security para Windows usará para almacenar los archivos que contienen el registro de auditoría del sistema que no sea la predeterminada.

Cómo ordenar eventos en el registro de auditoría del sistema

De manera predeterminada, los eventos en el nodo registro de auditoría del sistema se muestran en orden cronológico inverso.

Los eventos se pueden ordenar por los contenidos de cualquier columna, excepto la columna **Evento**.

Para ordenar eventos en el registro de auditoría del sistema:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el nodo secundario **Registro de auditoría del sistema**.
3. En el panel de resultados, seleccione el encabezado de la columna que desee usar para ordenar los eventos en la lista.

Los resultados ordenados se guardarán hasta que visualice de nuevo el registro de auditoría del sistema.

Filtrado de eventos en el registro de auditoría del sistema

Puede configurar el registro de auditoría del sistema para que muestre solo los registros de eventos que cumplen con las condiciones de filtrado (filtros) que ha especificado.

Para filtrar eventos en el registro de auditoría del sistema:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registro de auditoría del sistema** y seleccione **Filtrar**.

   Se abre la ventana **Configuración de filtro**.
3. Para agregar un filtro, siga estos pasos:

   a. En la lista **Nombre del campo**, seleccione la columna que desee usar para filtrar los eventos.

   b. En la lista **Operador**, seleccione la condición de filtrado. Las condiciones de filtrado varían según el elemento seleccionado en la lista **Nombre del campo**.

   c. En **Valor del campo**, seleccione un valor para el filtro.

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

   El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**.
4. Si es necesario, realice una de las siguientes acciones:

   - Para combinar varios filtros mediante el operador lógico "AND", seleccione **Si se cumplen todas las condiciones**.
   - Para combinar varios filtros mediante el operador lógico "OR", seleccione **Si se cumple alguna condición**.
5. Haga clic en el botón **Aplicar** para guardar las condiciones de filtrado en el registro de auditoría del sistema.

   La lista de eventos del registro de auditoría del sistema muestra solo los eventos que cumplen las condiciones de filtrado. Los resultados filtrados se guardarán hasta que visualice de nuevo el registro de auditoría del sistema.

Para deshabilitar el filtro:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registro de auditoría del sistema** y seleccione **Eliminar filtro**.

   La lista de eventos del registro de auditoría del sistema mostrará todos los eventos.

Eliminar eventos del registro de auditoría del sistema

De manera predeterminada, Kaspersky Embedded Systems Security para Windows almacena registros en el registro de auditoría del sistema durante un periodo indeterminado. Puede especificar el periodo de almacenamiento para los registros del registro de auditoría del sistema.

Se pueden eliminar manualmente todos los eventos del registro de auditoría del sistema.

Para eliminar eventos del registro de auditoría del sistema:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registro de auditoría del sistema** y seleccione **Eliminar**.
3. Realice una de las siguientes opciones:

- Si desea guardar el contenido del registro en un archivo de formato CSV o TXT antes de eliminar los eventos del registro de auditoría del sistema, haga clic en el botón **Sí** en la ventana en la que se le solicita confirmar la eliminación. En la ventana que se abre, especifique el nombre y la ubicación del archivo.

- Si no desea guardar el contenido del registro en un archivo, haga clic en el botón **No** en la ventana en la que se le solicita confirmar la eliminación.

Se borrará el registro de auditoría del sistema.

Registros de tareas

Esta sección proporciona información sobre los registros de tareas de Kaspersky Embedded Systems Security para Windows e instrucciones sobre cómo administrarlos.

Acerca de los registros de tareas

La información sobre la ejecución de las tareas de Kaspersky Embedded Systems Security para Windows se muestra en el panel de resultados cuando se selecciona el nodo **Registros de tareas** en la Consola de la aplicación.

En el registro de cada tarea, puede ver las estadísticas de ejecución de tareas, los detalles de cada uno de los objetos que la aplicación ha procesado desde el inicio de la tarea y la configuración de esta.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows almacena registros de tareas durante 30 días después de que la tarea se realice. Se puede cambiar el periodo de almacenamiento para los eventos del registro de tarea.

Puede especificar una carpeta diferente de la predeterminada para que Kaspersky Embedded Systems Security para Windows almacene los archivos que contienen los registros de tareas. También puede seleccionar los eventos que Kaspersky Embedded Systems Security para Windows asentará en los registros de tareas.

Visualización de la lista de eventos en los registros de tarea

Para visualizar los registros de tareas:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.

2. Seleccione el subnodo **Registros de tareas**.

   La lista de eventos guardados en los registros de tareas de Kaspersky Embedded Systems Security para Windows se mostrará en el panel de resultados.

Los eventos se pueden ordenar por cualquier columna o filtrar.

Cómo ordenar los registros de tareas

De manera predeterminada, los registros de tareas se muestran en orden cronológico inverso. Se pueden ordenar por cualquier columna.

Para ordenar los registros de tareas:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. En el panel de resultados, seleccione el encabezado de la columna que desee usar para ordenar los registros de tareas de Kaspersky Embedded Systems Security para Windows.

Los resultados ordenados se guardarán hasta que visualice de nuevo los registros de tareas.

Cómo filtrar los registros de tareas

Puede configurar la lista de registros de tareas para que muestren únicamente los registros de tareas que cumplan con las condiciones de filtrado (filtros) que especificó.

Para filtrar los registros de tareas:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registros de tareas** y seleccione **Filtrar**.

   Se abre la ventana **Configuración de filtro**.
3. Para agregar un filtro, siga estos pasos:
   a. En la lista **Nombre del campo**, seleccione la columna que desea usar para filtrar los registros de tareas.
   b. En la lista **Operador**, seleccione la condición de filtrado. Las condiciones de filtrado varían según el elemento seleccionado en la lista **Nombre del campo**.
   c. En **Valor del campo**, seleccione un valor para el filtro.
   d. Haga clic en el botón **Agregar**.

   El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**.
4. Si es necesario, realice una de las siguientes acciones:
   - Para combinar varios filtros mediante el operador lógico "AND", seleccione **Si se cumplen todas las condiciones**.
   - Para combinar varios filtros mediante el operador lógico "OR", seleccione **Si se cumple alguna condición**.
5. Haga clic en el botón **Aplicar** para guardar las condiciones de filtrado en la lista de registros de tarea.

La lista de registros de tareas muestra solo los registros de tareas que cumplen con las condiciones de filtrado. Los resultados filtrados se guardarán hasta que visualice de nuevo los registros de tareas.

Para deshabilitar el filtro:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registros de tareas** y seleccione **Eliminar filtro**.

En consecuencia, la lista de registros de tareas mostrará todos los registros de tareas.

Visualización de las estadísticas y la información acerca de una tarea de Kaspersky Embedded Systems Security para Windows en los registros de tareas

En los registros de tareas, puede ver información detallada sobre todos los eventos que han ocurrido en las tareas desde que iniciaron, así como las estadísticas de ejecución de las tareas y la configuración de las tareas.

Para ver las estadísticas y la información acerca de una tarea de Kaspersky Embedded Systems Security para Windows:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. En el panel de detalles, utilice uno de estos métodos para abrir la ventana **Registros**:
   - Haga doble clic en el registro de tareas que desea configurar.
   - Abra el menú contextual del registro de tareas que desea ver y seleccione **Ver registro**.
4. En la ventana que se abre, se muestra la siguiente información:
   - La pestaña **Estadísticas** muestra la hora de inicio y finalización de la tarea, así como las estadísticas de la tarea.
   - La pestaña **Eventos** muestra una lista de los eventos registrados durante la ejecución de la tarea.
   - La pestaña **Opciones** muestra la configuración de la tarea.
5. Si es necesario, haga clic en el botón **Filtrar** para filtrar los eventos en el registro de tareas.
6. Si es necesario, haga clic en el botón **Exportar** para exportar los datos desde el registro de tareas a un archivo con formato TXT o CSV.
7. Haga clic en el botón **Cerrar**.

Se cerrará la ventana **Registros**.

Exportación de la información desde un registro de tareas

Puede exportar los datos de un registro de tareas a un archivo con formato TXT o CSV.

Para exportar datos desde un registro de tareas:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. En el panel de detalles, utilice uno de estos métodos para abrir la ventana **Registros**:
   - Haga doble clic en el registro de tareas que desea configurar.

- Abra el menú contextual del registro de tareas que desea ver y seleccione **Ver registro**.

4. En la parte inferior de la ventana **Registros**, haga clic en el botón **Exportar**.

   Se abre la ventana **Guardar como**.

5. Especifique el nombre, la ubicación, el tipo y la codificación del archivo al que desea exportar los datos del registro de tareas.

6. Haga clic en el botón **Guardar**.

Se guarda la configuración especificada.

Cómo eliminar los registros de tareas

De forma predeterminada, Kaspersky Embedded Systems Security para Windows almacena registros de tareas durante 30 días después de que la tarea se realice. Se puede cambiar el periodo de almacenamiento para los eventos del registro de tarea.

Puede eliminar manualmente los registros de tareas que ya están completos.

No se eliminarán los eventos de los registros de tareas que se están ejecutando ni las tareas que están utilizando otros usuarios.

Para eliminar los registros de tareas:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.

2. Seleccione el subnodo **Registros de tareas**.

3. Realice una de las siguientes opciones:

   - Si desea eliminar los registros de todas las tareas que ya están completas, abra el menú contextual del nodo secundario **Registros de tareas** y seleccione **Eliminar**.

   - Si desea borrar el registro de una tarea individual, en el panel de resultados, abra el menú contextual del registro de tareas que desea eliminar y seleccione **Eliminar**.

   - Si desea borrar los registros de varias tareas:

     a. En el panel de resultados, use la tecla **Ctrl** o **Mayús** para seleccionar los registros de tareas que desee borrar.

     b. Abra el menú contextual de cualquier registro de tareas seleccionado y seleccione **Eliminar**.

4. Haga clic en el botón **Sí** de la ventana de confirmación de eliminación para confirmar que desea eliminar los registros.

Se borrarán los registros de las tareas que seleccionó. La eliminación de los registros de tareas se incluirá en el registro de auditoría del sistema.

Registro de seguridad

Kaspersky Embedded Systems Security para Windows mantiene un registro de eventos asociados con la violación de la seguridad o los intentos de violación de la seguridad en el dispositivo protegido. Los siguientes eventos se incluyen en este registro:

- Eventos de Prevención de exploits.
- Eventos de inspección de registros críticos.
- Los eventos críticos que indican un intento de infracción de la seguridad (para la Protección del equipo en tiempo real, el Análisis a pedido, el Monitor de integridad de archivos, el Control de inicio de aplicaciones y las tareas de Control de dispositivos).

Puede borrar el registro de seguridad. Además, Kaspersky Embedded Systems Security para Windows registra un evento de auditoría del sistema cuando se elimina el registro de seguridad.

Ver el registro de eventos de Kaspersky Embedded Systems Security para Windows en el Visor de eventos

Puede ver el registro del evento de Kaspersky Embedded Systems Security para Windows con el complemento Visor de eventos de Microsoft Windows para Microsoft Management Console. El registro contiene eventos registrados por Kaspersky Embedded Systems Security para Windows que son necesarios para diagnosticar las fallas de su funcionamiento.

Se pueden seleccionar los eventos que se registrarán en el registro de eventos en función de los siguientes criterios:

- **por tipos de evento**.
- **por nivel de detalle**. El nivel de detalle corresponde al nivel de importancia de los eventos registrados en el registro (eventos informativos, importantes o críticos). El Nivel informativo es el más detallado y registra todos los eventos. El Nivel Crítico es el menos detallado y solo registra los eventos críticos.

Para consultar el registro del evento de Kaspersky Embedded Systems Security para Windows:

1. Haga clic en el botón **Iniciar**, introduzca el comando `mmc` en la barra de búsqueda y presione **INTRO**.

   Se abre Microsoft Management Console.

2. Seleccione **Archivo** > **Agregar o eliminar complemento**.

   Se abre la ventana **Agregar o eliminar complementos**.

3. En la lista de complementos disponibles, seleccione el complemento **Visor de eventos** y haga clic en el botón **Agregar**.

   Se abre la ventana **Seleccionar equipo**.

4. En la ventana **Seleccionar equipo**, especifique el dispositivo protegido en el cual Kaspersky Embedded Systems Security para Windows está instalado y haga clic en **Aceptar**.

5. En la ventana **Agregar y eliminar complementos**, haga clic en **Aceptar**.

   En el árbol de Microsoft Management Console, aparece el nodo **Visor de eventos**.

6. Expanda el nodo **Visor de eventos** y seleccione el nodo secundario **Registros de aplicaciones y servicios** > **Kaspersky Embedded Systems Security para Windows**.

Se abre el registro del evento de Kaspersky Embedded Systems Security para Windows.

Configuración de las opciones de registro a través de la Consola de la aplicación

Puede editar la siguiente configuración de registros de Kaspersky Embedded Systems Security para Windows:

- Duración del periodo de almacenamiento para los eventos en los registros de tarea y el registro de auditoría del sistema.
- Ubicación de la carpeta en la que Kaspersky Embedded Systems Security para Windows almacena archivos del registro de tareas y el archivo de registro de auditoría del sistema.
- Umbrales de generación de los eventos para *Las bases de datos de la aplicación están desactualizadas*, *Las bases de datos de la aplicación son obsoletas* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.
- Eventos que Kaspersky Embedded Systems Security para Windows guarda en los registros de tareas, el registro de auditoría del sistema y el registro de eventos de Kaspersky Embedded Systems Security para Windows en el Visor de eventos.
- Ajustes para publicar eventos de auditoría y eventos de desempeño de la tarea en el servidor syslog a través del protocolo de syslog.

Para configurar las opciones de registro a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones** y seleccione **Propiedades**.

   Se abre la ventana **Configuración de registros y notificaciones**.

2. En la pestaña **General**, de ser necesario, seleccione los eventos que Kaspersky Embedded Systems Security para Windows guardará en los registros de tareas, en el registro de auditoría del sistema y en el registro de eventos de Kaspersky Embedded Systems Security para Windows disponible en el Visor de eventos:

   a. En la lista **Componente**, seleccione el componente de Kaspersky Embedded Systems Security para Windows para el cual desea configurar el nivel de detalle.

   b. En la lista **Nivel de importancia**, seleccione un nivel de detalle para los eventos en los registros de tareas, el registro de auditoría del sistema y el registro del evento para el componente seleccionado.

      En la siguiente tabla con una lista de eventos, las casillas están seleccionadas junto a los eventos que están registrados en registros de tareas, el registro de auditoría del sistema y el registro del evento, de acuerdo con el nivel de detalle actual.

   c. Si desea habilitar manualmente el registro de eventos específicos para un componente o una tarea seleccionados:

      1. En la lista **Nivel de importancia**, seleccione **Personalizado**.

      2. En la tabla con la lista de eventos, las casillas están seleccionadas junto a los eventos que desea que se registren en los registros de tarea, el registro de auditoría del sistema y el registro del evento.

3. En la pestañaAvanzado**Avanzado**, configure las opciones de almacenamiento de registros y umbrales de generación de eventos para el estado de protección del dispositivo:

- En el bloque **Almacenamiento de registros**:
  - **Carpeta de registros**
  - **Eliminar registros de tareas anteriores a (días)**
  - **Eliminar del registro de auditoría del sistema los eventos anteriores a (días)**
- En el bloque **Umbrales de generación de eventos**, indique el número de días después de los cuales ocurrirán los eventos *Las bases de datos de la aplicación están desactualizadas*, *Las bases de datos de la aplicación son obsoletas* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.

4. En la pestaña **Integración de SIEM**, configure los ajustes para publicar eventos de auditoría y eventos de desempeño de la tarea en el servidor syslog.
5. Haga clic en el botón **Aceptar** para guardar los cambios.

Acerca de la integración de SIEM

Para reducir la carga en dispositivos de rendimiento reducido y reducir el riesgo de la degradación del sistema como consecuencia del aumento en los tamaños de registros de la aplicación, puede configurar la publicación de eventos de auditoría y eventos de rendimiento de la tarea en el *servidor syslog* mediante el protocolo Syslog.

Un servidor syslog es un servidor externo para agregar eventos (SIEM). Almacena y analiza los eventos recibidos y realiza otras acciones de administración de registros.

Puede usar la integración de SIEM en dos modos:

- Duplicar eventos en el servidor syslog: en este modo, todos los eventos de rendimiento de la tarea cuya publicación se establece en la configuración de registros, así como todos los eventos de auditoría del sistema, continúan almacenándose en el dispositivo protegido hasta después de que se envían al servidor SIEM.

  Recomendamos utilizar este modo para reducir todo lo posible la carga en el dispositivo protegido.

- Eliminar copias locales de eventos: en este modo, todos los eventos que se registran durante el funcionamiento de la aplicación y se publican en el servidor SIEM se eliminan del dispositivo protegido.

  La aplicación nunca elimina las versiones locales del registro de seguridad.

Kaspersky Embedded Systems Security para Windows puede convertir eventos en los registros de la aplicación a formatos admitidos por el servidor syslog, de modo que dichos eventos se puedan transmitir y sean reconocidos de manera exitosa por el servidor SIEM. La aplicación admite la conversión al formato de datos estructurado y al formato JSON.

Recomendamos seleccionar el formato de eventos basados en la configuración del servidor SIEM utilizado.

Configuración de confiabilidad

Para reducir el riesgo de retransmisiones no exitosas de eventos al servidor SIEM, puede definir la configuración para realizar una conexión con un servidor syslog idéntico.

El servidor syslog idéntico es un servidor syslog adicional al cual la aplicación cambia automáticamente si la conexión con el servidor syslog principal no está disponible o si el servidor principal no se puede utilizar.

Kaspersky Embedded Systems Security para Windows también utiliza eventos de auditoría del sistema para notificarle sobre intentos fallidos de conexión al servidor SIEM y sobre errores al enviar eventos al servidor SIEM.

Configuración de las opciones de integración de SIEM

De forma predeterminada, la integración de SIEM no se usa. Puede habilitar y deshabilitar la integración de SIEM y configurar las opciones correspondientes (consulte la tabla a continuación).

Configuración de integración de SIEM

Configuración	Valor predeterminado	Descripción
Enviar eventos a un servidor remoto de Syslog, mediante el protocolo Syslog	No aplicado	Puede habilitar o deshabilitar la integración de SIEM al seleccionar o al desactivar la casilla, respectivamente.
Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog	No aplicado	Puede ajustar la configuración para almacenar copias locales de registros después de que se envíen al servidor SIEM al seleccionar o al desactivar la casilla.
Formato de los eventos	Datos estructurados	Puede seleccionar uno de dos formatos a los cuales la aplicación convierte sus eventos antes de enviarlos al servidor syslog para el mejor reconocimiento de estos eventos por el servidor SIEM.
Protocolo de conexión	TCP	Puede usar la lista desplegable para configurar la conexión con los servidores syslog principal e idéntico mediante protocolos de TCP o UDP.
Configuración de conexión al servidor syslog principal	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor syslog principal. Puede especificar la dirección IP solo en el formato IPv4.
Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal	No aplicado	Puede usar la casilla para habilitar o deshabilitar el uso de un servidor syslog idéntico.
Configuración de conexión al servidor syslog idéntico	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor reflejado de Syslog. Puede especificar la dirección IP solo en el formato IPv4.

Para configurar los ajustes para la integración con SIEM:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones**.
2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de registros y notificaciones**.
3. Seleccione la pestaña **Integración de SIEM**.
4. En el bloque **Ajustes de integración**, active la casilla Enviar eventos a un servidor remoto de Syslog, mediante el protocolo Syslog.

5. Si es necesario, en el bloque **Ajustes de integración**, active la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog**.

   El estado de la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog** no afecta la configuración para almacenar eventos del registro de seguridad: la aplicación nunca elimina automáticamente eventos del registro de seguridad.

6. En el bloque **Formato de los eventos**, especifique el formato al cual desee convertir los eventos de la aplicación de modo que se puedan enviar al servidor SIEM.

   De forma predeterminada, la aplicación los convierte en un formato de datos estructurado.

7. En el bloque **Configuración de conexión**:

   - Especifique el protocolo de conexión de SIEM.
   - En los campos del mismo nombre, especifique la dirección IPv4 y el puerto que se usarán para conectarse al servidor syslog principal.
   - Seleccione la casilla **Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal** si desea que la aplicación use otra configuración de conexión cuando sea incapaz de enviar eventos al servidor syslog principal.
   - En los campos del mismo nombre, especifique la dirección IPv4 y el puerto que se usarán para conectarse a un servidor syslog adicional.

8. Haga clic en el botón **Aceptar**.

   La configuración de integración de SIEM establecida se aplicará.

Configuración de las opciones de registros y notificaciones a través del Complemento de administración

La Consola de administración de Kaspersky Security Center puede usarse para configurar las notificaciones para el administrador y los usuarios sobre los siguientes eventos del funcionamiento de Kaspersky Embedded Systems Security y el estado de la protección antivirus en el dispositivo:

- El administrador puede recibir información sobre eventos de tipos seleccionados.
- Los usuarios de la LAN que tienen acceso al dispositivo protegido y los usuarios del dispositivo protegido de terminales pueden recibir información sobre eventos de *Objeto detectado*.

Las notificaciones sobre eventos Kaspersky Embedded Systems Security para Windows se pueden configurar para un solo dispositivo protegido a través de la ventana **Propiedades: <Nombre del dispositivo protegido>** del dispositivo protegido seleccionado, o para un grupo de dispositivos protegidos en la ventana **Propiedades: <Nombre de la directiva>** del grupo de administración seleccionado.

En la pestaña **Notificaciones de eventos** o en la ventana **Configuración de notificaciones**, puede configurar los siguientes tipos de notificaciones:

- Las notificaciones para el administrador sobre eventos de tipos seleccionados pueden configurarse mediante la pestaña **Notificaciones de eventos** (la pestaña estándar en Kaspersky Security Center). Para obtener más información sobre los métodos de notificación, consulte la *Ayuda de Kaspersky Security Center*.

- Las notificaciones para el administrador y para los usuarios se pueden configurar en la ventana **Configuración de notificaciones**.

Puede configurar notificaciones para algunos tipos de eventos solo en la ventana o en la pestaña; y puede usar tanto la ventana como la pestaña para configurar notificaciones para otros tipos de eventos.

Si configura las notificaciones sobre eventos del mismo tipo usando el mismo modo en la pestaña **Notificaciones de eventos** y en la ventana **Configuración de notificaciones**, el administrador del sistema recibirá las notificaciones de esos eventos dos veces, pero en el mismo modo.

Configuración de las opciones de registros de tareas

Para configurar los registros de Kaspersky Embedded Systems Security para Windows, realice los siguientes pasos:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de los registros para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar la aplicación para un único dispositivo protegido, seleccione la pestaña **Dispositivos** y abra los ajustes de la aplicación.
4. En la sección **Registros y notificaciones**, haga clic en el botón **Configuración** en el bloque **Registros de tareas**.
5. Se abre la ventana **Configuración de registros**, en la pestaña **Registros**.
6. Configure el nivel de detalle de los eventos en los registros:
   a. En la lista **Componente**, seleccione el componente de Kaspersky Embedded Systems Security para Windows para el cual desea configurar el nivel de detalle.
   b. En la lista **Nivel de importancia**, seleccione un nivel de detalle para los eventos en los registros de tareas, el registro de auditoría del sistema y el registro del evento para el componente seleccionado.
      En la siguiente tabla con una lista de eventos, las casillas están seleccionadas junto a los eventos que están registrados en registros de tareas, el registro de auditoría del sistema y el registro del evento, de acuerdo con el nivel de detalle actual.
   c. Si desea habilitar manualmente el registro de eventos específicos para un componente o una tarea seleccionados:
      1. En la lista **Nivel de importancia**, seleccione **Personalizado**.
      2. En la tabla con la lista de eventos, las casillas están seleccionadas junto a los eventos que desea que se registren en los registros de tarea, el registro de auditoría del sistema y el registro del evento.
7. En el bloque **Almacenamiento de registros**, configure los ajustes de almacenamiento de registros:

- **Carpeta de registros**
- **Eliminar registros de tareas anteriores a (días)**
- **Eliminar del registro de auditoría del sistema los eventos anteriores a (días)**

8. En la pestaña **Integración de SIEM**, configure los ajustes para publicar eventos de auditoría y eventos de desempeño de la tarea en el servidor syslog.
9. Haga clic en el botón **Aceptar**.

Los parámetros de registro configurados se guardaron.

Registro de seguridad

Kaspersky Embedded Systems Security para Windows mantiene un registro de eventos asociados con la violación de la seguridad o los intentos de violación de la seguridad en el dispositivo protegido. Los siguientes eventos se incluyen en este registro:

- Eventos de Prevención de exploits.
- Eventos de inspección de registros críticos.
- Los eventos críticos que indican un intento de infracción de la seguridad (para la Protección del equipo en tiempo real, el Análisis a pedido, el Monitor de integridad de archivos, el Control de inicio de aplicaciones y las tareas de Control de dispositivos).

Puede borrar el registro de seguridad. Además, Kaspersky Embedded Systems Security para Windows registra un evento de auditoría del sistema cuando se elimina el registro de seguridad.

Configuración de las opciones de integración de SIEM

Para reducir la carga en dispositivos de rendimiento reducido y reducir el riesgo de la degradación del sistema como consecuencia del aumento en los tamaños de registros de la aplicación, puede configurar la publicación de eventos de auditoría y eventos de rendimiento de la tarea en el *servidor syslog* mediante el protocolo Syslog.

Un servidor syslog es un servidor externo para agregar eventos (SIEM). Almacena y analiza los eventos recibidos y realiza otras acciones de administración de registros.

Puede usar la integración de SIEM en dos modos:

- Duplicar eventos en el servidor syslog: en este modo, todos los eventos de rendimiento de la tarea cuya publicación se establece en la configuración de registros, así como todos los eventos de auditoría del sistema, continúan almacenándose en el dispositivo protegido hasta después de que se envían al servidor SIEM.

  Recomendamos utilizar este modo para reducir todo lo posible la carga en el dispositivo protegido.

- Eliminar copias locales de eventos: en este modo, todos los eventos que se registran durante el funcionamiento de la aplicación y se publican en el servidor SIEM se eliminan del dispositivo protegido.

  La aplicación nunca elimina las versiones locales del registro de seguridad.

Kaspersky Embedded Systems Security para Windows puede convertir eventos en los registros de la aplicación a formatos admitidos por el servidor syslog, de modo que dichos eventos se puedan transmitir y sean reconocidos de manera exitosa por el servidor SIEM. La aplicación admite la conversión al formato de datos estructurado y al formato JSON.

Para reducir el riesgo de retransmisiones no exitosas de eventos al servidor SIEM, puede definir la configuración para realizar una conexión con un servidor syslog idéntico.

El servidor syslog idéntico es un servidor syslog adicional al cual la aplicación cambia automáticamente si la conexión con el servidor syslog principal no está disponible o si el servidor principal no se puede utilizar.

De forma predeterminada, la integración de SIEM no se usa. Puede habilitar y deshabilitar la integración de SIEM y configurar las opciones correspondientes (consulte la tabla a continuación).

Configuración de integración de SIEM

Configuración	Valor predeterminado	Descripción
Enviar eventos a un servidor remoto de Syslog, mediante el protocolo Syslog	No aplicado	Puede habilitar o deshabilitar la integración de SIEM al seleccionar o al desactivar la casilla, respectivamente.
Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog	No aplicado	Puede ajustar la configuración para almacenar copias locales de registros después de que se envíen al servidor SIEM al seleccionar o al desactivar la casilla.
Formato de los eventos	Datos estructurados	Puede seleccionar uno de dos formatos a los cuales la aplicación convierte sus eventos antes de enviarlos al servidor syslog para el mejor reconocimiento de estos eventos por el servidor SIEM.
Protocolo de conexión	TCP	Puede usar la lista desplegable para configurar la conexión con el servidor syslog principal mediante los protocolos TCP o UDP y con el servidor syslog idéntico mediante el protocolo TCP.
Configuración de conexión al servidor syslog principal	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor syslog principal. Puede especificar la dirección IP solo en el formato IPv4.
Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal	No aplicado	Puede usar la casilla para habilitar o deshabilitar el uso de un servidor syslog idéntico.
Configuración de conexión al servidor syslog idéntico	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor reflejado de Syslog. Puede especificar la dirección IP solo en el formato IPv4.

Para configurar los ajustes para la integración con SIEM:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

- Para establecer la configuración de los registros para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
- Para configurar la aplicación para un único dispositivo protegido, seleccione la pestaña **Dispositivos** y abra los ajustes de la aplicación.

4. En la sección **Registros y notificaciones**, haga clic en el botón **Registros de tareas** en el bloque **Configuración**.

   Se abre la ventana **Configuración de registros y notificaciones**.

5. Seleccione la pestaña **Integración de SIEM**.
6. En el bloque **Ajustes de integración**, active la casilla **Enviar eventos a un servidor remoto de Syslog, mediante el protocolo Syslog**.
7. Si es necesario, en el bloque **Ajustes de integración**, active la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog**.

   El estado de la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog** no afecta la configuración para almacenar eventos del registro de seguridad: la aplicación nunca elimina automáticamente eventos del registro de seguridad.

8. En el bloque **Formato de los eventos**, especifique el formato al cual desee convertir los eventos de la aplicación de modo que se puedan enviar al servidor SIEM.

   De forma predeterminada, la aplicación los convierte en un formato de datos estructurado.

9. En el bloque **Configuración de conexión**:
   - Especifique el protocolo de conexión de SIEM.
   - En los campos del mismo nombre, especifique la dirección IPv4 y el puerto que se usarán para conectarse al servidor syslog principal.
   - Seleccione la casilla **Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal** si desea que la aplicación use otra configuración de conexión cuando sea incapaz de enviar eventos al servidor syslog principal.
   - En los campos del mismo nombre, especifique la dirección IPv4 y el puerto que se usarán para conectarse a un servidor syslog adicional.
10. Haga clic en el botón **Aceptar**.

La configuración de integración de SIEM establecida se aplicará.

Configuración de las opciones de notificación

Para configurar las notificaciones de Kaspersky Embedded Systems Security para Windows:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Registros y notificaciones**, haga clic en el botón **Notificaciones de eventos** en la subsección **Configuración**.

5. En la ventana **Configuración de notificaciones**, defina la siguiente configuración de Kaspersky Embedded Systems Security para Windows según sus requisitos:

   - En la lista **Configuración de notificaciones**, seleccione el tipo de notificación cuya configuración desee establecer.

   - En la sección **Notificar a los usuarios**, configure el método de notificación a los usuarios. Si es necesario, escriba el texto del mensaje de notificación.

   - En la sección **Notificar a los administradores**, configure el método de notificación al administrador. Si es necesario, escriba el texto del mensaje de notificación. Si es necesario, establezca la configuración de notificaciones adicionales con un clic en el botón **Configuración**.

   - En la sección **Umbrales de generación de eventos**, especifique los intervalos de tiempo después de los cuales Kaspersky Embedded Systems Security para Windows registra los eventos *Las bases de datos de la aplicación están desactualizadas*, *Las bases de datos de la aplicación son obsoletas* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.

     - **La base de datos de la aplicación está desactualizada (días)**

     - **La base de datos de la aplicación es obsoleta (días)**

     - **Hace mucho tiempo que no se realiza un análisis de áreas críticas (días)**

6. Haga clic en el botón **Aceptar**.

La configuración de notificaciones se guarda.

Configuración de la interacción con el servidor de administración

Para seleccionar los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security para Windows envía información al Servidor de administración de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

- Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Registros y notificaciones**, haga clic en el botón **Interacción con Servidor de administración** en el bloque **Configuración**.

   La ventana **Lista de la red de servidores de administración** se abre.

5. En la ventana **Lista de la red de servidores de administración**, elija los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security para Windows enviará información al Servidor de administración de Kaspersky Security Center:

   - Objetos en Cuarentena.
   - Objetos con Copia de seguridad.

6. Haga clic en el botón **Aceptar**.

   Kaspersky Embedded Systems Security para Windows enviará información sobre los tipos de objeto seleccionados al Servidor de administración.

Configuración de notificaciones

Esta sección brinda información sobre las formas en que los usuarios y los administradores de Kaspersky Embedded Systems Security para Windows pueden recibir notificaciones sobre eventos de la aplicación y el estado de protección del dispositivo, además de instrucciones sobre cómo configurar notificaciones.

Métodos de notificación de administrador y usuario

Puede configurar la aplicación para notificar al administrador y a los usuarios que acceden al dispositivo acerca de lo siguientes eventos en el funcionamiento de Kaspersky Embedded Systems Security y el estado de la protección antivirus en el dispositivo.

- El administrador puede recibir información sobre eventos de tipos seleccionados.
- Los usuarios de LAN que acceden a un dispositivo y los usuarios de dispositivos terminales pueden recibir información sobre eventos del tipo *Objeto detectado* en la tarea de Protección de archivos en tiempo real.

En la Consola de la aplicación, las notificaciones para administradores y usuarios se pueden activar mediante diversos métodos:

- Métodos de notificación para usuarios:
  a. Herramientas de servicio de terminales.

     Se puede aplicar este método para notificar a los usuarios de dispositivos protegidos terminales si el dispositivo protegido se utiliza como terminal.

  b. Herramientas de servicio de mensajes.

     Se puede aplicar este método para la notificación a través de los servicios de mensajes de Microsoft Windows.

- Métodos de notificación para el administrador:
  a. Herramientas de servicio de mensajes.

     Se puede aplicar este método para la notificación a través de los servicios de mensajes de Microsoft Windows.

  b. Ejecución de un archivo ejecutable.

     Este método ejecuta un archivo ejecutable que se almacena en la unidad local del dispositivo protegido cuando ocurre un evento.

  c. Envío por correo electrónico.

     Este método utiliza el correo electrónico para transmitir los mensajes.

Puede crear el texto de un mensaje para los tipos de eventos individuales. Puede incluir un campo de información para describir un evento. De manera predeterminada, la aplicación utiliza un mensaje predeterminado para notificar a los usuarios.

Configuración de notificaciones de administrador y usuario

La configuración de notificaciones de eventos ofrece diversos métodos para configurar y redactar un texto del mensaje.

Para configurar las opciones de notificación de eventos:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones** y seleccione **Propiedades**.

   Se abre la ventana **Configuración de registros y notificaciones**.

2. En la pestaña **Notificaciones**, seleccione el modo de notificación:

   a. Seleccione el evento para el que desea seleccionar un método de notificación de la lista **Tipo de evento**.

   b. En el grupo de configuraciones **Notificar a los administradores** o **Notificar a los usuarios**, seleccione la casilla de verificación junto a los métodos de notificación que desea configurar.

   > Solo puede configurar las notificaciones del usuario para los siguientes eventos: **Objeto detectado**, **Dispositivo externo no confiable detectado y bloqueado** y **La sesión de red está en la lista de sesiones dudosas**.

3. Para agregar el texto de un mensaje:

   a. Haga clic en el botón **Texto del mensaje**.

   b. En la ventana que se abre, introduzca el texto que se mostrará en el mensaje del evento correspondiente.

   > Puede crear el mismo mensaje para varios tipos de eventos: después de seleccionar un método de notificación para un tipo de evento, utilice la tecla **Ctrl** o **Mayús** para seleccionar los otros tipos de eventos para los que desea utilizar el mismo mensaje y, a continuación, haga clic en el botón **Texto del mensaje**.

   a. Para agregar campos con información sobre un evento, haga clic en el botón **Macro** y seleccione los campos relevantes de la lista desplegable. En la tabla de esta sección se describen campos con información sobre los eventos.

   b. Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Predeterminado**.

4. Para configurar cómo se notificará a los administradores sobre un evento seleccionado, seleccione la pestaña **Notificaciones** y, en la sección **Configuración**, haga clic en el botón **Notificar a los administradores**. Luego, en la ventana **Configuración avanzada**, configure los métodos de notificación seleccionados. Para ello, realice las siguientes acciones:

   a. Para las notificaciones por correo electrónico, abra la pestaña **Correo electrónico** y especifique las direcciones de correo electrónico de los destinatarios (delimite las direcciones con punto y coma), el nombre o la dirección de red del servidor SMTP y el número de puerto en los campos correspondientes. Si es necesario, especifique el texto que se mostrará en los campos **Sujeto** y **De**. El texto del campo **Sujeto** también puede incluir variables con información sobre el evento (consulte la tabla a continuación).

   Si desea aplicar la autenticación con cuentas de usuario al establecer conexión con el servidor SMTP, seleccione **Configuración de autenticación** en el grupo **Usar autenticación SMTP** y especifique el nombre y la contraseña del usuario cuya cuenta de usuario se autenticará.

   b. Para notificaciones con el Servicio Windows Messenger, cree una lista de dispositivos protegidos de destinatarios para notificaciones en la pestaña **Servicio Windows Messenger**: para cada dispositivo protegido que desea agregar, haga clic en el botón **Agregar** y escriba su nombre de red en el campo de entrada.

c. Para que se ejecute un archivo, en la pestaña **Archivo ejecutable**, seleccione un archivo ejecutable que se encuentre en la unidad local del dispositivo protegido (o ingrese la ruta completa a dicho archivo). El archivo se ejecutará en el dispositivo protegido cuando ocurra el evento. Introduzca el nombre de usuario y la contraseña que se utilizarán para ejecutar el archivo.

Se pueden utilizar variables del entorno del sistema cuando se especifica la ruta al archivo ejecutable; no se permiten variables del entorno del usuario.

Si desea limitar la cantidad de mensajes para un tipo de evento durante un periodo, en la pestaña **Avanzado** seleccione **No enviar la misma notificación más de** y especifique la cantidad de veces y un intervalo de tiempo.

5. Haga clic en el botón **Aceptar**.

La configuración de notificaciones se guarda.

Campos con información sobre el evento

Variable	Descripción
%EVENT_TYPE%	Tipo de evento.
%EVENT_TIME%	Hora del evento.
%EVENT_SEVERITY%	Nivel de importancia.
%OBJECT%	Nombre del objeto (en tareas de Protección del equipo en tiempo real y de Análisis a pedido). La tarea de Actualización de módulos del programa incluye el nombre de la actualización y la dirección de la página web con información sobre la actualización.
%VIRUS_NAME%	El nombre del objeto según la clasificación de la Enciclopedia de virus. Cuando se detecta un objeto, este nombre se incluye en el nombre completo otorgado por Kaspersky Embedded Systems Security para Windows al objeto detectado. Puede ver el nombre completo de un objeto detectado en el registro de tareas.
%VIRUS_TYPE%	El tipo de objeto detectado según la clasificación de Kaspersky, como "virus" o "troyano". Esta cadena se incluye en el nombre completo que se muestra para el objeto detectado cuando Kaspersky Embedded Systems Security para Windows encuentra un objeto infectado o probablemente infectado. Puede ver el nombre completo de un objeto detectado en el registro de tareas.
%USER_COMPUTER%	En las tareas de Protección de archivos en tiempo real, el nombre del dispositivo protegido del usuario que accedió al objeto en el dispositivo.
%USER_NAME%	En las tareas de Protección de archivos en tiempo real, el nombre del usuario que accedió al objeto en el dispositivo.
%FROM_COMPUTER%	Nombre del dispositivo protegido en el que se originó la notificación.
%EVENT_REASON%	Motivo por el cual ocurrió el evento (algunos eventos no tienen este campo).
%ERROR_CODE%	Código de error (solo para evento de "Error interno de tarea").
%TASK_NAME%	Nombre de la tarea (solo para eventos relacionados con el rendimiento de la tarea).

Cómo iniciar y detener Kaspersky Embedded Systems Security para Windows

Esta sección contiene información sobre el inicio de la Consola de la aplicación y sobre el inicio y la detención del servicio de Kaspersky Security.

Inicio del Complemento de administración de Kaspersky Embedded Systems Security para Windows

No se requiere ninguna acción avanzada para iniciar el Complemento de administración de Kaspersky Embedded Systems Security para Windows en Kaspersky Security Center. Una vez que el Complemento de administración se instala en el dispositivo protegido del administrador, se inicia junto con Kaspersky Security Center. La información detallada sobre Kaspersky Security Center inicial se puede encontrar en la *Ayuda de Kaspersky Security Center*.

Inicio de la Consola de Kaspersky Embedded Systems Security para Windows desde el menú Inicio

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

*Para iniciar la Consola de la aplicación desde el menú **Inicio**:*

1. En el menú **Inicio**, seleccione **Programas** > **Kaspersky Embedded Systems Security para Windows** > **Herramientas de administración** > **Consola de Kaspersky Embedded Systems Security para Windows**.

Para agregar otros complementos a la Consola de la aplicación, abra la Consola en modo de creación.

Para iniciar la Consola de la aplicación en modo autor:

1. En el menú **Iniciar**, seleccione **Programas** > **Kaspersky Embedded Systems Security para Windows** > **Herramientas de administración**.
2. En el menú contextual de la Consola de la aplicación, seleccione el comando **Creación**.

   Se inicia la Consola de la aplicación en modo de creación.

Si la Consola de la aplicación se ha iniciado en el dispositivo protegido, se abrirá la ventana Consola de la aplicación.

Si inició la Consola de la aplicación en un dispositivo no protegido, conéctese al dispositivo protegido.

Para conectarse con el dispositivo protegido:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.
2. Seleccione el comando **Conectarse a otro equipo**.

   Se abre la ventana **Seleccionar dispositivo protegido**.
3. Seleccione **Otro dispositivo** en la ventana que se abre.

4. Especifique el nombre de la red del dispositivo protegido en el campo de entrada a la derecha.

5. Haga clic en el botón **Aceptar**.

La Consola de la aplicación se conectará con el dispositivo protegido.

Si la cuenta del usuario que usa para iniciar sesión en Microsoft Windows no tiene permisos suficientes para acceder al servicio de Kaspersky Security Management en el dispositivo protegido, seleccione la casilla de verificación **Conectarse como usuario** y especifique una cuenta de usuario diferente que tenga los permisos requeridos.

Inicio y detención del servicio de Kaspersky Security

De forma predeterminada, el servicio de Kaspersky Security se inicia automáticamente después del inicio del sistema operativo. El servicio de Kaspersky Security administra los procesos de trabajo que ejecutan las tareas de Actualización, Protección del equipo en tiempo real, Control del equipo y Análisis a pedido.

De forma predeterminada, cuando se inicia el servicio de Kaspersky Embedded Systems Security para Windows, se inician las tareas de Protección de archivos en tiempo real, Análisis al inicio del sistema operativo y Control de integridad de la aplicación, así como otras tareas que están programadas para iniciarse **Al inicio de la aplicación**.

Si se detiene el servicio de Kaspersky Security, todas las tareas en ejecución se detienen. Una vez que el servicio de Kaspersky Security se reinicia, la aplicación inicia automáticamente solo aquellas tareas programadas para ejecutarse **Al inicio de la aplicación**. Las demás tareas deben iniciarse manualmente.

Puede iniciar y detener el servicio de Kaspersky Security con el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows** o con el complemento Servicios de Microsoft Windows.

Puede iniciar y detener Kaspersky Embedded Systems Security para Windows si es miembro del grupo de Administradores en el dispositivo protegido.

Para detener o iniciar la aplicación con la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.

2. Seleccione uno de los siguientes elementos:

   - **Detener el servicio**

   - **Iniciar el servicio**

El servicio de Kaspersky Security se iniciará o se detendrá.

Inicio de los componentes de Kaspersky Embedded Systems Security para Windows en el modo seguro del sistema operativo

Esta sección proporciona información sobre cómo funciona Kaspersky Embedded Systems Security para Windows en el modo seguro del sistema operativo.

Acerca de Kaspersky Embedded Systems Security para Windows cuando se ejecuta en el modo seguro del sistema operativo

Los componentes de Kaspersky Embedded Systems Security para Windows pueden iniciarse cuando el sistema operativo se carga en modo seguro. Además del servicio de Kaspersky Security (kavfs.exe), se carga el controlador klam.sys. Se utiliza para registrar el servicio de Kaspersky Security como un servicio protegido durante el inicio del sistema operativo. Para obtener más información, consulte la sección Registro del servicio de Kaspersky Security como servicio protegido.

Kaspersky Embedded Systems Security para Windows puede iniciarse en los siguientes modos seguros del sistema operativo:

- Modo seguro mínimo: este modo se inicia cuando se selecciona la opción estándar del modo seguro del sistema operativo. En ese momento, Kaspersky Embedded Systems Security para Windows puede iniciar los siguientes componentes:
  - Protección de archivos en tiempo real.
  - Análisis a pedido.
  - Control de inicio de aplicaciones y Generador de reglas de Control de inicio de aplicaciones.
  - Inspección de registros.
  - Monitor de integridad de archivos.
  - Monitor comparativo de integridad de archivos.
  - Control de integridad de la aplicación.

Modo seguro con red: en este modo, el sistema operativo se carga en modo seguro con controladores de red. Además de los componentes que se inician en el modo seguro mínimo, Kaspersky Embedded Systems Security para Windows puede iniciar los siguientes componentes en este modo:

- Actualización de bases de datos
- Actualización de módulos del programa

Inicio de Kaspersky Embedded Systems Security para Windows en modo seguro

De forma predeterminada, Kaspersky Embedded Systems Security para Windows no se inicia cuando el sistema operativo se carga en modo seguro.

Para hacer que Kaspersky Embedded Systems Security para Windows se inicie en el modo seguro del sistema operativo:

1. Inicie el editor de Registro de Windows (C:\Windows\regedit.exe).

2. Abra la clave [HKEY_LOCAL_MACHINE \ SYSTEM\CurrentControlSet\Services\klam\Parameters] del registro del sistema.

3. Abra el parámetro LoadInSafeMode.

4. Ajuste el valor a `1`.

5. Haga clic en el botón **Aceptar**.

Para cancelar el inicio de Kaspersky Embedded Systems Security para Windows en el modo seguro del sistema operativo:

1. Inicie el editor de Registro de Windows (C:\Windows\regedit.exe).

2. Abra la clave [HKEY_LOCAL_MACHINE \ SYSTEM\CurrentControlSet\Services\klam\Parameters] del registro del sistema.

3. Abra el parámetro LoadInSafeMode.

4. Ajuste el valor a `0`.

5. Haga clic en el botón **Aceptar**.

Autoprotección de Kaspersky Embedded Systems Security para Windows

Esta sección brinda información sobre los mecanismos de autoprotección de Kaspersky Embedded Systems Security para Windows.

Acerca de la autoprotección de Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows tiene mecanismos de autoprotección que protegen la aplicación contra la modificación o eliminación de sus carpetas, los procesos de memoria y las entradas de registro del sistema.

Protección contra cambios en carpetas con componentes de Kaspersky Embedded Systems Security para Windows instalados

Kaspersky Embedded Systems Security para Windows bloquea el cambio de nombre y la eliminación de carpetas con los componentes de la aplicación instalada por cualquier cuenta de usuario. De forma predeterminada, las rutas de las carpetas de instalación de la aplicación son las siguientes:

- En la versión de 32 bits de Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Protección contra cambios en las claves de registro de Kaspersky Embedded Systems Security para Windows

Kaspersky Embedded Systems Security para Windows restringe el acceso a las siguientes ramas y claves del registro, que facilitan la carga de los controladores y servicios de la aplicación:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.3] (en Microsoft Windows de 64 bits)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.3\Trace]

Los derechos para cambiar estas ramas y claves del registro se otorgan solo a la cuenta del Sistema Local (SISTEMA). Las cuentas de usuario y administrador se otorgan con derechos de solo lectura.

Protección contra cambios a la memoria de las partes de servicio del programa

Para proteger las partes de servicio del programa frente a procesos de terceros, los controladores de Kaspersky Embedded Systems Security para Windows restringen el acceso a los siguientes archivos ejecutables:

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

De forma predeterminada, el acceso a la memoria de las partes de servicio de Kaspersky Embedded Systems Security para Windows está restringido para los procesos de terceros.

Puede habilitar las funciones de autoprotección en las propiedades de la directiva dentro de la Consola de Kaspersky Embedded Systems Security para Windows y del Complemento de administración de Kaspersky Embedded Systems Security para Windows.

Registro del servicio de Kaspersky Security como servicio protegido

La tecnología de protección de procesos *Protected Process Light* (conocida por sus siglas "PPL") garantiza que el sistema operativo solo cargue servicios y procesos de confianza. Para que un servicio se ejecute como servicio protegido, debe instalarse el controlador de *antimalware de ejecución temprana* en el dispositivo protegido.

Un controlador de *antimalware de ejecución temprana* (también denominado "ELAM") ofrece protección para los dispositivos en la red cuando se inician, antes de que se inicien los controladores de terceros.

El controlador ELAM se instala automáticamente durante la instalación de Kaspersky Embedded Systems Security para Windows y se utiliza para registrar el servicio de Kaspersky Security como PPL cuando se inicia el sistema operativo. Cuando el servicio de Kaspersky Security (KAVFS) se inicia como proceso protegido del sistema, otros procesos no protegidos en el sistema no pueden inyectar subprocesos, escribir en la memoria virtual del proceso protegido o detener el servicio.

Cuando un proceso se inicia como PPL, no puede ser administrado por un usuario independientemente de los permisos del usuario asignados. El registro del servicio de Kaspersky Security como PPL usando el controlador ELAM se admite en sistemas operativos Microsoft Windows 10 y superiores. Si instala Kaspersky Embedded Systems Security para Windows en un servidor que ejecute un sistema operativo compatible con PPL, la gestión de permisos no estará disponible para el servicio de Kaspersky Security (KAVFS).

Para instalar Kaspersky Embedded Systems Security para Windows como PPL, ejecute el siguiente comando:

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security para Windows

Esta sección contiene información acerca de los permisos para administrar Kaspersky Embedded Systems Security para Windows y los servicios del sistema operativo registrados por la aplicación, e instrucciones sobre cómo configurar estos permisos.

Acerca de los permisos para administrar Kaspersky Embedded Systems Security para Windows

De forma predeterminada, tienen acceso a todas las funciones de Kaspersky Embedded Systems Security para Windows los usuarios del grupo de "Administradores" del dispositivo protegido, los usuarios del grupo de administradores de ESS creado en el dispositivo protegido durante la instalación de Kaspersky Embedded Systems Security para Windows y el grupo SYSTEM.

Los usuarios que tienen acceso al nivel Editar permisos de Kaspersky Embedded Systems Security para Windows pueden conceder acceso a las funciones de Kaspersky Embedded Systems Security para Windows a otros usuarios registrados en el dispositivo protegido o incluidos en el dominio.

Los usuarios que no están registrados en la lista de usuarios de Kaspersky Embedded Systems Security para Windows no pueden abrir la Consola de la aplicación.

Puede elegir uno de los siguientes niveles preestablecidos de acceso para un usuario o un grupo de usuarios:

- **Control total**: acceso a todas las funciones de la aplicación, p. ej., la capacidad de ver y modificar la configuración general de Kaspersky Embedded Systems Security para Windows, la configuración de los componentes y los permisos de usuarios de Kaspersky Embedded Systems Security para Windows, y la capacidad de ver estadísticas de Kaspersky Embedded Systems Security para Windows.
- **Modificación**: acceso a todas las funciones de la aplicación, excepto la edición de permisos del usuario, p. ej., la capacidad de ver y editar la configuración general de Kaspersky Embedded Systems Security para Windows y los parámetros de los componentes de Kaspersky Embedded Systems Security para Windows.
- **Lectura**: la capacidad de ver la configuración general de Kaspersky Embedded Systems Security para Windows, la configuración de los componentes de Kaspersky Embedded Systems Security para Windows, las estadísticas de Kaspersky Embedded Systems Security para Windows y los permisos de usuario de Kaspersky Embedded Systems Security para Windows.

También puede configurar permisos de acceso avanzados: permita o bloquee el acceso a funciones específicas de Kaspersky Embedded Systems Security para Windows.

Si ha configurado manualmente permisos de acceso para un usuario o grupo, el nivel de acceso **Permisos especiales** se configura para este usuario o grupo.

Acerca de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security para Windows

Derechos de usuario	Descripción
Administración de tareas	Capacidad para iniciar/detener/pausar/reanudar tareas de Kaspersky Embedded Systems Security para Windows.
Crear y eliminar tareas	Capacidad para crear y eliminar tareas de Análisis a pedido.

de Análisis a pedido	
Editar configuración	Capacidad para: • Importar ajustes de Kaspersky Embedded Systems Security para Windows desde un archivo de configuración. • Editar la configuración de la aplicación.
Leer configuración	Capacidad para: • Ver la configuración general y la configuración de tareas de Kaspersky Embedded Systems Security para Windows. • Exportar la configuración de Kaspersky Embedded Systems Security para Windows a un archivo de configuración. • Ver la configuración de los registros de tareas, del registro de auditoría del sistema y de las notificaciones.
Administrar depósitos	Capacidad para: • Mover objetos a Cuarentena. • Eliminar objetos de la Cuarentena y de la Copia de seguridad. • Restaurar objetos de la Cuarentena y de la Copia de seguridad.
Administrar registros	Capacidad para eliminar registros de tareas y borrar el registro de auditoría del sistema.
Leer registros	Capacidad para ver eventos del antivirus en los registros de tareas y el registro de auditoría del sistema.
Leer estadísticas	Capacidad para ver estadísticas por cada tarea de Kaspersky Embedded Systems Security para Windows.
Licencia de la aplicación	Capacidad de activar Kaspersky Embedded Systems Security para Windows.
Desinstalar la aplicación	Capacidad de desinstalar Kaspersky Embedded Systems Security para Windows.
Leer permisos	Capacidad para ver la lista de usuarios de Kaspersky Embedded Systems Security para Windows y los privilegios de acceso de los usuarios.
Editar permisos	Capacidad para: • Modificar la lista de usuarios con acceso a la administración de la aplicación. • Modificar los permisos de acceso para las funciones de Kaspersky Embedded Systems Security para Windows.

Acerca de los permisos para administrar servicios registrados

Durante la instalación, Kaspersky Embedded Systems Security para Windows registra en Windows el servicio de Kaspersky Security (KAVFS), el servicio de Kaspersky Security Management (KAVFSGT) y el servicio de Kaspersky Security Exploit Prevention (KAVFSSLP).

El servicio de Kaspersky Security puede registrarse como Protected Process Light mediante el controlador ELAM en sistemas operativos Microsoft Windows 10 y superiores. Cuando un proceso se inicia como PPL, no puede ser administrado por un usuario independientemente de los permisos del usuario asignados. Si instala Kaspersky Embedded Systems Security para Windows en un dispositivo protegido que ejecute un sistema operativo compatible con PPL, la gestión de permisos no estará disponible para el servicio de Kaspersky Security (KAVFS).

Servicio de Kaspersky Security

De forma predeterminada, los permisos de acceso para administrar el servicio de Kaspersky Security se conceden a los usuarios del grupo Administradores en el dispositivo protegido, así como a los grupos de SERVICE e INTERACTIVE con permisos de lectura y al grupo SYSTEM con permisos de lectura y ejecución.

Los usuarios que tienen acceso al nivel Editar permisos pueden otorgar permisos de acceso para administrar el servicio de Kaspersky Security a los demás usuarios registrados en el dispositivo protegido o incluido en el dominio.

Servicio de Kaspersky Security Management

Para administrar la aplicación mediante la Consola de la aplicación instalada en otro dispositivo protegido, la cuenta con los permisos para conectarse a Kaspersky Embedded Systems Security para Windows debe tener acceso absoluto al servicio de Kaspersky Security Management en el dispositivo protegido.

De forma predeterminada, tienen acceso al servicio de Kaspersky Security Management los usuarios del grupo "Administradores" del dispositivo protegido y los usuarios del grupo de administradores de ESS que se crea en el dispositivo protegido durante la instalación de Kaspersky Embedded Systems Security para Windows.

Solo puede administrar el servicio de Kaspersky Security Management a través del complemento Servicios de Microsoft Windows.

Servicio de Kaspersky Security Exploit Prevention

De forma predeterminada, tienen permiso de acceso para administrar el servicio de Kaspersky Security Exploit Prevention los usuarios del grupo "Administradores" del dispositivo protegido. También se concede este permiso al grupo SYSTEM, con permisos de lectura y ejecución.

Acerca de los permisos de acceso para el servicio de Kaspersky Security Management

Puede revisar la lista de servicios de Kaspersky Embedded Systems Security para Windows.

Durante la instalación, Kaspersky Embedded Systems Security para Windows registra el servicio de Kaspersky Security Management (KAVFSGT). Para administrar la aplicación mediante la Consola de la aplicación instalada en otro dispositivo protegido, la cuenta utilizada para conectarse a Kaspersky Embedded Systems Security para Windows debe tener acceso absoluto al servicio de Kaspersky Security Management en el dispositivo protegido.

De forma predeterminada, tienen acceso al servicio de Kaspersky Security Management los usuarios del grupo "Administradores" del dispositivo protegido y los usuarios del grupo de administradores de ESS que se crea en el dispositivo protegido durante la instalación de Kaspersky Embedded Systems Security para Windows.

Solo puede administrar el servicio de Kaspersky Security Management a través del complemento Servicios de Microsoft Windows.

No puede autorizar o bloquear el acceso de los usuarios al servicio de Kaspersky Security Management con Kaspersky Embedded Systems Security para Windows.

Puede conectarse a Kaspersky Embedded Systems Security para Windows desde una cuenta local si se registró una cuenta con el mismo nombre de usuario y contraseña en el dispositivo protegido.

Acerca de los permisos para administrar el servicio de Kaspersky Security

Durante la instalación, Kaspersky Embedded Systems Security para Windows registra el servicio de Kaspersky Security (KAVFS) en Windows, e internamente habilita los componentes funcionales que se comienzan cuando se inicia el sistema operativo. Para reducir el riesgo de que un tercero acceda a las funciones de la aplicación y a los ajustes de seguridad del dispositivo protegido mediante el servicio de Kaspersky Security, puede restringir los permisos para administrar el servicio de Kaspersky Security desde la Consola de la aplicación o el Complemento de administración.

De forma predeterminada, los permisos de acceso para administrar el servicio de Kaspersky Security se conceden a usuarios en el grupo de Administradores en el dispositivo protegido. Los permisos de lectura se conceden a los grupos de SERVICIO e INTERACTIVOS, y los permisos de lectura y ejecución se conceden al grupo SYSTEM.

No se puede eliminar la cuenta de usuario de SYSTEM o modifica permisos para esta cuenta. Si se modifican los permisos de la cuenta SYSTEM, los privilegios máximos se restauran para esta cuenta cuando guarda los cambios.

Los usuarios que tienen acceso a funciones para las que se requieren permisos de nivel "Editar" pueden otorgar permisos de acceso para administrar el servicio de Kaspersky Security a otros usuarios registrados en el dispositivo protegido o incluidos en el dominio.

Los usuarios o grupos de usuarios de Kaspersky Embedded Systems Security para Windows pueden contar con uno de los siguientes niveles de permisos de acceso predeterminados para administrar el servicio de Kaspersky Security:

- **Control total**: capacidad de ver y modificar la configuración general y los permisos de usuario para el servicio de Kaspersky Security, e iniciar y detener el servicio de Kaspersky Security.
- **Lectura**: capacidad de ver la configuración general y los permisos de usuario del servicio de Kaspersky Security.
- **Modificación**: capacidad de ver y modificar la configuración general y los permisos de usuario del servicio de Kaspersky Security.
- **Ejecución**: capacidad de iniciar y detener el servicio de Kaspersky Security.

También puede configurar los permisos del acceso avanzado: autorice o deniegue el acceso a funciones específicas de Kaspersky Embedded Systems Security para Windows (ver la tabla a continuación).

Si ha configurado manualmente permisos de acceso para un usuario o grupo, el nivel de acceso **Permisos especiales** se configura para este usuario o grupo.

Permisos de acceso para las funciones del servicio de Kaspersky Security.

Función	Descripción
Ver configuraciones del servicio	Capacidad para ver las configuraciones generales y los permisos de usuario del servicio de Kaspersky Security.
Solicitar estado del servicio al Administrador de control de servicios	Capacidad para solicitar el estado de ejecución del servicio de Kaspersky Security al administrador de control de servicios de Microsoft Windows.
Solicitar estado al servicio	Capacidad para solicitar el estado de ejecución del servicio desde el servicio de Kaspersky Security.
Leer lista de servicios dependientes	Capacidad para ver una lista con los servicios de los que depende el servicio de Kaspersky Security y aquellos que dependen del servicio de Kaspersky Security.
Modificación de la configuración del servicio	Capacidad de ver y modificar la configuración general y los permisos del usuario del servicio de Kaspersky Security.
Iniciar el servicio	Capacidad para iniciar el servicio de Kaspersky Security.
Detener el servicio	Capacidad para detener el servicio de Kaspersky Security.
Pausar/reanudar el servicio	Capacidad para pausar y reanudar el servicio de Kaspersky Security.
Leer permisos	Capacidad para ver la lista de usuarios del servicio de Kaspersky Security y los privilegios de acceso de cada usuario.
Editar permisos	Capacidad para: • Agregar y eliminar usuarios del servicio de Kaspersky Security. • Modificar los permisos de acceso de usuarios para el servicio de Kaspersky Security.
Eliminar el servicio	Capacidad para eliminar el registro del servicio de Kaspersky Security en el Administrador de control de servicios de Microsoft Windows.
Solicitudes definidas por el usuario al servicio	Capacidad para crear y enviar solicitudes de usuario al servicio de Kaspersky Security.

Administración de los permisos de acceso mediante el Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y configurar los permisos de acceso para uno o todos los dispositivos en la red.

Configuración de los permisos de acceso para Kaspersky Embedded Systems Security para Windows y el servicio de Kaspersky Security

Puede editar la lista de usuarios y grupos de usuarios autorizados para acceder a las funciones de Kaspersky Embedded Systems Security para Windows y administrar el servicio de Kaspersky Security. También puede editar los permisos de acceso de esos usuarios y grupos de usuarios.

Para agregar o quitar un usuario o un grupo de la lista:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Adicional**, siga uno de estos pasos:
   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar las funciones de Kaspersky Embedded Systems Security para Windows.
   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar el servicio de Kaspersky Security.

     Se abre la ventana **Permisos para Kaspersky Embedded Systems Security para Windows**.
5. En la ventana que se abre, realice las siguientes operaciones:
   - Para agregar un usuario o un grupo a la lista, haga clic en el botón **Agregar** y seleccione el usuario o el grupo a quien desea otorgar privilegios.
   - Para eliminar un usuario o un grupo de la lista, seleccione el usuario o el grupo cuyo acceso desea restringir, y haga clic en el botón **Eliminar**.
6. Haga clic en el botón **Aplicar**.

Los usuarios seleccionados (grupos) se agregan o se eliminan.

Para modificar permisos de un usuario o un grupo para la administración de Kaspersky Embedded Systems Security para Windows o el servicio de Kaspersky Security:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Adicional**, siga uno de estos pasos:

- Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar las funciones de Kaspersky Embedded Systems Security para Windows.

- Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar la aplicación mediante el servicio de Kaspersky Security.

  Se abre la ventana **Permisos para Kaspersky Embedded Systems Security para Windows**.

5. En la ventana que se abre, en la lista **Nombres de usuarios o grupos**, seleccione el usuario o grupo de usuarios a los que desea cambiar los permisos.

6. En la sección **Permisos para <Usuario (Grupo)>**, seleccione las casillas de verificación **Autorizar** o **Denegar** para los siguientes niveles de acceso:

   - **Control total**: conjunto completo de permisos para administrar Kaspersky Embedded Systems Security para Windows o el servicio de Kaspersky Security.

   - **Lectura**:

     - Los siguientes permisos para administrar Kaspersky Embedded Systems Security para Windows: **Leer estadísticas**, **Leer configuración**, **Leer registros** y **Permisos de lectura**.

     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Leer configuración del servicio**, **Solicitar estado del Administrador de control de servicios**, **Solicitar estado al servicio**, **Leer lista de servicios dependientes**, **Permisos de lectura**.

   - **Modificación**:

     - Todos los permisos para administrar Kaspersky Embedded Systems Security para Windows, excepto **Permisos de edición**.

     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Modificar configuración del servicio**, **Permisos de lectura**.

   - **Permisos especiales**: los siguientes permisos para administrar el servicio de Kaspersky Security: **Iniciando el servicio**, **Detener el servicio**, **Pausar o reanudar el servicio**, **Permisos de lectura**, **Solicitudes definidas por el usuario al servicio**.

7. Para establecer permisos avanzados para un usuario o grupo (**Permisos especiales**), haga clic en el botón **Avanzado**.

   a. En la ventana **Configuración de seguridad avanzada para Kaspersky Embedded Systems Security para Windows** que se abre, seleccione el usuario o grupo deseados.

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

   c. En la lista desplegable ubicada en la parte superior de la ventana, seleccione el tipo de control de acceso (**Autorizar** o **Bloquear**).

   d. Seleccione las casillas de verificación al lado de las funciones que desea autorizar o bloquear para el usuario o el grupo seleccionado.

   e. Haga clic en el botón **Aceptar**.

   f. En la ventana **Configuración de seguridad avanzada para Kaspersky Embedded Systems Security para Windows**, haga clic en **Aceptar**.

8. En la ventana **Permisos para Kaspersky Embedded Systems Security para Windows**, haga clic en el botón **Aplicar**.

Los permisos configurados para administrar Kaspersky Embedded Systems Security para Windows o el servicio de Kaspersky Security se guardarán.

Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security para Windows

Se puede restringir el acceso a la gestión de aplicaciones y servicios registrados al configurar los permisos del usuario. También se puede establecer la protección con contraseña en Kaspersky Embedded Systems Security para Windows para obtener una protección adicional de las operaciones críticas.

Kaspersky Embedded Systems Security para Windows solicita una contraseña cuando se intenta acceder a las siguientes funciones de la aplicación:

- conectarse a la Consola de la aplicación;
- desinstalar Kaspersky Embedded Systems Security para Windows;
- modificar los componentes de Kaspersky Embedded Systems Security para Windows;
- ejecutar los comandos de la línea de comandos.

La interfaz de Kaspersky Embedded Systems Security para Windows oculta la contraseña especificada en la pantalla. Kaspersky Embedded Systems Security para Windows almacena la contraseña como una suma de control calculada cuando se ingresa la contraseña.

Kaspersky Embedded Systems Security para Windows no verifica la seguridad de la contraseña y no bloquea la entrada de la contraseña después de varios intentos fallidos.

Al crear una contraseña, se recomienda cumplir con las siguientes condiciones:

- La contraseña no contiene el nombre de la cuenta ni el nombre del equipo.
- La contraseña tiene al menos 8 caracteres de longitud.
- La contraseña contiene caracteres que coinciden con al menos tres de las siguientes categorías:
  - Letras latinas mayúsculas (A-Z)
  - Letras latinas minúsculas (a-z)
  - Números (0-9)
  - Símbolos de signo de exclamación (!), signo de dólar ($), signo de numeral (#) y signo de porcentaje (%)

Se puede exportar e importar una configuración de aplicación protegida por contraseña. Un archivo de configuración creado al exportar una configuración de aplicación protegida contiene la suma de control de contraseña y el valor del modificador utilizado para completar la cadena de contraseña.

No cambie la suma de control ni el modificador en el archivo de configuración. La importación de una configuración protegida por contraseña que se ha cambiado manualmente puede provocar que el acceso a la aplicación se bloquee por completo.

Para proteger el acceso a funciones de Kaspersky Embedded Systems Security para Windows:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**. Seleccione el grupo de administración con los dispositivos protegidos cuyos parámetros de aplicación desea configurar.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para configurar los parámetros de las directivas para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra las propiedades de **<Nombre de la directiva>** mediante el menú contextual.
   - Si desea configurar los ajustes de la aplicación para un solo dispositivo protegido, abra los ajustes requeridos en la ventana **Configuración de la aplicación** en Kaspersky Security Center.
3. En la sección **Configuración de la aplicación** de la pestaña **Seguridad y confiabilidad**, haga clic en el botón **Configuración**.

   Se abre la ventana **Configuración de seguridad**.
4. En la sección **Configuración de protección con contraseña**, seleccione la casilla de verificación **Aplicar protección con contraseña**.

   Los campos **Contraseña** y **Confirmar contraseña** se activan.
5. En el campo **Contraseña**, escriba la contraseña que desea usar para proteger el acceso a las funciones de Kaspersky Embedded Systems Security para Windows.
6. En el campo **Confirmar contraseña**, escriba la contraseña nuevamente.
7. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada. Kaspersky Embedded Systems Security para Windows solicitará la contraseña especificada para acceder a las funciones protegidas.

Esta contraseña no se puede recuperar. Si pierde su contraseña, perderá completamente el control de la aplicación. Además, será imposible desinstalar la aplicación del dispositivo protegido.

Puede reiniciar la contraseña en cualquier momento. Para hacerlo, desactive la casilla **Aplicar protección con contraseña** y guarde los cambios. Se deshabilitará la protección con contraseña y se eliminará la suma de control de la contraseña anterior. Repita el proceso de creación de contraseña con una contraseña nueva.

Administración de los permisos de acceso mediante la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y configurar los permisos de acceso en un dispositivo protegido.

Configuración de los permisos de acceso para administrar Kaspersky Embedded Systems Security para Windows y el servicio de Kaspersky Security

Puede editar la lista de usuarios y grupos de usuarios autorizados para acceder a las funciones de Kaspersky Embedded Systems Security para Windows y administrar el servicio de Kaspersky Security. También puede editar los permisos de acceso de esos usuarios y grupos de usuarios.

Para agregar o quitar un usuario o un grupo de la lista:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Adicional**, siga uno de estos pasos:
   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar las funciones de Kaspersky Embedded Systems Security para Windows.
   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar el servicio de Kaspersky Security.

     Se abre la ventana **Permisos para Kaspersky Embedded Systems Security para Windows**.
5. En la ventana que se abre, realice las siguientes operaciones:
   - Para agregar un usuario o un grupo a la lista, haga clic en el botón **Agregar** y seleccione el usuario o el grupo a quien desea otorgar privilegios.
   - Para eliminar un usuario o un grupo de la lista, seleccione el usuario o el grupo cuyo acceso desea restringir, y haga clic en el botón **Eliminar**.
6. Haga clic en el botón **Aplicar**.

Los usuarios seleccionados (grupos) se agregan o se eliminan.

Para modificar permisos de un usuario o un grupo para la administración de Kaspersky Embedded Systems Security para Windows o el servicio de Kaspersky Security:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Adicional**, siga uno de estos pasos:

   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar las funciones de Kaspersky Embedded Systems Security para Windows.

   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar la aplicación mediante el servicio de Kaspersky Security.

     Se abre la ventana **Permisos para Kaspersky Embedded Systems Security para Windows**.

5. En la ventana que se abre, en la lista **Nombres de usuarios o grupos**, seleccione el usuario o grupo de usuarios a los que desea cambiar los permisos.

6. En la sección **Permisos para <Usuario (Grupo)>**, seleccione las casillas de verificación **Autorizar** o **Denegar** para los siguientes niveles de acceso:

   - **Control total**: conjunto completo de permisos para administrar Kaspersky Embedded Systems Security para Windows o el servicio de Kaspersky Security.

   - **Lectura**:

     - Los siguientes permisos para administrar Kaspersky Embedded Systems Security para Windows: **Leer estadísticas**, **Leer configuración**, **Leer registros** y **Permisos de lectura**.

     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Leer configuración del servicio**, **Solicitar estado del Administrador de control de servicios**, **Solicitar estado al servicio**, **Leer lista de servicios dependientes**, **Permisos de lectura**.

   - **Modificación**:

     - Todos los permisos para administrar Kaspersky Embedded Systems Security para Windows, excepto **Permisos de edición**.

     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Modificar configuración del servicio**, **Permisos de lectura**.

   - **Permisos especiales**: los siguientes permisos para administrar el servicio de Kaspersky Security: **Iniciando el servicio**, **Detener el servicio**, **Pausar o reanudar el servicio**, **Permisos de lectura**, **Solicitudes definidas por el usuario al servicio**.

7. Para establecer permisos avanzados para un usuario o grupo (**Permisos especiales**), haga clic en el botón **Avanzado**.

   a. En la ventana **Configuración de seguridad avanzada para Kaspersky Embedded Systems Security para Windows** que se abre, seleccione el usuario o grupo deseados.

b. Haga clic en el botón **Editar**.

c. En la lista desplegable ubicada en la parte superior de la ventana, seleccione el tipo de control de acceso (**Autorizar** o **Bloquear**).

d. Seleccione las casillas de verificación al lado de las funciones que desea autorizar o bloquear para el usuario o el grupo seleccionado.

e. Haga clic en el botón **Aceptar**.

f. En la ventana **Configuración de seguridad avanzada para Kaspersky Embedded Systems Security para Windows**, haga clic en **Aceptar**.

8. En la ventana **Permisos para Kaspersky Embedded Systems Security para Windows**, haga clic en el botón **Aplicar**.

9. Los permisos configurados para administrar Kaspersky Embedded Systems Security para Windows o el servicio de Kaspersky Security se guardarán.

Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security para Windows

Se puede restringir el acceso a la gestión de aplicaciones y servicios registrados al configurar los permisos del usuario. También se puede establecer la protección con contraseña en Kaspersky Embedded Systems Security para Windows para obtener una protección adicional de las operaciones críticas.

Kaspersky Embedded Systems Security para Windows solicita una contraseña cuando se intenta acceder a las siguientes funciones de la aplicación:

- conectarse a la Consola de la aplicación;
- desinstalar Kaspersky Embedded Systems Security para Windows;
- modificar los componentes de Kaspersky Embedded Systems Security para Windows;
- ejecutar los comandos de la línea de comandos.

La interfaz de Kaspersky Embedded Systems Security para Windows oculta la contraseña especificada en la pantalla. Kaspersky Embedded Systems Security para Windows almacena la contraseña como una suma de control calculada cuando se ingresa la contraseña.

Kaspersky Embedded Systems Security para Windows no verifica la seguridad de la contraseña y no bloquea la entrada de la contraseña después de varios intentos fallidos.

Al crear una contraseña, se recomienda cumplir con las siguientes condiciones:

- La contraseña no contiene el nombre de la cuenta ni el nombre del equipo.
- La contraseña tiene al menos 8 caracteres de longitud.
- La contraseña contiene caracteres que coinciden con al menos tres de las siguientes categorías:

- Letras latinas mayúsculas (A-Z)
- Letras latinas minúsculas (a-z)
- Números (0-9)
- Símbolos de signo de exclamación (!), signo de dólar ($), signo de numeral (#) y signo de porcentaje (%)

Se puede exportar e importar una configuración de aplicación protegida por contraseña. Un archivo de configuración creado al exportar una configuración de aplicación protegida contiene la suma de control de contraseña y el valor del modificador utilizado para completar la cadena de contraseña.

No cambie la suma de control ni el modificador en el archivo de configuración. La importación de una configuración protegida por contraseña que se ha cambiado manualmente puede provocar que el acceso a la aplicación se bloquee por completo.

Para proteger el acceso a funciones de Kaspersky Embedded Systems Security para Windows:

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security para Windows** y realice una de las siguientes acciones:
   - Haga clic en el vínculo **Propiedades de la aplicación** en el panel de detalles del nodo.
   - Seleccione **Propiedades** en el menú contextual del nodo.

   Se muestra la ventana **Configuración de la aplicación**.
2. En la pestaña **Seguridad y fiabilidad** en la sección **Configuración de protección con contraseña**, seleccione la casilla de verificación **Aplicar protección con contraseña**.

   Los campos **Contraseña** y **Confirmar contraseña** se activan.
3. En el campo **Contraseña**, escriba la contraseña que desea usar para proteger el acceso a las funciones de Kaspersky Embedded Systems Security para Windows.
4. En el campo **Confirmar contraseña**, escriba la contraseña nuevamente.
5. Haga clic en el botón **Aceptar**.

Esta contraseña no se puede recuperar. Si pierde su contraseña pierde completamente el control de la aplicación. Además, será imposible desinstalar la aplicación del dispositivo protegido.

Puede reiniciar la contraseña en cualquier momento. Para hacerlo, desactive la casilla **Aplicar protección con contraseña** y guarde los cambios. Se deshabilitará la protección con contraseña y se eliminará la suma de control de la contraseña anterior. Repita el proceso de creación de contraseña con una contraseña nueva.

Administración de los permisos de acceso mediante el Complemento web

En esta sección, aprenderá a navegar la interfaz del Complemento web y configurar los permisos de acceso para uno o todos los dispositivos en la red.

Configuración de los permisos de acceso para Kaspersky Embedded Systems Security para Windows y el servicio de Kaspersky Security

Para configurar los permisos de acceso para un usuario o grupo, debe especificar la cadena del descriptor de seguridad con el lenguaje de definición del descriptor de seguridad (SDDL). Para obtener información detallada sobre la cadena del descriptor de seguridad, visite el sitio web de Microsoft.

Para configurar los permisos de acceso para un usuario o grupo:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Adicional**.
5. Realice una de las siguientes opciones:
   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar las funciones de Kaspersky Embedded Systems Security para Windows.
   - Haga clic en el botón **Configuración** de la subsección **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar el servicio de Kaspersky Security.
6. Agregue un usuario o grupo; para ello, ingrese la cadena del descriptor de seguridad en la ventana **Permisos de acceso de usuario para administrar la aplicación** o **Permisos de acceso de usuario para la administración del servicio de Kaspersky Security**.
7. Haga clic en el botón **Aceptar**.

Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security para Windows

Se puede restringir el acceso a la gestión de aplicaciones y servicios registrados al configurar los permisos del usuario. También se puede establecer la protección con contraseña en Kaspersky Embedded Systems Security para Windows para obtener una protección adicional de las operaciones críticas.

Kaspersky Embedded Systems Security para Windows solicita una contraseña cuando se intenta acceder a las siguientes funciones de la aplicación:

- conectarse a la Consola de la aplicación;
- desinstalar Kaspersky Embedded Systems Security para Windows;
- modificar los componentes de Kaspersky Embedded Systems Security para Windows;

- ejecutar los comandos de la línea de comandos.

La interfaz de Kaspersky Embedded Systems Security para Windows oculta la contraseña especificada en la pantalla. Kaspersky Embedded Systems Security para Windows almacena la contraseña como una suma de control calculada cuando se ingresa la contraseña.

Kaspersky Embedded Systems Security para Windows no verifica la seguridad de la contraseña y no bloquea la entrada de la contraseña después de varios intentos fallidos.

Al crear una contraseña, se recomienda cumplir con las siguientes condiciones:

- La contraseña no contiene el nombre de la cuenta ni el nombre del equipo.
- La contraseña tiene al menos 8 caracteres de longitud.
- La contraseña contiene caracteres que coinciden con al menos tres de las siguientes categorías:
  - Letras latinas mayúsculas (A-Z)
  - Letras latinas minúsculas (a-z)
  - Números (0-9)
  - Símbolos de signo de exclamación (!), signo de dólar ($), signo de numeral (#) y signo de porcentaje (%)

Se puede exportar e importar una configuración de aplicación protegida por contraseña. Un archivo de configuración creado al exportar una configuración de aplicación protegida contiene la suma de control de contraseña y el valor del modificador utilizado para completar la cadena de contraseña.

No cambie la suma de control ni el modificador en el archivo de configuración. La importación de una configuración protegida por contraseña que se ha cambiado manualmente puede provocar que el acceso a la aplicación se bloquee por completo.

Para proteger el acceso a funciones de Kaspersky Embedded Systems Security para Windows:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Configuración de la aplicación**.
5. En la sección **Seguridad y confiabilidad**, haga clic en el botón **Configuración**.
6. En la sección **Configuración de protección con contraseña**, seleccione la casilla de verificación **Aplicar protección con contraseña**.
7. En el campo **Contraseña**, escriba la contraseña que desea usar para proteger el acceso a las funciones de Kaspersky Embedded Systems Security para Windows.
8. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada. Kaspersky Embedded Systems Security para Windows solicitará la contraseña especificada para acceder a las funciones protegidas.

Esta contraseña no se puede recuperar. Si pierde su contraseña, perderá completamente el control de la aplicación. Además, será imposible desinstalar la aplicación del dispositivo protegido.

Puede reiniciar la contraseña en cualquier momento. Para hacerlo, desactive la casilla **Aplicar protección con contraseña** y guarde los cambios. Se deshabilitará la protección con contraseña y se eliminará la suma de control de la contraseña anterior. Repita el proceso de creación de contraseña con una contraseña nueva.

Protección de archivos en tiempo real

Esta sección contiene información acerca de la tarea de Protección de archivos en tiempo real y cómo configurarla.

Acerca de la tarea Protección de archivos en tiempo real

Cuando se está ejecutando la tarea de Protección de archivos en tiempo real, Kaspersky Embedded Systems Security para Windows analiza los siguientes objetos del dispositivo protegido cuando se accede a ellos:

- Objetos del sistema operativo.
- Flujos NTFS de datos alternativos.
- Sectores de inicio y registros de inicio maestro en discos duros locales y dispositivos externos.

Cuando una aplicación escribe o lee un archivo en el dispositivo protegido, Kaspersky Embedded Systems Security para Windows intercepta el archivo, lo analiza en busca de amenazas y, si detecta una amenaza, realiza una acción predeterminada o la acción que usted haya especificado (intenta desinfectar el archivo, lo pasa a Cuarentena o lo elimina). Antes de la desinfección o eliminación, Kaspersky Embedded Systems Security para Windows guarda una copia cifrada del archivo de origen en la carpeta de copia de seguridad.

Kaspersky Embedded Systems Security para Windows también detecta malware para procesos que se ejecutan bajo el Subsistema de Windows para Linux®. Para tales procesos, la tarea de Protección de archivos en tiempo real aplica la acción definida por la configuración vigente.

Acerca del área de protección de la tarea y la configuración de seguridad

De forma predeterminada, la tarea de Protección de archivos en tiempo real protege a todos los objetos del sistema de archivos del dispositivo. Si no hay requisitos de seguridad para proteger todos los objetos del sistema de archivos o si desea excluir cualquier objeto del alcance de la tarea, puede limitar el área de protección.

En la Consola de la aplicación, el área de la protección se muestra como un árbol o lista de recursos de archivos del dispositivo que Kaspersky Embedded Systems Security para Windows puede supervisar. De forma predeterminada, los recursos de archivos en red del dispositivo se muestran como una lista.

En el Complemento de administración, solo está disponible la vista de la lista.

Para ver recursos de archivos en red como un árbol en la Consola de la aplicación,

abra la lista desplegable en la sección superior izquierda de la ventana **Configuración del área de protección** y seleccione **Vista de árbol**.

Ya sea que los recursos de archivos del dispositivo protegido se muestren como una lista o un árbol, los iconos de los nodos tienen los siguientes significados:

☑ El nodo se incluye en el área de protección.

☐ El nodo se excluye del área de protección.

Al menos uno de los nodos secundarios de este nodo se excluye del área de protección o la configuración de seguridad de los nodos secundarios difiere de la configuración del nodo principal (solo para la vista de árbol).

El icono se muestra si están seleccionados todos los nodos secundarios, pero no el principal. En este caso, los cambios en la composición de las carpetas y los archivos del nodo principal se ignoran automáticamente cuando se crea el área de la protección para el nodo secundario seleccionado.

Utilizando la Consola de la aplicación, también puede agregar unidades virtuales al área de protección. Los nombres de los nodos virtuales se muestran en azul.

Configuración de seguridad

La configuración de seguridad de la tarea se puede ajustar como la configuración común para todos los nodos o elementos incluidos en el área de la protección, o como configuraciones diferentes para cada nodo o elemento en el árbol o lista del recurso del archivo del dispositivo.

La configuración de seguridad para el nodo principal seleccionado se aplica automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

La configuración de un área de protección seleccionada se puede realizar mediante uno de los métodos siguientes:

- Seleccionar uno de tres niveles de seguridad predefinidos.
- Configuración manual de las opciones de seguridad para los nodos o elementos seleccionados en el árbol o lista de recursos del archivo (el nivel de seguridad cambia a **Personalizado**).

Es posible guardar un conjunto de opciones de configuración para un nodo o elemento en una plantilla a fin de aplicarlo más tarde a otros nodos o elementos.

Acerca de las áreas virtuales de protección

Kaspersky Embedded Systems Security para Windows puede analizar no solo carpetas y archivos existentes en discos duros y unidades extraíbles, sino también unidades creadas dinámicamente en el dispositivo protegido por distintas aplicaciones y servicios.

Si todos los objetos del dispositivo se incluyen en el área de la protección, estos nodos dinámicos se incluirán automáticamente en dicha área. No obstante, si desea especificar valores especiales para la configuración de seguridad de estos nodos dinámicos o si solo ha seleccionado una parte del dispositivo para su protección, entonces primero deberá crear las unidades, archivos o carpetas virtuales en la Consola de la aplicación para incluirlos en el área de la protección: es decir, especificar el área virtual de protección. Las unidades, archivos y carpetas que se crearon existirán solo en la Consola de la aplicación, pero no en la estructura de archivos del dispositivo protegido.

Si, durante la creación de un área de la protección, se seleccionan todas las subcarpetas o archivos sin seleccionar la carpeta principal, todos los archivos o carpetas virtuales que aparecen en ella no se incluirán automáticamente en el área protegida. Se deben crear "copias virtuales" de ellos en la Consola de la aplicación y agregarlas al área de protección.

Áreas de protección predefinidas

El árbol o la lista de recursos de archivos muestran los nodos a los cuales tiene acceso de lectura según las opciones de seguridad configuradas de Microsoft Windows.

Kaspersky Embedded Systems Security para Windows abarca las Áreas de protección predefinidas siguientes:

- **Discos duros locales**. Kaspersky Embedded Systems Security para Windows protege archivos en los discos duros del dispositivo.
- **Unidades extraíbles**. Kaspersky Embedded Systems Security para Windows protege archivos en dispositivos externos, por ejemplo, unidades extraíbles o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse o excluirse del área de protección.
- **Red**. Kaspersky Embedded Systems Security para Windows analiza los archivos que se escriben en las carpetas de red o que son leídos por las aplicaciones que se ejecutan en el dispositivo. Kaspersky Embedded Systems Security para Windows no protege archivos cuando aplicaciones de otros dispositivos protegidos acceden a ellos.
- **Unidades virtuales**. Las unidades, archivos y carpetas virtuales conectados temporalmente al dispositivo pueden incluirse en el área de la protección, por ejemplo, unidades de clústeres comunes.

De forma predeterminada, puede ver y configurar las áreas de protección predefinidas en el árbol de recursos de archivos en red; también puede agregar áreas de protección predefinidas a la lista de recursos de archivos en red durante su formación en la configuración del área de protección.

De forma predeterminada, el área de protección incluye todas las áreas predefinidas, excepto las unidades virtuales.

Las unidades virtuales creadas mediante un comando SUBST no se muestran en el árbol de recursos de archivo del dispositivo protegido de la Consola de la aplicación. Para incluir objetos de la unidad virtual en el área de la protección, incluya la carpeta del dispositivo asociado con la unidad virtual en el área de la protección.

Las unidades de red conectadas tampoco se mostrarán en la lista de recursos de archivos del dispositivo protegido. Para incluir objetos de unidades de red en el área de la protección, especifique la ruta a la carpeta que corresponde a esta unidad de red en formato UNC.

Acerca de los niveles de seguridad predefinidos

Se puede aplicar uno de los siguientes niveles de seguridad predefinidos para los nodos seleccionados en el árbol de recursos de archivos del dispositivo protegido o la lista de recursos de archivo: **Máximo rendimiento**, **Recomendado** y **Máxima protección**. Cada uno de estos niveles contiene su propio conjunto de configuraciones de seguridad predefinidas (consulte la tabla a continuación).

Máximo rendimiento

El nivel de seguridad **Máximo rendimiento** se recomienda si su red tiene medidas de seguridad adicionales para los dispositivos protegidos, por ejemplo, firewalls y directivas de seguridad existentes, además de usar Kaspersky Embedded Systems Security para Windows en dispositivos protegidos.

Recomendado

El nivel de seguridad **Recomendado** garantiza la mejor combinación de protección e impacto en el rendimiento de los dispositivos protegidos. Los expertos de Kaspersky recomiendan este nivel porque es adecuado para proteger los dispositivos en la mayoría de las redes corporativas. El nivel de seguridad **Recomendado** está configurado de manera predeterminada.

Máxima protección

Se recomienda el nivel de seguridad **Máxima protección** si la red de la organización ha elevado los requisitos de seguridad del dispositivo.

Solo notificar

Se recomienda el nivel de seguridad **Solo notificar** cuando pueden existir muchos equipos infectados en la red corporativa y bloquearlos podría tener un impacto significativo en el funcionamiento de la organización.

Niveles de seguridad predefinidos y valores de configuración correspondientes

Opciones	Nivel de seguridad			
	Máximo rendimiento	**Recomendado**	**Máxima protección**	**Solo notificar**
Protección de objetos	Por extensión	Por formato	Por formato	Por formato
Proteger solo los archivos nuevos y modificados	Habilitado	Habilitado	Deshabilitado	Habilitado
Acción que se realizará con los objetos infectados y otros objetos	Bloquear acceso y desinfectar. Si falla la desinfección, eliminar	Bloquear el acceso y realizar la acción recomendada por los expertos de Kaspersky	Bloquear acceso y desinfectar. Si falla la desinfección, eliminar	Solo notificar
Acción que se realizará con los objetos probablemente infectados	Bloquear acceso y poner en cuarentena	Bloquear el acceso y realizar la acción recomendada por los expertos de Kaspersky	Bloquear acceso y poner en cuarentena	Solo notificar
La denominación "objeto crítico del sistema" hace referencia a aquellos archivos que el sistema operativo y Kaspersky Embedded Systems Security para Windows requieren para funcionar. Estos archivos no se pueden eliminar. Los procesos asociados con dichos objetos no se pueden finalizar.				
Excluir archivos	No	No	No	No
No detectar	No	No	No	No

Detener el análisis si demora más de (s)	60 segundos.	60 segundos.	60 segundos.	60 segundos.
Omitir objetos compuestos de más de (MB)	8192 MB	8192 MB	No definida	8192 MB
Analizar secuencias alternativas de NTFS	Sí	Sí	Sí	Sí
Analizar sectores de inicio del disco y MBR	Sí	Sí	Sí	Sí
Protección de objetos compuestos	• Objetos empaquetados* * Sólo objetos nuevos y modificados	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Sólo objetos nuevos y modificados	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Sólo objetos nuevos y modificados
Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar	No	No	Sí	No

Los parámetros **Protección de objetos**, **Usar la tecnología iChecker**, **Usar la tecnología iSwift** y **Usar el analizador heurístico** no se incluyen en la configuración de los niveles de seguridad predefinidos. Si modifica la configuración de seguridad de **Protección de objetos**, **Usar la tecnología iChecker**, **Usar la tecnología iSwift** o **Usar el analizador heurístico** después de seleccionar uno de los niveles de seguridad predefinidos, el nivel de seguridad que ha seleccionado no cambiará.

Extensiones de archivo analizadas de forma predeterminada en la tarea de Protección de archivos en tiempo real

De manera predeterminada, Kaspersky Embedded Systems Security para Windows analiza los archivos con las siguientes extensiones:

- *386;*
- *acm;*
- *ade, adp;*

- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *.exe*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*

- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*

- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*

- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

Configuración de la tarea Protección de archivos en tiempo real predeterminada

De manera predeterminada, la tarea de Protección de archivos en tiempo real utiliza la configuración descrita en la siguiente tabla. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea Protección de archivos en tiempo real

Configuración	Valor predeterminado	Descripción
Área de protección	El dispositivo protegido completo, excluidas las unidades virtuales.	Utilice esta opción para cambiar el área de protección.
Configuración de seguridad	La configuración común para toda el área de protección corresponde al nivel de seguridad **Recomendado**.	Para los nodos seleccionados en la lista o el árbol de recursos de archivos del dispositivo protegido, puede realizar lo siguiente: • Seleccionar un nivel de seguridad predefinido diferente • Cambiar manualmente la configuración de seguridad Puede guardar un grupo de opciones de seguridad para un nodo seleccionado como una plantilla y usarla más tarde en un nodo diferente.
Modo de protección de objetos	**Modo inteligente**	Utilice esta opción para seleccionar el modo de protección, es decir, definir el tipo de intentos de acceso para los que Kaspersky Embedded Systems Security analiza objetos.
Analizador heurístico	Se aplica el nivel de seguridad **Medio**.	Se puede habilitar o deshabilitar el Analizador heurístico y se puede configurar el nivel de análisis.
Aplicar la Zona de confianza	Aplicado.	Lista general de exclusiones que se pueden utilizar en tareas seleccionadas.
Usar KSN para protección	Aplicado.	Utilice esta opción para mejorar la protección del dispositivo con el servicio en la nube de Kaspersky Security Network (disponible si se acepta la Declaración de KSN).
Programación de inicio de tareas	Al inicio de la aplicación.	Utilice esta opción para configurar el inicio de la tarea programada.

Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa	No aplicado.	Utilice esta opción para bloquear la sesión actual y agregar la IP del host o el LUID del host hacia el cual se detectó actividad maliciosa en la sección Depósito de hosts bloqueados.
Iniciar análisis de áreas críticas al detectar infección activa	Aplicado.	Cuando se detecta una infección activa, Kaspersky Embedded Systems Security para Windows crea e inicia una tarea temporal de Análisis de áreas críticas.

Gestión de la tarea Protección de archivos en tiempo real a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración de la tarea para uno o todos los dispositivos protegidos en la red.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real

Para abrir la configuración de la tarea Protección de archivos en tiempo real a través de la directiva Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Protección del equipo en tiempo real**.
6. Haga clic en **Configuración** en la subsección **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección de archivos en tiempo real**.

Si un dispositivo protegido es administrado por una directiva activa de Kaspersky Security Center y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede editar a través de la Consola de la aplicación.

Cómo abrir la configuración de la tarea Protección de archivos en tiempo real

Para abrir la ventana de configuración de la tarea Protección de archivos en tiempo real para un solo dispositivo en red:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del dispositivo protegido.
   - Abra el menú contextual del nombre del dispositivo protegido y seleccione el elemento **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
5. En la sección **Tareas**, seleccione la tarea **Protección de archivos en tiempo real**.
6. Haga clic en el botón **Propiedades**.
   Se abre la ventana **Propiedades: Protección de archivos en tiempo real**.

Configuración de la tarea Protección de archivos en tiempo real

Para establecer la configuración de la tarea Protección de archivos en tiempo real:

1. Abra la ventana **Protección de archivos en tiempo real**.
2. Defina los siguientes valores de configuración de tarea:
   - En la pestaña **General**:
     - Parámetros de interceptación
     - **Analizador heurístico**
     - **Integración con otros componentes**
   - En la pestaña **Administración de tareas**:
     - Ajustes para programar el inicio de la tarea.
3. Seleccione la pestaña **Área de protección** y haga lo siguiente:
   - Haga clic en el botón **Agregar** o **Editar** para editar el área de protección.

- En la ventana que se abre, elija lo que desea incluir en el área de protección de la tarea:
  - **Área predefinida**
  - **Disco, carpeta o ubicación de red**
  - **Archivo**
- Seleccione uno de los niveles de seguridad predefinidos o configure manualmente las opciones de protección.

4. Haga clic en el botón **Aceptar** de la ventana **Protección de archivos en tiempo real**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La fecha y hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Selección del modo de protección

En la tarea Protección de archivos en tiempo real, se puede seleccionar el modo de protección. La sección **Modo de protección de objetos** le permite especificar el tipo de intentos de acceso para los que Kaspersky Embedded Systems Security para Windows analiza objetos.

El valor de la configuración **Modo de protección de objetos** se aplica a toda el área de la protección especificada en la tarea. No es posible especificar valores diferentes en el parámetro para nodos individuales dentro del área de protección.

Para seleccionar el modo de protección:

1. Abra la ventana **Protección de archivos en tiempo real**.
2. En la ventana que se abre, abra la pestaña **General** y seleccione el modo de protección que desea configurar:
   - **Modo inteligente**
   - **Al acceder y realizar modificaciones**
   - **Al acceder**
   - **Durante ejecución**
   - **Análisis detallado de los procesos que se iniciarán (la ejecución del proceso se bloqueará hasta que finalice el análisis)**
3. Haga clic en el botón **Aceptar**.

Se aplicará el modo de protección seleccionado.

Configuración del Analizador heurístico e integración con otros componentes de la aplicación

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

Para configurar el Analizador heurístico y la integración con otros componentes:

1. Abra la ventana **Protección de archivos en tiempo real**.
2. En la pestaña **General**, desactive o seleccione la casilla de verificación **Usar el analizador heurístico**.
3. Si es necesario, ajuste el nivel de análisis con el control deslizante.
4. En la sección **Integración con otros componentes**, configure las siguientes opciones:
   - Seleccione o desactive la casilla de verificación **Aplicar zona de confianza**.
   - Seleccione o desactive la casilla de verificación **Usar KSN para protección**.

     La casilla de verificación **Enviar datos sobre archivos analizados** debe estar seleccionada en la configuración de la tarea Uso de KSN.

   - Seleccione o desactive la casilla **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa**.
   - Seleccione o desactive la casilla **Iniciar análisis de áreas críticas al detectar infección activa**.
5. Haga clic en el botón **Aceptar**.

La configuración de la tarea establecida se aplica inmediatamente a una tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Tareas de programación

Puede programar las tareas personalizadas y las tareas locales del sistema en la Consola de la aplicación. No puede programar tareas de grupo en la Consola de la aplicación.

Para programar tareas de grupo mediante el Complemento de administración, realice lo siguiente:

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Seleccione el grupo al cual pertenece el dispositivo protegido.
3. En el panel de detalles, seleccione la pestaña **Tareas**.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea.
   - Abra el menú contextual del nombre de la tarea y seleccione el elemento Propiedades.
5. Seleccione la sección **Programación**.

6. En el bloque **Configuración de programación**, seleccione la casilla de verificación **Ejecutar según programación**.

Los campos con la configuración de programación para las tareas análisis a pedido y actualización no estarán disponibles si una directiva de Kaspersky Security Center bloquea la programación de estas tareas.

7. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:

a. En la lista **Frecuencia**, seleccione uno de los siguientes valores:

- **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
- **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
- **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
- **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security para Windows.
- **Tras actualizarse las bases de datos**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

c. En el campo **Fecha de inicio**, especifique la fecha de inicio de la programación.

Luego de programar la hora de inicio, fecha y frecuencia de la tarea, se muestra el tiempo estimado hasta el próximo inicio.

Vaya a la pestaña **Programación** y abra la ventana **Configuración de tareas**. En el campo **Próximo inicio** en la parte superior de la ventana, se muestra la hora de inicio estimada. Cada vez que abre la ventana, la hora estimada de inicio se actualiza y se muestra.

El campo **Próximo inicio** muestra el valor **Bloqueado por directiva** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas locales del sistema programadas.

8. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos.

- En la sección **Configuración de detención de tareas**:

a. Seleccione la casilla de verificación **Duración** y, en los campos a la derecha, ingrese el número máximo de horas y minutos de la ejecución de la tarea.

b. Seleccione la casilla de verificación **Pausar de** y, en los campos a la derecha, introduzca los valores de inicio y final de un intervalo de tiempo inferior a 24 horas durante el cual se detendrá la ejecución de la

tarea.

- En el bloque **Configuración avanzada**:

  a. Seleccione la casilla de verificación **Cancelar programación desde** y especifique la fecha desde la cual la programación dejará de aplicar.

  b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.

  c. Seleccione la casilla de verificación **Aleatorizar la hora de inicio de la tarea usando un margen de** y especifique el valor en minutos.

9. Haga clic en el botón **Aceptar**.

10. Haga clic en el botón **Aplicar** para guardar la configuración del inicio de la tarea.

Si desea establecer la configuración de la aplicación para una sola tarea con Kaspersky Security Center, consulte la sección "Configuración de tareas locales en la ventana de configuración de la aplicación de Kaspersky Security Center".

Creación y configuración del área de protección de la tarea

Para crear y configurar el área de protección de la tarea a través de Kaspersky Security Center:

1. Abra la ventana **Protección de archivos en tiempo real**.

2. Seleccione la pestaña **Área de protección**.

   Todos los elementos ya protegidos por la tarea se enumeran en la tabla **Área de protección**.

3. Haga clic en el botón **Agregar** para agregar el nuevo elemento a la lista.

   Se abre la ventana **Agregar objetos al área de protección**.

4. Seleccione un tipo de objeto para agregarlo a un área de protección:

   - **Área predefinida** para incluir una de las áreas predefinidas en el área de la protección en el dispositivo. A continuación, en la lista desplegable, seleccione un área de la protección deseada.

   - **Disco, carpeta o ubicación de red** para incluir una unidad individual, carpeta o un objeto de red en el área de la protección. A continuación, seleccione el área de la protección deseada con un clic en el botón **Examinar**.

   - **Archivo** para incluir un archivo particular en el área de la protección. A continuación, seleccione el área de la protección deseada con un clic en el botón **Examinar**.

     No puede agregar un objeto a un área de la protección si ya se agregó como una exclusión de un área de la protección.

5. Para excluir elementos individuales del área de protección, desactive las casillas al lado de los nombres de estos elementos o siga estos pasos:

a. Abra el menú contextual del área de la protección haciendo clic en él con el botón derecho del mouse.

b. En el menú contextual, seleccione la opción **Agregar exclusión**.

c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del área de la protección siguiendo el procedimiento utilizado al añadir un objeto al área de la protección.

6. Para modificar el área de la protección o una exclusión existente, seleccione la opción **Editar área** en el menú contextual del área de la protección deseada.

7. Para ocultar un área de la protección agregada anteriormente o una exclusión en la lista de recursos de archivos en red, seleccione la opción **Eliminar área** en el menú contextual del área de la protección deseada.

   El área de la protección se elimina del área de la tarea de Protección de archivos en tiempo real cuando se elimina de la lista de recursos de archivos en red.

8. Haga clic en el botón **Aceptar**.

Se cierra la ventana Configuración del área de protección. Se guarda la configuración especificada.

La tarea **Protección de archivos en tiempo real** puede iniciarse solo si al menos uno de los nodos de recursos de archivos del dispositivo se ha incluido en un área de protección.

Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido

Se puede aplicar uno de los siguientes tres niveles de seguridad predefinidos a un nodo seleccionado en la lista de recursos de archivos del dispositivo: **Máximo rendimiento**, **Recomendado** y **Máxima protección**.

Para seleccionar uno de los niveles de seguridad predefinidos:

1. Abra la ventana **Propiedades: Protección de archivos en tiempo real**.

2. Seleccione la pestaña **Área de protección**.

3. En la lista del dispositivo protegido, seleccione un elemento incluido en el área de protección para configurar un nivel de seguridad predefinido.

4. Haga clic en el botón **Configurar**.

   La ventana **Configuración de Protección de archivos en tiempo real** se abre.

5. En la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se deba aplicar.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.

6. Haga clic en el botón **Aceptar**.

7. Haga clic en el botón **Aceptar** de la ventana **Propiedades: Protección de archivos en tiempo real**.

   La configuración de la tarea se guarda y se aplica inmediatamente a una tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración manual de las opciones de seguridad

De manera predeterminada, la tarea de Protección de archivos en tiempo real utiliza la configuración de seguridad común para toda el área de protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área de la protección o como valores diferentes para los elementos individuales de la lista de recursos de archivos del dispositivo o nodos del árbol.

Para configurar las opciones de seguridad del nodo seleccionado en forma manual:

1. Abra la ventana **Protección de archivos en tiempo real**.
2. En la pestaña **Área de protección**, seleccione el nodo cuya configuración de seguridad desea configurar y hacer clic en **Configurar**.

   La ventana **Configuración de Protección de archivos en tiempo real** se abre.
3. En la pestaña **Nivel de seguridad**, haga clic en el botón **Configuración** para personalizar la configuración.
4. Se pueden configurar los valores de seguridad personalizados del nodo seleccionado de acuerdo con sus requisitos:
   - Configuración general
   - Acciones
   - Rendimiento
5. Haga clic en el botón **Aceptar** de la ventana **Protección de archivos en tiempo real**.

Se guarda la nueva configuración del área de la protección.

Configuración de las opciones generales de tareas

Para configurar las opciones de seguridad generales de la tarea Protección de archivos en tiempo real:

1. Abra la ventana **Configuración de Protección de archivos en tiempo real**.
2. Abra la pestaña **General**.
3. En el bloque **Protección de objetos**, especifique los tipos de objetos que desea incluir en el área de protección:
   - **Todos los objetos**
   - **Objetos analizados según su formato**
   - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
   - **Objetos analizados según la lista de extensiones especificada**

- Analizar sectores de inicio del disco y MBR
- Analizar secuencias alternativas de NTFS

4. En el cuadro de grupo **Rendimiento**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.

   Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En el bloque **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área de protección:

   - **Todos** / **Solo nuevos archivos comprimidos**
   - **Todos** / **Solo nuevos archivos SFX**
   - **Todos** / **Solo nuevas bases de datos de correo electrónico**
   - **Todos** / **Solo nuevos objetos empaquetados**
   - **Todos** / **Solo nuevo correo electrónico simple**
   - **Todos** / **Solo nuevos objetos OLE incorporados**

6. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

Para configurar acciones en objetos infectados y otros objetos detectados durante la tarea de Protección de archivos en tiempo real:

1. Abra la ventana **Configuración de Protección de archivos en tiempo real**.
2. Seleccione la pestaña **Acciones**.
3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:

   - **Solo notificar**.
   - **Bloquear acceso**.
   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:

     - **Desinfectar**.
     - **Desinfectar; si falla la desinfección, eliminar**Si falla la desinfección, eliminar
     - **Eliminar**.

- Recomendado.

4. Seleccione la acción a realizar en los objetos probablemente infectados:

   - Solo notificar.
   - Bloquear acceso.
   - **Realizar acción adicional**

     Seleccione la acción en la lista desplegable:

     - **Poner en cuarentena**.
     - Eliminar.
     - Recomendado.

5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

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

   c. En la ventana que se abre, seleccione una acción primaria y una acción secundaria (a realizarse en caso de que falle la acción primaria) para cada tipo de objeto detectado.

   d. Haga clic en el botón **Aceptar**.

6. Seleccione la acción a realizar en archivos compuestos no modificables: seleccione o desactive la casilla de verificación **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

7. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

Para establecer la configuración de rendimiento para la tarea Protección de archivos en tiempo real:

1. Abra la ventana **Configuración de Protección de archivos en tiempo real**.
2. Seleccione la pestaña **Rendimiento**.
3. En el bloque **Exclusiones**:

   - Desactive o seleccione la casilla de verificación **Excluir archivos**.
   - Borre o seleccione la casilla de verificación **No detectar**.
   - Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.

4. En el bloque **Configuración avanzada**:

- Detener el análisis si demora más de (s)
- Omitir objetos compuestos de más de (MB)
- Usar la tecnología iSwift
- Usar la tecnología iChecker

Administración de la tarea Protección de archivos en tiempo real a través de la Consola de la aplicación

En esta sección, aprenderá a navegar por la interfaz de la Consola de la aplicación y a definir la configuración de la tarea en un dispositivo protegido.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la tarea Protección de archivos en tiempo real

Para abrir la ventana de la configuración de la tarea general:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.
3. Haga clic en el vínculo **Propiedades** del panel de resultados.
   Aparece la ventana **Configuración de tareas**.

Cómo abrir la configuración del área de la tarea Protección de archivos en tiempo real

Para abrir la ventana de configuración del área de protección de la tarea Protección de archivos en tiempo real:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.
3. Haga clic en el vínculo **Configurar el área de protección** en el panel de resultados.
   Se abre la ventana **Configuración del área de protección**.

Configuración de la tarea Protección de archivos en tiempo real

Para establecer la configuración de la tarea Protección de archivos en tiempo real:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **General**, configure la siguiente configuración de tarea:
   - Modo de protección de objetos
   - **Analizador heurístico**
   - **Integración con otros componentes**
3. En las pestañas **Programación** y **Avanzado**, especifique las opciones de inicio programado.
4. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

   La configuración modificada se guarda.
5. En el panel de resultados del nodo **Protección de archivos en tiempo real**, haga clic en el vínculo **Configurar el área de protección**.
6. Haga lo siguiente:
   - En el árbol o lista de los recursos de archivos del dispositivo, seleccione los nodos o elementos que desea incluir en el área de protección de la tarea.
   - Seleccione uno de los niveles de seguridad predefinidos o ajuste la configuración de protección del objeto manualmente.
7. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La fecha y hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Selección del modo de protección

En la tarea Protección de archivos en tiempo real, se puede seleccionar el modo de protección. La sección **Modo de protección de objetos** le permite especificar el tipo de intentos de acceso para los que Kaspersky Embedded Systems Security para Windows analiza objetos.

El valor de la configuración **Modo de protección de objetos** se aplica a toda el área de la protección especificada en la tarea. No es posible especificar valores diferentes en el parámetro para nodos individuales dentro del área de protección.

Para seleccionar el modo de protección:

1. Abra la ventana **Configuración de tareas**.

2. En la ventana que se abre, abra la pestaña **General** y seleccione el modo de protección que desea configurar:

   - **Modo inteligente**
   - **Al acceder y realizar modificaciones**
   - **Al acceder**
   - **Durante ejecución**
   - **Análisis detallado de los procesos que se iniciarán (la ejecución del proceso se bloqueará hasta que finalice el análisis)**

3. Haga clic en el botón **Aceptar**.

Se aplicará el modo de protección seleccionado.

Configuración del Analizador heurístico e integración con otros componentes de la aplicación

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

Para configurar el Analizador heurístico y la integración con otros componentes:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **General**, desactive o seleccione la casilla de verificación **Usar el analizador heurístico**.
3. Si es necesario, ajuste el nivel de análisis con el control deslizante.
4. En la sección **Integración con otros componentes**, configure las siguientes opciones:

   - Seleccione o desactive la casilla de verificación **Aplicar la Zona de confianza**.

     Haga clic en el vínculo **Zona de confianza** para abrir la configuración de la Zona de confianza.

   - Seleccione o desactive la casilla de verificación **Usar KSN para protección**.

     La casilla de verificación **Enviar datos sobre archivos analizados** debe estar seleccionada en la configuración de la tarea Uso de KSN.

   - Seleccione o desactive la casilla de verificación **Bloquear acceso a recursos compartidos en la red para las sesiones que muestran actividad maliciosa**.
   - Seleccione o desactive la casilla **Iniciar análisis de áreas críticas al detectar infección activa**.

5. Haga clic en el botón **Aceptar**.

Se aplica la configuración reciente.

Configuración de las opciones de programación de tareas

En la Consola de la aplicación, puede programar el tiempo de inicio de tareas locales del sistema y tareas personalizadas. Sin embargo, no puede programar el tiempo de inicio de tareas de grupo.

Para programar una tarea, realice lo siguiente:

1. Abra el menú contextual de la tarea que quiere programar.
2. Seleccione **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
3. En la ventana que se abre, en la pestaña **Programación**, seleccione la casilla de verificación **Ejecutar según programación**.
4. Siga estos pasos para especificar la configuración de programación:

   a. En el menú desplegable **Frecuencia**, seleccione uno de los siguientes:

   - **Horaria**: para ejecutar la tarea con una frecuencia medida en horas; indique el número de horas a través del campo **Cada<número>hora(s)**.
   - **Diaria**: para ejecutar la tarea con una frecuencia medida en días; indique el número de días a través del campo **Cada<número>día(s)**.
   - **Semanal**: para ejecutar la tarea con una frecuencia medida en semanas; indique el número de semanas a través del campo **Cada<número>semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
   - **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security para Windows.
   - **Tras actualizarse las bases de datos**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

   b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

   c. En el campo **Fecha de inicio**, especifique la fecha para iniciar la tarea por primera vez.

   Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La hora estimada del próximo inicio de la tarea se actualizará y mostrará cada vez que abra la ventana **Configuración de tareas** en la pestaña **Programación**.

   El campo **Próximo inicio** muestra el valor **Bloqueado por directiva** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas locales del sistema programadas.
5. Use la pestaña **Avanzado** para especificar la siguiente configuración de programación:

   - En la sección **Configuración de detención de tareas**:

a. Seleccione la casilla de verificación **Duración**. En los campos a la derecha, ingrese la duración máxima de la tarea en horas y minutos.

b. Seleccione la casilla de verificación **Pausar de**. En los campos a la derecha, especifique cuándo pausar y reanudar la tarea (menos de 24 horas).

- En el bloque **Configuración avanzada**:

a. Seleccione la casilla de verificación **Cancelar programación desde** y especifique la fecha de finalización de la programación de la tarea.

b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para iniciar las tareas omitidas.

c. Seleccione la casilla de verificación **Aleatorizar el inicio de la tarea usando un margen de** y especifique el valor en minutos.

6. Haga clic en el botón **Aceptar**.

Se guarda la configuración de programación de la tarea.

Creación del área de protección

Esta sección proporciona instrucciones sobre la creación y la administración de un área de protección en la tarea Protección de archivos en tiempo real.

Configuración de la visualización para recursos de archivos en red

Para seleccionar la visualización para recursos de archivos en red durante la configuración del área de protección:

1. Abra la ventana **Configuración del área de protección**.

2. Abra la lista desplegable en la sección superior izquierda de la ventana y seleccione una de las siguientes opciones:

   - Seleccione la opción **Vista de árbol** para ver los recursos de archivos en red como un árbol.

   - Seleccione la opción **Vista de lista** para ver los recursos de archivos en red como una lista.

   De forma predeterminada, los recursos de archivos en red del dispositivo protegido se muestran en un modo de vista de lista.

3. Haga clic en el botón **Guardar**.

Creación del área de protección

El procedimiento para crear el alcance de la tarea Protección de archivos en tiempo real depende de la vista de recursos de archivos en red seleccionada. Puede configurar la visualización de los recursos de archivos en red como un árbol o como una lista (vista predeterminada).

Para aplicar los nuevos ajustes del área de protección a la tarea, se debe reanudar la tarea Protección de archivos en tiempo real.

Para crear un área de la protección con el árbol de recursos de archivos en red:

1. Abra la ventana **Configuración del área de protección**.
2. En la sección izquierda de la ventana, abra el árbol de recursos de archivos en red para ver todos los nodos y nodos secundarios.
3. Haga lo siguiente:
   - Para excluir nodos individuales del área de protección, desactive las casillas de verificación al lado de los nombres de estos nodos.
   - Para incluir nodos individuales al área de protección, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
     - Si desea incluir todas las unidades de un mismo tipo en el área de protección, seleccione la casilla adyacente al tipo de unidades que corresponda. Por ejemplo, para incluir todas las unidades extraíbles de un dispositivo, seleccione la casilla **Unidades extraíbles**.
     - Si desea incluir un disco individual de un determinado tipo en el área de protección, expanda el nodo que contiene la lista de unidades de este tipo y seleccione la casilla junto al nombre de la unidad requerida. Por ejemplo, para seleccionar la unidad extraíble "F:", expanda el nodo **Unidades extraíbles** y seleccione la casilla correspondiente a la unidad **F:**.
     - Si desea incluir solamente una carpeta o un archivo de la unidad, seleccione la casilla de verificación ubicada al lado del nombre de esa carpeta o de ese archivo.
4. Haga clic en el botón **Guardar**.

Se cierra la ventana **Configuración del área de protección**. Se guarda la configuración especificada.

Para crear un área de protección utilizando la lista de recursos de archivos en red:

1. Abra la ventana **Configuración del área de protección**.
2. Para incluir nodos individuales al área de protección, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
   a. Abra el menú contextual del área de la protección haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual del botón, seleccione **Agregar área de protección**.
   c. En la ventana **Agregar área de protección**, seleccione un tipo de objeto para agregarlo al área de protección:
      - **Área predefinida** para incluir una de las áreas predefinidas en el área de la protección en el dispositivo. A continuación, en la lista desplegable, seleccione un área de la protección deseada.
      - **Disco, carpeta o ubicación de red** para incluir una unidad individual, carpeta o un objeto de red en el área de la protección. A continuación, seleccione el área deseada con un clic en el botón **Examinar**.

- **Archivo** para incluir un archivo particular en el área de la protección. A continuación, seleccione el área deseada con un clic en el botón **Examinar**.

No puede agregar un objeto a un área de la protección si ya se agregó como una exclusión de un área de la protección.

3. Para excluir nodos individuales del área de protección, desactive las casillas al lado de los nombres de estos nodos o siga estos pasos:

   a. Abra el menú contextual del área de la protección haciendo clic en él con el botón derecho del mouse.

   b. En el menú contextual, seleccione la opción **Agregar exclusión**.

   c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del área de la protección siguiendo el procedimiento utilizado al añadir un objeto al área de la protección.

4. Para modificar el área de la protección o una exclusión existente, seleccione la opción **Editar área** en el menú contextual del área de la protección deseada.

5. Para ocultar un área de la protección agregada anteriormente o una exclusión en la lista de recursos de archivos en red, seleccione la opción **Eliminar de la lista** en el menú contextual del área de la protección deseada.

   El área de la protección se elimina del área de la tarea de Protección de archivos en tiempo real cuando se elimina de la lista de recursos de archivos en red.

6. Haga clic en el botón **Guardar**.

Se cierra la ventana **Configuración del área de protección**. Se guarda la configuración especificada.

La tarea Protección de archivos en tiempo real puede iniciarse solo si al menos uno de los nodos de recursos de archivos del dispositivo se incluye en un área de la protección.

Si se especifica un área de la protección compleja, por ejemplo, si se especifican valores de seguridad diferentes para la configuración de varios nodos en el árbol de recursos de archivos del dispositivo, puede provocar cierta ralentización en el análisis de objetos al acceder a ellos.

Inclusión de objetos de red en el área de la protección

Se pueden agregar unidades, carpetas o archivos en red en el área de protección mediante la especificación de su ruta en formato UNC (convención de nomenclatura universal).

Puede analizar carpetas de la red con la cuenta de sistema.

Para agregar una ubicación de la red al área de protección:

1. Abra la ventana Configuración del área de protección.

2. Abra la lista desplegable en la parte superior izquierda de la ventana y seleccione **Vista de árbol**.
3. En el menú contextual del nodo **Red**:
   - Seleccione **Agregar carpeta de red** si desea agregar una carpeta de red al área de protección.
   - Seleccione **Agregar archivo de red** si desea agregar un archivo en red al área de protección.
4. Ingrese la ruta a la carpeta o archivo de red en formato UNC.
5. Presione la tecla **INTRO**.
6. Seleccione la casilla de verificación junto al objeto de red agregado recientemente para incluirlo en el área de protección.
7. Si es necesario, cambie la configuración de seguridad para el objeto de red agregado.
8. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea especificada.

Creación de área virtual de protección

Se puede ampliar el área del análisis o protección si se agregan unidades virtuales, carpetas o archivos individuales solo si el área del análisis o protección se presenta como un árbol de recursos de archivo.

Para agregar una unidad virtual al área de protección:

1. Abra la ventana **Configuración del área de protección**.
2. Abra la lista desplegable en la parte superior izquierda de la ventana y seleccione **Vista de árbol**.
3. Abra el menú contextual del nodo **Unidades virtuales**.
4. Seleccione la opción **Agregar unidad virtual**.
5. En la lista de nombres disponibles, seleccione el nombre de la unidad virtual que se está creando.
6. Seleccione la casilla junto a la unidad para incluir la unidad en el área de la protección.
7. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Se guarda la configuración especificada.

Para agregar un archivo o carpeta virtual al área de protección:

1. Abra la ventana **Configuración del área de protección**.
2. Abra la lista desplegable en la parte superior izquierda de la ventana y seleccione **Vista de árbol**.
3. Abra el menú contextual de la unidad virtual a la cual desea agregar una carpeta o un archivo y seleccione una de las opciones siguientes:

- **Agregar carpeta virtual** si desea agregar una carpeta virtual al área de la protección.
- **Agregar archivo virtual** si desea agregar un archivo virtual al área de la protección.

4. En el campo de entrada, especifique el nombre de la carpeta o el archivo.
5. En la línea que contiene el nombre de la carpeta o el archivo creado, seleccione la casilla de verificación para incluir la carpeta o el archivo en el área de protección.
6. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea especificada.

Configuración manual de las opciones de seguridad

De manera predeterminada, las tareas de Protección del equipo en tiempo real utilizan la configuración de seguridad para toda el área de protección. Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área de la protección o como valores diferentes para los elementos individuales de la lista de recursos de archivos del dispositivo o nodos del árbol.

Al trabajar con el árbol de recursos de archivos del dispositivo protegido, las opciones de seguridad que se configuran para el nodo principal seleccionado se aplican automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

Para configurar las opciones de seguridad manualmente:

1. Abra la ventana **Configuración del área de protección**.
2. En la sección de la ventana izquierda, seleccione el nodo para configurar las opciones de seguridad.

   Puede aplicar una plantilla de configuración de seguridad predefinida a un nodo o elemento seleccionado en el área de protección.

   En la parte izquierda de la ventana, puede seleccionar la vista de recursos de archivos en red, crear un alcance de protección o crear un área virtual de protección.
3. En la parte derecha de la ventana, realice una de las siguientes acciones:
   - En la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad a aplicar.
   - En las siguientes pestañas, configure los valores de seguridad del nodo o elemento seleccionado de acuerdo con sus requisitos:
     - **General**
     - **Acciones**
     - **Rendimiento**
4. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Se guarda la nueva configuración del área de la protección.

Selección de los niveles de seguridad predefinidos para la tarea Protección de archivos en tiempo real

Se puede aplicar uno de los siguientes tres niveles de seguridad predefinidos a un nodo seleccionado en el árbol o la lista de recursos de archivos del dispositivo protegido: **Máximo rendimiento**, **Recomendado** y **Máxima protección**.

Para seleccionar uno de los niveles de seguridad predefinidos:

1. Abra la ventana **Configuración del área de protección**.
2. En la lista o árbol de recursos de archivos en red del dispositivo protegido, seleccione un nodo o elemento para establecer el nivel de seguridad predefinido.
3. Asegúrese de que el nodo o elemento seleccionado se incluya en el área de protección.
4. En la parte derecha de la ventana, en la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se aplicará.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.
5. Haga clic en el botón **Guardar**.

   La configuración de la tarea se guarda y se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración de las opciones generales de tareas

Para configurar las opciones de seguridad generales de la tarea Protección de archivos en tiempo real:

1. Abra la ventana **Configuración del área de protección**.
2. Abra la pestaña **General**.
3. En la sección **Protección de objetos**, especifique los objetos que desea incluir en el área de protección:
   - **Todos los objetos**
   - **Objetos analizados según su formato**
   - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
   - **Objetos analizados según la lista de extensiones especificada**
   - **Analizar sectores de inicio del disco y MBR**
   - **Analizar secuencias alternativas de NTFS**
4. En el cuadro de grupo **Rendimiento**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.

Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En el bloque **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área de protección:
   - **Todos** / **Solo nuevos archivos comprimidos**
   - **Todos** / **Solo nuevos archivos SFX**
   - **Todos** / **Solo nuevas bases de datos de correo electrónico**
   - **Todos** / **Solo nuevos objetos empaquetados**
   - **Todos** / **Solo nuevo correo electrónico simple**
   - **Todos** / **Solo nuevos objetos OLE incorporados**
6. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

Para configurar acciones en objetos infectados y otros objetos detectados durante la tarea de Protección de archivos en tiempo real:

1. Abra la ventana **Configuración del área de protección**.
2. Seleccione la pestaña **Acciones**.
3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
   - **Solo notificar**.
   - **Bloquear acceso**.
   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:
     - **Desinfectar**.
     - **Desinfectar; si falla la desinfección, eliminar**.
     - **Eliminar**.
     - **Recomendado**.
4. Seleccione la acción a realizar en los objetos probablemente infectados:
   - **Solo notificar**.
   - **Bloquear acceso**.

- **Realizar acción adicional**

  Seleccione la acción en la lista desplegable:

  - **Poner en cuarentena**.
  - **Eliminar**.
  - **Recomendado**.

5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

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

   c. En la ventana que se abre, seleccione una acción primaria y una acción secundaria (a realizarse en caso de que falle la acción primaria) para cada tipo de objeto detectado.

   d. Haga clic en el botón **Aceptar**.

6. Seleccione la acción a realizar en archivos compuestos no modificables: seleccione o desactive la casilla de verificación **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

7. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

Para establecer la configuración de rendimiento para la tarea Protección de archivos en tiempo real:

1. Abra la ventana **Configuración del área de protección**.
2. Seleccione la pestaña **Rendimiento**.
3. En el bloque **Exclusiones**:
   - Desactive o seleccione la casilla de verificación **Excluir archivos**.
   - Borre o seleccione la casilla de verificación **No detectar**.
   - Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.
4. En el bloque **Configuración avanzada**:
   - **Detener el análisis si demora más de (s)**
   - **Omitir objetos compuestos de más de (MB)**
   - **Usar la tecnología iSwift**
   - **Usar la tecnología iChecker**

Estadísticas de la tarea de Protección de archivos en tiempo real

Mientras se ejecuta la tarea de Protección de archivos en tiempo real, puede ver información detallada en tiempo real sobre la cantidad de objetos procesados por Kaspersky Embedded Systems Security para Windows desde que se inició la tarea.

Para ver las estadísticas de la tarea Protección de archivos en tiempo real:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.

   Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de resultados del nodo seleccionado.

Se puede ver la información sobre los objetos procesados por Kaspersky Embedded Systems Security para Windows desde que se inició (consulte la tabla a continuación).

Estadísticas de la tarea de Protección de archivos en tiempo real

Campo	Descripción
Detectado	Número de objetos detectados por Kaspersky Embedded Systems Security para Windows. Por ejemplo, si Kaspersky Embedded Systems Security para Windows detecta un objeto malicioso en cinco archivos, el valor de este campo aumenta en uno.
Objetos infectados y otros objetos detectados	La cantidad de objetos que Kaspersky Embedded Systems Security para Windows encontró y clasificó como infectados, o la cantidad encontrada de archivos de software legítimos que los intrusos pueden usar para dañar su dispositivo o sus datos personales.
Objetos probablemente infectados detectados	Cantidad de objetos probablemente infectados encontrados por Kaspersky Embedded Systems Security para Windows.
Objetos no desinfectados	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows no desinfectó debido a los siguientes motivos: • El tipo de objeto detectado no se puede desinfectar. • Se produjo un error durante la desinfección.
Objetos que no se pasaron a Cuarentena	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows intentó poner en cuarentena sin éxito, por ejemplo, debido a espacio insuficiente en el disco.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows intentó eliminar sin éxito debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos no analizados	Cantidad de objetos en el área de la protección que Kaspersky Embedded Systems Security para Windows no pudo analizar debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos sin copia de seguridad	Cantidad de objetos cuyas copias Kaspersky Embedded Systems Security para Windows intentó guardar sin éxito en Copia de seguridad; por ejemplo, debido a espacio insuficiente en el disco.

Errores de procesamiento	Cantidad de objetos en los que se produjo un error durante su procesamiento.
Objetos desinfectados	Número de objetos desinfectados por Kaspersky Embedded Systems Security para Windows.
Pasados a Cuarentena	Número de objetos pasados a Cuarentena por Kaspersky Embedded Systems Security para Windows.
Pasados a Copia de seguridad	Cantidad de objetos cuyas copias Kaspersky Embedded Systems Security para Windows guardó en Copia de seguridad.
Objetos eliminados	Número de objetos eliminados por Kaspersky Embedded Systems Security para Windows.
Objetos protegidos con contraseña	Cantidad de objetos (por ejemplo, archivos) que Kaspersky Embedded Systems Security para Windows omitió porque estaban protegidos por contraseña.
Objetos dañados	Cantidad de objetos omitidos por Kaspersky Embedded Systems Security para Windows porque el formato estaba dañado.
Objetos procesados	Cantidad total de objetos que procesó Kaspersky Embedded Systems Security para Windows.

Puede ver las estadísticas de la tarea Protección de archivos en tiempo real en el registro de tareas si hace clic en el vínculo **Abrir el registro de tareas** en la sección **Administración** del panel de detalles.

Si el valor del campo **Eventos en total** en la ventana de registro de tareas Protección de archivos en tiempo real supera 0, se recomienda procesar manualmente los eventos en el registro de tareas en la pestaña **Eventos**.

Administración de la tarea Protección de archivos en tiempo real a través del Complemento web

En esta sección, aprenderá a administrar la tarea Protección de archivos en tiempo real mediante la interfaz del Complemento web.

Configuración de la tarea Protección de archivos en tiempo real

El nivel de seguridad predefinido no se puede cambiar para la tarea Protección de archivos en tiempo real a través del Complemento web.

Para configurar la tarea Protección de archivos en tiempo real a través del Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Elija la sección **Protección del equipo en tiempo real**.

5. Haga clic en **Configuración** en la subsección **Protección de archivos en tiempo real**.

6. Configure las opciones que se describen en la tabla a continuación.

Configuración de la tarea Protección de archivos en tiempo real

Configuración	Descripción
Modo inteligente	Kaspersky Embedded Systems Security para Windows selecciona objetos para analizar por su cuenta. Un objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si se accede al objeto varias veces y el proceso lo modifica, Kaspersky Embedded Systems Security para Windows vuelve a analizar el objeto sólo después de que el proceso lo guarde por última vez.
Al acceder	Kaspersky Embedded Systems Security para Windows analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.
Al acceder y realizar modificaciones	Kaspersky Embedded Systems Security para Windows analiza un objeto cuando se abre y, si el objeto se modifica, vuelve a analizarlo después de que se guarda. De forma predeterminada, esta opción está seleccionada.
Durante ejecución	Kaspersky Embedded Systems Security para Windows analiza un archivo solo cuando se accede para su ejecución.
Análisis detallado de los procesos que se iniciarán (la ejecución del proceso se bloqueará hasta que finalice el análisis)	Kaspersky Embedded Systems Security para Windows realiza un análisis más extenso de los procesos de inicio con una mayor probabilidad de detectar una amenaza. El inicio del proceso se bloquea hasta el final del análisis.
Usar el analizador heurístico	Esta casilla de verificación habilita y deshabilita el Analizador heurístico durante el análisis de objetos. Si la casilla está activada, el Analizador heurístico está habilitado. Si la casilla está desactivada, el Analizador heurístico está deshabilitado. De forma predeterminada, la casilla está activada.
Nivel del análisis heurístico	El nivel del análisis heurístico ofrece un equilibrio entre la profundidad de las búsquedas de nuevas amenazas, el consumo de recursos del sistema operativo y el tiempo requerido para el análisis. Los siguientes niveles de sensibilidad del análisis están disponibles: • **Ligero**. El Analizador heurístico realiza menos instrucciones dentro de archivos ejecutables. La probabilidad de detección de amenazas en este modo es en cierto grado inferior. El análisis es más rápido y consume menos recursos. • **Medio**. El Analizador heurístico realiza el número de instrucciones de archivos ejecutables recomendadas por los expertos de Kaspersky. Este nivel está seleccionado de forma predeterminada. • **Profundo**. El Analizador heurístico realiza más instrucciones dentro de archivos ejecutables. La probabilidad de detección de amenazas en este

	modo es mayor. El análisis utiliza más recursos del sistema, lleva más tiempo y puede causar un número más alto de falsas alarmas. La opción está disponible si la casilla **Usar el analizador heurístico** está seleccionada.
Aplicar zona de confianza	Esta casilla de verificación habilita y deshabilita el uso de la Zona de confianza para una tarea. Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows agrega operaciones del archivo de procesos de confianza a las exclusiones de análisis configuradas en la tarea. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows ignora las operaciones del archivo de procesos de confianza al formar el área de protección para la tarea. De forma predeterminada, la casilla está activada.
Usar KSN para protección	Esta casilla de verificación habilita o deshabilita el uso de servicios de KSN. Si se selecciona la casilla, la aplicación utiliza los datos de Kaspersky Security Network para asegurarse de que la aplicación responda con mayor rapidez a amenazas nuevas y para reducir la posibilidad de falsos positivos. Si la casilla de verificación está desactivada, la tarea no usa los servicios de KSN. De forma predeterminada, la casilla está activada.
Bloquear acceso a recursos compartidos en la red para las sesiones de red que muestran actividad maliciosa	La casilla habilita o deshabilita el bloqueo de la sesión actual y controla la disponibilidad de los recursos compartidos en la red en términos de la sesión actual. Si se selecciona la casilla, Kaspersky Embedded Systems Security bloquea la sesión actual y, en términos de la sesión actual, provoca que los recursos compartidos en la red no estén disponibles para los hosts en los que se detectó actividad maliciosa en la sección Depósito de hosts bloqueados Si la casilla está desactivada, las condiciones no se aplican y las funciones de Kaspersky Embedded Systems Security funcionan con normalidad. De forma predeterminada, la casilla no está activada. Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados. Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.
Iniciar análisis de áreas críticas al detectar infección activa	Si la casilla de verificación está seleccionada, cuando se detecta una infección activa, Kaspersky Embedded Systems Security para Windows crea e inicia una tarea temporal de Análisis de áreas críticas. Cuando finaliza la tarea temporal Análisis de áreas críticas, Kaspersky Embedded Systems Security para Windows elimina esta tarea temporal. Si la casilla de verificación está desactivada, cuando se detecta una infección activa, Kaspersky Embedded Systems Security para Windows no crea e inicia la tarea Análisis de áreas críticas. De forma predeterminada, la casilla está activada.
Área de protección	

	Puede configurar las opciones de seguridad del alcance de protección.

Configuración del alcance de la protección de la tarea

Para configurar un alcance de la protección para la tarea Protección de archivos en tiempo real, realice lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Protección del equipo en tiempo real**.
5. Haga clic en **Configuración** en la subsección **Protección de archivos en tiempo real**.
6. Seleccione la sección **Área de protección**.
7. Realice una de las siguientes opciones:
   - Haga clic en el botón **Agregar** para agregar una nueva regla.
   - Seleccione una regla existente y haga clic en el botón **Editar**.

   Se abre la ventana **Editar área**.
8. Cambie el botón de alternancia a **Activa** y seleccione un tipo de objeto.
9. En la sección **Protección de objetos**, configure las siguientes opciones:
   - **Modo de protección de objetos**:
     - **Todos los objetos**
     - **Objetos analizados según su formato**
     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
     - **Objetos analizados según la lista de extensiones especificada**
   - **Analizar sectores de inicio del disco y MBR**
   - **Analizar secuencias alternativas de NTFS**
10. En la sección **Protección de objetos**, seleccione o desactive la casilla de verificación **Proteger solo los archivos nuevos y modificados**.
11. En la sección **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:
    - **Archivos comprimidos**

- Archivos SFX
- Objetos empaquetados
- Bases de datos de correo electrónico
- Correo electrónico simple
- Objetos OLE incorporados
- Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar

12. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:

- Solo notificar.
- Bloquear acceso.
- **Realizar acción adicional**.
  Seleccione la acción en la lista desplegable:
  - **Desinfectar**.
  - **Desinfectar; si falla la desinfección, eliminar**.
  - Eliminar.
  - Recomendado.

13. Seleccione la acción a realizar en los objetos probablemente infectados:

- Solo notificar.
- Bloquear acceso.
- **Realizar acción adicional**.
  Seleccione la acción en la lista desplegable:
  - **Poner en cuarentena**.
  - Eliminar.
  - Recomendado.

14. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

a. Borre o seleccione la casilla de verificación Realizar acciones según el tipo de objeto detectado.

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

c. En la ventana que se abre, seleccione una acción primaria y una acción secundaria (a realizarse en caso de que falle la acción primaria) para cada tipo de objeto detectado.

d. Haga clic en el botón **Aceptar**.

15. En la sección **Exclusiones**, configure las siguientes opciones:

    - Desactive o seleccione la casilla de verificación **Excluir archivos**.
    - Borre o seleccione la casilla de verificación **No detectar**.

16. En la sección **Rendimiento**, configure las siguientes opciones:

    - **Detener el análisis si demora más de (s)**
    - **No analizar objetos compuestos de más de (MB)**
    - **Usar la tecnología iSwift**
    - **Usar la tecnología iChecker**

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

Uso de KSN

Esta sección contiene información acerca de la tarea de Uso de KSN y cómo configurarla.

Acerca de la tarea Uso de KSN

Kaspersky Security Network (también denominado "KSN") es una infraestructura de servicios en línea que proporciona acceso a la base de conocimientos operativa de Kaspersky sobre la reputación de archivos, recursos web y programas. Kaspersky Security Network permite que Kaspersky Embedded Systems Security para Windows reaccione rápidamente ante amenazas nuevas, mejora el rendimiento de varios componentes de protección y reduce la posibilidad de falsos positivos.

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

La información recibida por Kaspersky Embedded Systems Security para Windows de Kaspersky Security Network solo pertenece a la reputación de los programas.

La participación en KSN permite a Kaspersky recibir información en tiempo real sobre tipos y fuentes de amenazas nuevas, desarrollar modos de neutralizarlas y reducir el número de falsos positivos en los componentes de la aplicación.

La información más detallada sobre la transferencia, el procesamiento, el almacenamiento y la destrucción de información sobre uso de aplicaciones está disponible en la ventana **Declaración de Kaspersky Security Network** de la tarea Uso de KSN y en la Política de privacidad en el sitio web de Kaspersky.

La participación en Kaspersky Security Network es voluntaria. La decisión en cuanto a la participación en Kaspersky Security Network se toma después de la instalación de Kaspersky Embedded Systems Security para Windows. Puede cambiar de opinión sobre la participación en Kaspersky Security Network en cualquier momento.

Kaspersky Security Network puede utilizarse en las siguientes tareas de Kaspersky Embedded Systems Security para Windows:

- Protección de archivos en tiempo real.
- Análisis a pedido.
- Reglas de Control de inicio de aplicaciones

Kaspersky Private Security Network

Consulte detalles sobre la forma de configurar Kaspersky Private Security Network (de aquí en más, "KSN Privada") en la *Ayuda de Kaspersky Security Center*.

Si utiliza KSN Privada en el dispositivo, en la ventana **Declaración de Kaspersky Security Network** de la tarea Uso de KSN, puede leer la Declaración de KSN y activar la casilla **Acepto los términos de participación en Kaspersky Security Network** para habilitar la tarea. Al aceptar los términos, acepta enviar todos los tipos de datos mencionados en la Declaración de KSN (solicitudes de seguridad, datos estadísticos) a servicios de KSN.

Después de aceptar los términos de KSN Privada, las casillas de verificación que configuran el uso de KSN global no están disponibles.

Si deshabilita KSN Privada cuando se está ejecutando la tarea Uso de KSN, se produce el error *Infracción de la licencia* y la tarea se detiene. Para seguir protegiendo el dispositivo, debe aceptar la Declaración de KSN en la ventana **Declaración de Kaspersky Security Network** y reiniciar la tarea.

Cancelación de la aceptación de la Declaración de KSN

Puede cancelar la aceptación y detener todo intercambio de datos con Kaspersky Security Network en cualquier momento. Las siguientes acciones se consideran como una cancelación completa o parcial de la Declaración de KSN:

- Si se desactiva la casilla de verificación **Enviar datos sobre archivos analizados**: la aplicación deja de enviar sumas de control de archivos analizados al servicio de KSN.
- Si se desactiva la casilla de verificación **Enviar estadísticas de Kaspersky Security Network**: la aplicación deja de procesar datos con estadísticas de KSN adicionales.
- Si se desactiva la casilla de verificación **Acepto los términos de participación en Kaspersky Security Network**: la aplicación detiene todo el procesamiento de datos relacionados con KSN y se detiene la tarea Uso de KSN.
- Si se desinstala el componente Uso de KSN: se detiene todo el procesamiento de datos relacionado con KSN.
- Si se desinstala Kaspersky Embedded Systems Security para Windows: se detiene todo el procesamiento de datos relacionado con KSN.
- Desinstalación de una clave de licencia para Kaspersky Embedded Systems Security para Windows o suspensión de la licencia: se detiene todo el procesamiento de datos relacionado con KSN.

Configuración de tarea predeterminada de Uso de KSN

Puede cambiar la configuración predeterminada de la tarea Uso de KSN (consulte la siguiente tabla).

Configuración de tarea predeterminada de Uso de KSN

Configuración	Valor predeterminado	Descripción
Acción para realizar con los objetos no confiables según KSN	Eliminar	Puede especificar acciones que Kaspersky Embedded Systems Security para Windows tomará sobre los objetos que KSN identifique como no confiables.
Transferencia de datos	Se calcula la suma de control del archivo (hash MD5) para los archivos que no	Puede especificar el tamaño máximo de archivos para los cuales se calcula una suma de control con el algoritmo MD5 para la entrega a KSN. Si la casilla de verificación está desactivada,

	superan 2 MB de tamaño.	Kaspersky Embedded Systems Security para Windows calcula el hash MD5 para los archivos de cualquier tamaño.
Programación de inicio de tareas	La primera ejecución no está programada.	Puede iniciar la tarea manualmente o configurar un inicio programado.
Usar Kaspersky Security Center como KSN Proxy	Seleccionada	De forma predeterminada, los datos se envían a KSN mediante Kaspersky Security Center. Puede cambiar esta configuración solo mediante el Complemento de administración.
Acepto los términos de participación en Kaspersky Security Network	Desactivada	Si se selecciona, acepta la participación en KSN después de la instalación. Puede cambiar su decisión en cualquier momento.
Enviar estadísticas de Kaspersky Security Network	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si se aceptó la Declaración de KSN, se enviarán automáticamente las estadísticas de KSN a menos que desactive la casilla de verificación.
Enviar datos sobre archivos analizados	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si se aceptó la Declaración de KSN, se envían los datos sobre los archivos analizados desde el inicio de la tarea. Puede desactivar la casilla de verificación en cualquier momento.

Gestión del Uso de KSN a través del Complemento de administración

En esta sección, aprenda cómo configurar la tarea Uso de KSN y Manejo de datos mediante el Complemento de administración.

Configuración de la tarea Uso de KSN

Para configurar la tarea Uso de KSN:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configuración** en la subsección **Uso de KSN**.

Se abre la ventana **Uso de KSN**.

5. En la pestaña **General**, configure la siguiente configuración de tarea:

   - En la sección **Acción para realizar con los objetos no confiables según KSN**, especifique la acción que Kaspersky Embedded Systems Security para Windows debe realizar si detecta un objeto identificado por KSN como dudoso:

     - **Eliminar**
     - **Registrar información**

   - En la sección **Transferencia de datos**, limite el tamaño de los archivos para los cuales se calcula la suma de control:

     - Active o desactive la casilla **No calcular la suma de control que se envía a KSN si el tamaño del archivo es superior a (MB)**.
     - Si es necesario, en el campo a la derecha, cambie el tamaño máximo de archivos para los cuales Kaspersky Embedded Systems Security para Windows calcula la suma de control.

   - En la sección **KSN Proxy**, desactive o seleccione la casilla de verificación **Usar Kaspersky Security Center como KSN Proxy**.

     Para habilitar el KSN Proxy, debe haberse aceptado la Declaración de KSN, y Kaspersky Security Center debe estar configurado correctamente. Consulte la *Ayuda de Kaspersky Security Center* para obtener más detalles.

6. De ser necesario, configure la programación de inicio de la tarea en la pestaña **Administración de tareas**. Por ejemplo, puede habilitar el inicio de la tarea según una programación y especificar la frecuencia del inicio como **Al inicio de la aplicación** si desea que la tarea se ejecute automáticamente cuando el dispositivo protegido se reinicia.

   La aplicación iniciará automáticamente la tarea Uso de KSN según la programación.

7. Configure el manejo de datos antes de iniciar la tarea.

8. Haga clic en el botón **Aceptar**.

Se aplica la configuración modificada. La fecha y tiempo de modificación de la configuración, así como la información sobre la configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración del procesamiento de la información

Para configurar los datos que procesarán los servicios de KSN y aceptar la Declaración de KSN:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

- Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

- Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Declaración de KSN** en la subsección **Uso de KSN**.

   Se abre la ventana **Declaración de Kaspersky Security Network**.

5. En la ficha **Estadísticas y servicios**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de participación en Kaspersky Security Network**.

6. Para aumentar el nivel de protección, se seleccionan automáticamente las siguientes casillas de verificación:

   - Enviar datos sobre archivos analizados
   - Enviar estadísticas de Kaspersky Security Network

   Puede desactivar estas casillas de verificación y dejar de enviar datos adicionales en cualquier momento.

7. La casilla de verificación Enviar estadísticas de Kaspersky Security Network está seleccionada de forma predeterminada. Si no desea que Kaspersky Embedded Systems Security para Windows envíe estadísticas adicionales a Kaspersky, puede desactivar esta casilla en cualquier momento.

8. Haga clic en el botón **Aceptar**.

   Se guardará la configuración de procesamiento de datos.

Gestión del Uso de KSN a través de la Consola de la aplicación

En esta sección, aprenda cómo configurar la tarea Uso de KSN y Manejo de datos mediante la Consola de la aplicación.

Configuración de la tarea Uso de KSN

Para configurar la tarea Uso de KSN:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.

2. Seleccione el nodo secundario **Uso de KSN**.

3. Haga clic en el vínculo **Propiedades** del panel de resultados.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.

4. Configure la tarea:

   - En la sección **Acción para realizar con los objetos no confiables según KSN**, especifique la acción que Kaspersky Embedded Systems Security para Windows debe realizar si detecta un objeto identificado por KSN como dudoso:

- **Eliminar**
- **Registrar información**

- En la sección **Transferencia de datos**, limite el tamaño de los archivos para los cuales se calcula la suma de control:
  - Active o desactive la casilla **No calcular la suma de control que se envía a KSN si el tamaño del archivo es superior a (MB)**.
  - Si es necesario, en el campo a la derecha, cambie el tamaño máximo de archivos para los cuales Kaspersky Embedded Systems Security para Windows calcula la suma de control.

5. De ser necesario, configure la programación de inicio de tareas en las pestañas **Programación** y **Avanzado**. Por ejemplo, puede habilitar el inicio de la tarea según una programación y especificar la frecuencia del inicio como **Al inicio de la aplicación** si desea que la tarea se ejecute automáticamente cuando el dispositivo protegido se reinicia.

   La aplicación iniciará automáticamente la tarea Uso de KSN según la programación.

6. Configure el manejo de datos antes de iniciar la tarea.

7. Haga clic en el botón **Aceptar**.

Se aplica la configuración modificada. La fecha y tiempo de modificación de la configuración, así como la información sobre la configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración del procesamiento de la información

Para configurar los datos que procesarán los servicios de KSN y aceptar la Declaración de KSN:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.

2. Seleccione el nodo secundario **Uso de KSN**.

3. Haga clic en el vínculo **Declaración de KSN** del panel de detalles.

   Se abre la ventana **Declaración de Kaspersky Security Network**.

4. En la ficha **Estadísticas y servicios**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de participación en Kaspersky Security Network**.

5. Para aumentar el nivel de protección, se seleccionan automáticamente las siguientes casillas de verificación:

   - **Enviar datos sobre archivos analizados**
   - **Enviar estadísticas de Kaspersky Security Network**

   Puede desactivar estas casillas de verificación y dejar de enviar datos adicionales en cualquier momento.

6. La casilla de verificación **Enviar estadísticas de Kaspersky Security Network** está seleccionada de forma predeterminada. Si no desea que Kaspersky Embedded Systems Security para Windows envíe estadísticas adicionales a Kaspersky, puede desactivar esta casilla en cualquier momento.

7. Haga clic en el botón **Aceptar**.

Se guardará la configuración de procesamiento de datos.

Administración del Uso de KSN a través del Complemento web

Para configurar la tarea Uso de KSN y el manejo de datos mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Protección del equipo en tiempo real**.
5. Haga clic en **Configuración** en la subsección **Uso de KSN**.
6. Configure las opciones que se describen en la tabla a continuación.

Tarea Uso de KSN y manejo de datos a través de la configuración del Complemento de administración

Configuración	Descripción
Eliminar	Kaspersky Embedded Systems Security para Windows elimina el objeto de estado dudoso según KSN y coloca una copia en Copia de seguridad. De forma predeterminada, esta opción está seleccionada.
Registrar información	Kaspersky Embedded Systems Security para Windows registra información sobre el objeto de estado dudoso según KSN en el registro de tareas. Kaspersky Embedded Systems Security para Windows no elimina el objeto dudoso.
No calcular la suma de control antes de enviar a KSN si el tamaño del archivo es superior a	Esta casilla de verificación habilita o deshabilita el cálculo de la suma de control para archivos del tamaño especificado para la entrega de esta información al servicio KSN. La duración del cálculo de la suma de control depende del tamaño del archivo. Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows no calcula la suma de control para los archivos que superan el tamaño especificado (en MB). Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows calcula la suma de control para los archivos de cualquier tamaño. De forma predeterminada, la casilla está activada.
Confirmo que he leído los términos de participación en Kaspersky Security Network, los comprendo y acepto	Al seleccionar esta casilla de verificación, confirma que ha leído y aceptado los términos de la Declaración de Kaspersky Security Network.
Enviar datos sobre archivos	Si se selecciona la casilla, Kaspersky Embedded Systems Security para Windows envía la suma de control de los archivos analizados a Kaspersky. La conclusión sobre la

analizados	seguridad de cada archivo se basa en la reputación recibida de KSN. Si se desactiva la casilla, Kaspersky Embedded Systems Security para Windows no envía la suma de control de los archivos a KSN. Tenga en cuenta que las solicitudes de reputación de archivos se podrían enviar en un modo limitado. Las limitaciones se utilizan para proteger a los servidores de reputación de Kaspersky contra los ataques de DDoS. En esta situación, los parámetros de solicitudes de reputación de archivos que se envían se definen por las reglas y los métodos establecidos por los expertos de Kaspersky, y no pueden ser configurados por el usuario en un dispositivo protegido. Las actualizaciones de estas reglas y métodos se reciben junto con las actualizaciones de la base de datos de la aplicación. Si se aplican las limitaciones, aparece el estado *habilitado por Kaspersky para proteger los servidores de KSN contra DDoS* en las estadísticas de la tarea Uso de KSN. De forma predeterminada, la casilla está activada.
Aceptar el procesamiento de datos como parte de las estadísticas de Kaspersky Security Network	Si se selecciona la casilla, Kaspersky Embedded Systems Security para Windows envía estadísticas adicionales que pueden contener datos personales. La lista de todos los datos que se envían como estadísticas de KSN se especifica en la Declaración de KSN. Los datos recibidos por Kaspersky se usan para mejorar la calidad de las aplicaciones y el nivel del índice de detección de amenazas. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no envía estadísticas adicionales. De forma predeterminada, la casilla está activada.
Administración de tareas	Puede configurar las opciones para iniciar la tarea en base a una programación.

Configuración de la transferencia de datos adicional

Kaspersky Embedded Systems Security para Windows se puede configurar para enviar los siguientes datos a Kaspersky:

- Sumas de control de archivos analizados (casilla de verificación **Enviar datos sobre archivos analizados**).
- Estadísticas adicionales, incluidos datos personales (casilla de verificación **Enviar estadísticas de Kaspersky Security Network**).

Consulte la sección "Manejo de datos locales" de este guía para acceder a información detallada sobre los datos que se envían a Kaspersky.

Las casillas correspondientes se pueden seleccionar o desactivar solo si se seleccionó la casilla **Acepto los términos de participación en Kaspersky Security Network**.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows envía sumas de control y estadísticas adicionales después de aceptar la Declaración de KSN.

La casilla de verificación **Acepto los términos de participación en Kaspersky Security Network** no se puede editar solo si la directiva de Kaspersky Security Center bloquea los cambios en la configuración de manejo de datos.

Posibles estados de las casillas de verificación y condiciones correspondientes

Estado de la casilla	Condiciones para el estado de la casilla Enviar datos sobre archivos analizados	Condiciones para el estado de la casilla Enviar estadísticas de Kaspersky Security Network	Condiciones para del estado de la casilla de verificación Acepto los términos de participación en Kaspersky Security Network
☑	• se envían solicitudes de reputación • la casilla es editable	• se envían estadísticas adicionales • la casilla es editable	• se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla es editable
☑	• se envían solicitudes de reputación • la casilla no es editable	• se envían estadísticas adicionales • la casilla no es editable	• se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla no es editable
☐	• no se envían solicitudes de reputación • la casilla es editable	• no se envían estadísticas adicionales • la casilla es editable	• no se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla es editable
☐	• no se envían solicitudes de reputación • la casilla no es editable	• no se envían estadísticas adicionales • la casilla no es editable	• no se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla no es editable

Estadísticas de la tarea Uso de KSN

Mientras se está ejecutando la tarea Uso de KSN, es posible ver información detallada en tiempo real sobre el número de objetos procesados por Kaspersky Embedded Systems Security para Windows desde su inicio hasta ese momento. La información sobre todos los eventos que ocurren durante la tarea se registra en el registro de tareas.

Para ver las estadísticas de la tarea Uso de KSN:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Uso de KSN**.

Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de detalles del nodo seleccionado.

Puede consultar la información sobre objetos procesados por Kaspersky Embedded Systems Security para Windows desde que la tarea se inició (consulte la tabla a continuación).

Estadísticas de la tarea Uso de KSN

Campo	Descripción

Errores de envío de solicitudes	Cantidad solicitudes de KSN cuyo procesamiento produjo un error de la tarea.
Estadísticas creadas	Número de paquetes estadísticos generados enviados a KSN.
Objetos eliminados	Número de objetos que Kaspersky Embedded Systems Security para Windows eliminó al ejecutar la tarea Uso de KSN.
Pasados a Copia de seguridad	Cantidad de objetos cuyas copias Kaspersky Embedded Systems Security para Windows guardó en Copia de seguridad.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows intentó eliminar, pero no pudo hacerlo debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación. La información sobre tales objetos se registra en el registro de tareas.
Objetos sin copia de seguridad	Una cantidad de objetos cuyas copias Kaspersky Embedded Systems Security para Windows intentó guardar en Copia de seguridad, pero no pudo hacerlo; por ejemplo, debido a espacio insuficiente en el disco. La aplicación no desinfecta ni elimina archivos que no se pueden mover a las Copia de seguridad. La información sobre tales objetos se registra en el registro de tareas.
Modo limitado	El estado significa si la aplicación envía solicitudes de reputación de archivos en un modo limitado. En un modo limitado, Kaspersky Embedded Systems Security para Windows envía solo una parte de las solicitudes de reputación de archivos según la recomendación de los expertos de Kaspersky.

Protección contra amenazas de red

Esta sección contiene información acerca de la tarea de Protección contra amenazas de red y cómo configurarla.

Acerca de la tarea Protección contra amenazas de red

La Protección contra amenazas de red solo se puede instalar en un dispositivo con Microsoft Windows 7 y cualquier versión posterior o Windows Server 2008 R2 y cualquier versión posterior.

La tarea Protección contra amenazas de red analiza el tráfico de red entrante en busca de actividad típica de los ataques de red. Al detectar un intento de ataque de red que apunta a su equipo, Kaspersky Embedded Systems Security para Windows bloquea la actividad de red del equipo atacante. Luego, su pantalla muestra una advertencia que indica que se intentó un ataque de red y muestra información sobre el equipo atacante.

De forma predeterminada, la tarea Protección contra amenazas de red se ejecuta en el modo **Bloquear las conexiones al detectar un ataque**. En este modo, Kaspersky Embedded Systems Security para Windows agrega direcciones IP de hosts que muestran la actividad típica de los ataques de red a la lista de hosts bloqueados.

Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.

Las direcciones IP de los hosts que muestran la actividad típica de los ataques de red se eliminan de la lista de hosts bloqueados en los siguientes casos:

- Se desinstala Kaspersky Embedded Systems Security para Windows.
- La dirección IP se eliminó manualmente de la lista de hosts bloqueados.
- El plazo de bloqueo del host ha caducado.
- La tarea Protección contra amenazas de red se detuvo y la casilla **No detener el análisis de tráfico cuando la tarea no está en ejecución** está desactivada.
- El modo **Bloquear las conexiones al detectar un ataque** fue desactivado.

Configuración predeterminada de la tarea Protección contra amenazas de red

La tarea Protección contra amenazas de red utiliza la configuración predeterminada que se describe en la tabla a continuación. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea Protección contra amenazas de red

Configuración	Valor predeterminado	Descripción
Modo de procesamiento	**Bloquear las conexiones al detectar un ataque**	La tarea Protección contra amenazas de red se puede iniciar en los modos **No monitorear**, **Informar únicamente**

		sobre los ataques de red o Bloquear las conexiones al detectar un ataque. La casilla de verificación habilita o deshabilita la adición de hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados. Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada y agrega las direcciones IP de los hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados. Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados. Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados. Este modo está seleccionado en forma predeterminada. Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada, pero no bloquea la actividad de red del equipo atacante. Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, pero no registra eventos sobre la actividad detectada y no bloquea la actividad de red del equipo atacante. Por ejemplo, puede usar este modo en caso de una disminución en el rendimiento del dispositivo protegido.
Exclusiones	La lista de exclusiones no se aplica.	Especifique áreas que desea excluir del alcance de protección de la tarea.
Configuración de programación	De manera predeterminada, la tarea Protección contra amenazas de red se ejecuta automáticamente cuando se inicia Kaspersky Embedded Systems Security para Windows.	Puede configurar la programación del horario.

Configuración de la tarea Protección contra amenazas de red mediante la Consola de la aplicación

En esta sección, aprenda cómo administrar la tarea Protección contra amenazas de red mediante la interfaz de la Consola de la aplicación.

Configuración general de la tarea

Para configurar los ajustes generales de la tarea Protección contra amenazas de red a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario de **Protección contra amenazas de red**.
3. Haga clic en el vínculo **Protección contra amenazas de red**, en el panel de detalles del nodo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
4. Abra la pestaña **General**.
5. En la sección **Modo de procesamiento**, seleccione el modo de procesamiento:

   - **No monitorear**.

     Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, pero no registra eventos sobre la actividad detectada y no bloquea la actividad de red del equipo atacante.

     Por ejemplo, puede usar este modo en caso de una disminución en el rendimiento del dispositivo protegido.

   - **Informar únicamente sobre los ataques de red**.

     Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada, pero no bloquea la actividad de red del equipo atacante.

   - **Bloquear las conexiones al detectar un ataque**.

La casilla de verificación habilita o deshabilita la adición de hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada y agrega las direcciones IP de los hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.

Este modo está seleccionado en forma predeterminada.

6. En el bloque **Protección contra suplantación de MAC**, active o desactive la casilla **Habilitar la protección contra suplantación de MAC**.

Un ataque de suplantación de direcciones MAC consiste en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Esto permite redirigir los datos destinados a un dispositivo a otro dispositivo, lo cual le brinda acceso a esos datos al atacante.

Si la casilla está activada y el modo de la tarea Protección contra amenazas de red no es **No monitorear**, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de acciones típicas de los ataques de suplantación de direcciones MAC y realiza las acciones que correspondan al modo seleccionado para la tarea Protección contra amenazas de red.

Si se desactiva la casilla o se ha seleccionado el modo **No monitorear**, Kaspersky Embedded Systems Security para Windows no analiza el tráfico de red entrante en busca de acciones típicas de los ataques de suplantación de direcciones MAC.

De forma predeterminada, la casilla no está activada.

7. Seleccione o desactive la casilla de verificación **No detener el análisis de tráfico cuando la tarea no está en ejecución**.

Si esta casilla está activada, incluso cuando la tarea Protección contra amenazas de red está detenida, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividades típicas de los ataques de red y bloquea la actividad de red de los equipos atacantes si así lo exige el modo seleccionado para la tarea.

Si esta casilla está desactivada, cuando se detiene la tarea Protección contra amenazas de red, Kaspersky Embedded Systems Security para Windows deja de analizar el tráfico de red entrante en busca de actividades típicas de los ataques de red.

De forma predeterminada, la casilla no está activada.

8. Haga clic en el botón **Aceptar**.

Cómo agregar exclusiones

Para agregar exclusiones a la tarea Protección contra amenazas de red, siga estos pasos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario de **Protección contra amenazas de red**.

3. Haga clic en el vínculo **Protección contra amenazas de red**, en el panel de detalles del nodo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

4. En la pestaña **Exclusiones**, seleccione la casilla de verificación **No controlar las direcciones IP excluidas**.

   Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows no analiza el tráfico de red entrante de las direcciones IP excluidas.

   Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no aplica la lista de exclusión.

5. Especifique la dirección IP y haga clic en el botón **Agregar**.

6. Haga clic en el botón **Aceptar**.

Configuración de la tarea Protección contra amenazas de red mediante el Complemento de administración

En esta sección, aprenda cómo administrar la tarea Protección contra amenazas de red mediante la interfaz del Complemento de administración.

Configuración general de la tarea

Para configurar la tarea Protección contra amenazas de red mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Protección del equipo en tiempo real**, en el bloque **Protección contra amenazas de red**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección contra amenazas de red**.

5. Abra la pestaña **General**.

6. En la sección **Modo de procesamiento**, seleccione un modo para la tarea:

   - No monitorear.

Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, pero no registra eventos sobre la actividad detectada y no bloquea la actividad de red del equipo atacante.

Por ejemplo, puede usar este modo en caso de una disminución en el rendimiento del dispositivo protegido.

- **Informar únicamente sobre los ataques de red**.

  Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada, pero no bloquea la actividad de red del equipo atacante.

- **Bloquear las conexiones al detectar un ataque**.

  La casilla de verificación habilita o deshabilita la adición de hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

  Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada y agrega las direcciones IP de los hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

  Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

  Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.

  Este modo está seleccionado en forma predeterminada.

7. En el bloque **Protección contra suplantación de MAC**, active o desactive la casilla **Habilitar la protección contra suplantación de MAC**.

   Un ataque de suplantación de direcciones MAC consiste en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Esto permite redirigir los datos destinados a un dispositivo a otro dispositivo, lo cual le brinda acceso a esos datos al atacante.

   Si la casilla está activada y el modo de la tarea Protección contra amenazas de red no es **No monitorear**, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de acciones típicas de los ataques de suplantación de direcciones MAC y realiza las acciones que correspondan al modo seleccionado para la tarea Protección contra amenazas de red.

   Si se desactiva la casilla o se ha seleccionado el modo **No monitorear**, Kaspersky Embedded Systems Security para Windows no analiza el tráfico de red entrante en busca de acciones típicas de los ataques de suplantación de direcciones MAC.

   De forma predeterminada, la casilla no está activada.

8. Seleccione o desactive la casilla de verificación **No detener el análisis de tráfico cuando la tarea no está en ejecución**.

Si esta casilla está activada, incluso cuando la tarea Protección contra amenazas de red está detenida, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividades típicas de los ataques de red y bloquea la actividad de red de los equipos atacantes si así lo exige el modo seleccionado para la tarea.

Si esta casilla está desactivada, cuando se detiene la tarea Protección contra amenazas de red, Kaspersky Embedded Systems Security para Windows deja de analizar el tráfico de red entrante en busca de actividades típicas de los ataques de red.

De forma predeterminada, la casilla no está activada.

9. Haga clic en el botón **Aceptar**.

Cómo agregar exclusiones

Para agregar exclusiones a la tarea Protección contra amenazas de red, siga estos pasos:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configuración** en la subsección **Protección contra amenazas de red**.

   Se abre la ventana **Protección contra amenazas de red**.
5. En la pestaña **Exclusiones**, seleccione la casilla de verificación **No controlar las direcciones IP excluidas**.

   Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows no analiza el tráfico de red entrante de las direcciones IP excluidas.

   Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no aplica la lista de exclusión.
6. Especifique la dirección IP y haga clic en el botón **Agregar**.
7. Haga clic en el botón **Aceptar**.

Configuración de la tarea Protección contra amenazas de red mediante el Complemento web

En esta sección, aprenda cómo administrar la tarea Protección contra amenazas de red mediante la interfaz del Complemento web.

Configuración general de la tarea

Para configurar los ajustes generales de la tarea Protección contra amenazas de red a través de Web Console:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Protección del equipo en tiempo real**.
5. En el bloque **Protección contra amenazas de red**, haga clic en el botón **Configuración**.

   Se abre la ventana **Protección contra amenazas de red**.
6. Seleccione la pestaña **General**.
7. En la sección **Modo de procesamiento**, seleccione el modo de procesamiento:

   - **No monitorear**.

     Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, pero no registra eventos sobre la actividad detectada y no bloquea la actividad de red del equipo atacante.

     Por ejemplo, puede usar este modo en caso de una disminución en el rendimiento del dispositivo protegido.

   - **Informar únicamente sobre los ataques de red**.

     Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada, pero no bloquea la actividad de red del equipo atacante.

   - **Bloquear las conexiones al detectar un ataque**.

La casilla de verificación habilita o deshabilita la adición de hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

Si se selecciona este modo, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividad típica de los ataques de red, registra eventos sobre la actividad detectada y agrega las direcciones IP de los hosts que muestren la actividad típica de los ataques de red a la lista de hosts bloqueados.

Puede ver la lista de hosts bloqueados en el depósito de Hosts bloqueados.

Puede restaurar el acceso a los hosts bloqueados y especificar la cantidad de días, horas y minutos tras la cual los hosts recuperarán el acceso a los recursos de archivos en red después de ser bloqueados a través de los ajustes de almacenamiento para hosts bloqueados.

Este modo está seleccionado en forma predeterminada.

8. En el bloque **Protección contra suplantación de MAC**, active o desactive la casilla **Habilitar la protección contra suplantación de MAC**.

   Un ataque de suplantación de direcciones MAC consiste en cambiar la dirección MAC de un dispositivo de red (tarjeta de red). Esto permite redirigir los datos destinados a un dispositivo a otro dispositivo, lo cual le brinda acceso a esos datos al atacante.

   Si la casilla está activada y el modo de la tarea Protección contra amenazas de red no es **No monitorear**, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de acciones típicas de los ataques de suplantación de direcciones MAC y realiza las acciones que correspondan al modo seleccionado para la tarea Protección contra amenazas de red.

   Si se desactiva la casilla o se ha seleccionado el modo **No monitorear**, Kaspersky Embedded Systems Security para Windows no analiza el tráfico de red entrante en busca de acciones típicas de los ataques de suplantación de direcciones MAC.

   De forma predeterminada, la casilla no está activada.

9. Seleccione o desactive la casilla de verificación **No detener el análisis de tráfico cuando la tarea no está en ejecución**.

   Si esta casilla está activada, incluso cuando la tarea Protección contra amenazas de red está detenida, Kaspersky Embedded Systems Security para Windows analiza el tráfico de red entrante en busca de actividades típicas de los ataques de red y bloquea la actividad de red de los equipos atacantes si así lo exige el modo seleccionado para la tarea.

   Si esta casilla está desactivada, cuando se detiene la tarea Protección contra amenazas de red, Kaspersky Embedded Systems Security para Windows deja de analizar el tráfico de red entrante en busca de actividades típicas de los ataques de red.

   De forma predeterminada, la casilla no está activada.

10. Haga clic en el botón **Aceptar**.

Cómo agregar exclusiones

Para agregar exclusiones a la tarea Protección contra amenazas de red, siga estos pasos:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva que desea configurar.

3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Elija la sección **Protección del equipo en tiempo real**.

5. Haga clic en el botón **Configuración** en la subsección **Protección contra amenazas de red**.

6. En la pestaña **Exclusiones**, seleccione la casilla de verificación **No controlar las direcciones IP excluidas**.

   Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows no analiza el tráfico de red entrante de las direcciones IP excluidas.

   Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no aplica la lista de exclusión.

7. Especifique la dirección IP y haga clic en el botón **Agregar**.

8. Haga clic en el botón **Aceptar**.

Control de inicio de aplicaciones

Esta sección contiene información acerca de la tarea de Control de inicio de aplicaciones y cómo configurarla.

Acerca de la tarea Control de inicio de aplicaciones

Al ejecutar la tarea Control de inicio de aplicaciones, Kaspersky Embedded Systems Security para Windows supervisa los intentos del usuario de iniciar aplicaciones y permite o deniega el inicio de estas aplicaciones. La tarea Control de inicio de aplicaciones confía en el principio Denegar por defecto, que significa que cualquier aplicación que no esté permitida en la configuración de la tarea se bloqueará automáticamente.

Puede autorizar el inicio de las aplicaciones con uno de los siguientes métodos:

- Definir reglas de autorización para aplicaciones de confianza.
- Comprobar la reputación de aplicaciones de confianza en KSN al iniciarlas.

La tarea le da máxima prioridad a denegar el inicio de las aplicaciones. Por ejemplo, si una aplicación no puede iniciarse por una de las reglas de bloqueo, se denegará el inicio de la aplicación independientemente de la conclusión de confianza para KSN. En ese momento, si los servicios de KSN consideran que la aplicación no es de confianza, pero está incluida en el alcance de la regla de autorización, este inicio de aplicación será denegado.

Todos los intentos de iniciar aplicaciones se registran en el registro de tareas.

La tarea Control de inicio de aplicaciones puede funcionar en uno de los dos modos siguientes:

- **Activo**. Kaspersky Embedded Systems Security para Windows usa un conjunto de reglas para controlar el inicio de aplicaciones que entran dentro del alcance de las reglas de la tarea de Control de inicio de aplicaciones. El alcance de las reglas de Control de inicio de aplicaciones se especifica en la configuración de esta tarea. Si una aplicación entra dentro del alcance de la regla de la tarea Control de inicio de aplicaciones y su configuración no satisface ninguna regla especificada, tal inicio de aplicación se denegará.

  Los inicios de las aplicaciones que no entran dentro del alcance de uso de ninguna regla especificada en la configuración de la tarea Control de inicio de aplicaciones se rechazan, independientemente de la configuración de la tarea Control de inicio de aplicaciones.

  La tarea **Control de inicio de aplicaciones** no puede iniciarse en el modo Activo si no se ha creado ninguna regla o si hay más de 65,535 reglas para un dispositivo protegido.

- **Solo estadísticas**. Kaspersky Embedded Systems Security para Windows no utiliza reglas de Control de inicio de aplicaciones para permitir o denegar el inicio de aplicaciones. En cambio, solo registra la información sobre inicios de aplicación, las reglas cumplidas por aplicaciones en ejecución y las acciones que se hubieran realizado si la tarea se ejecutara en el modo **Activo**. Se permite el inicio de todas las aplicaciones. Este modo está configurado de forma predeterminada.

  Puede utilizar este modo para crear Reglas de Control de inicio de aplicaciones según la información del registro de tareas.

Puede configurar la tarea Control de inicio de aplicaciones según uno de los siguientes escenarios:

- Configuración avanzada y aplicación de reglas de control de inicio de aplicaciones.

- Configuración de reglas básica y uso de KSN para Control de inicio de aplicaciones.

Si los archivos del sistema operativo se encuentran dentro del alcance de la tarea Control de inicio de aplicaciones, le recomendamos que al crear reglas de Control de inicio de aplicaciones se asegure que tales aplicaciones estén permitidas por las reglas recién creadas. De otra forma, es posible que el sistema operativo tenga un error al iniciarse.

Kaspersky Embedded Systems Security para Windows también intercepta los procesos iniciados en el subsistema Windows para Linux (excepto en el caso de scripts ejecutados desde el shell de UNIX™ o intérpretes de línea de comandos). Para tales procesos, la tarea Control de inicio de aplicaciones aplica la acción definida por la configuración actual. La tarea Generador de reglas de Control de inicio de aplicaciones detecta los inicios de aplicaciones y genera las reglas correspondientes para las aplicaciones que se ejecutan en el subsistema Windows para Linux.

Acerca de las Reglas de Control de inicio de aplicaciones

Cómo funcionan las reglas de Control de inicio de aplicaciones

La operación de las Reglas de Control de inicio de aplicaciones se basa en los componentes siguientes:

- Tipo de regla.

  Las reglas de Control de inicio de aplicaciones pueden permitir o denegar el inicio de una aplicación. En consecuencia, se las llama reglas de *autorización* o *denegación*. Para crear una lista de reglas de autorización para el Control de inicio de aplicaciones, puede usar el Generador de reglas para generar reglas de autorización o la tarea Control de inicio de aplicaciones en el modo **Solo estadísticas**. También puede agregar las reglas de autorización manualmente.

- Usuario o grupo de usuarios.

  Las reglas de Control de inicio de aplicaciones pueden controlar el inicio de aplicaciones especificadas por un usuario y/o grupo de usuarios.

- Área de aplicación de regla.

  Las reglas de Control de inicio de aplicaciones pueden aplicarse a *archivos ejecutables*, *scripts* y *paquetes MSI*.

- Criterio de activación de la regla.

  Las reglas de Control de inicio de aplicaciones regulan el inicio de archivos que satisfacen uno o varios de los criterios especificados en la configuración de reglas: está firmado por el *certificado digital* especificado, coincide con el *hash SHA256* especificado, está ubicado en la *ruta* especificada y coincide con los argumentos de la *línea de comandos* especificados. Debe seleccionar al menos una opción. De lo contrario, no se agrega la regla Control de inicio de aplicaciones.

  Si el criterio de activación de una regla es **Certificado digital**, la regla creada controlará el inicio de todas las aplicaciones de confianza en el sistema operativo. Puede establecer condiciones más estrictas para este criterio si selecciona las siguientes casillas de verificación:

  - **Usar sujeto**
  - **Usar huella**

Las huellas permiten reglas de inicio de la aplicación más restrictivas según un certificado digital, porque una huella identifica en forma exclusiva a un certificado digital y no se puede falsificar, a diferencia del asunto de un certificado digital.

Puede especificar exclusiones para las Reglas de Control de inicio de aplicaciones. Las exclusiones a las Reglas de Control de inicio de aplicaciones se basan en los mismos criterios utilizados para activar las reglas: el certificado digital, el hash SHA256 y la ruta de archivo. Pueden requerirse exclusiones a las reglas de Control de inicio de aplicaciones para ciertas reglas de autorización: por ejemplo, si desea autorizar que usuarios inicien aplicaciones desde la ruta C:\Windows y, al mismo tiempo, bloquear el inicio del archivo Regedit.exe.

Si los archivos del sistema operativo se encuentran dentro del alcance de la tarea Control de inicio de aplicaciones, le recomendamos que al crear reglas de Control de inicio de aplicaciones se asegure que tales aplicaciones estén permitidas por las reglas recién creadas. De otra forma, es posible que el sistema operativo tenga un error al iniciarse.

Administración de Reglas de Control de inicio de aplicaciones

Puede realizar las siguientes acciones con las Reglas de Control de inicio de aplicaciones:

- Agregar reglas manualmente
- Generar y agregar reglas automáticamente
- Eliminar reglas
- Exportar reglas a un archivo
- Examinar archivos seleccionados para ver reglas que permiten la ejecución de estos archivos
- Filtrar reglas en la lista según el criterio especificado

Acerca del control de distribución de software

La generación de las reglas de Control de inicio de aplicaciones puede ser complicada si también tiene que controlar la distribución del software en un dispositivo protegido, por ejemplo, en dispositivos protegidos donde el software instalado se actualiza periódicamente en forma automática. En este caso, se debe actualizar la lista de reglas de autorización después de cada actualización de software para que los archivos creados recientemente se consideren en la configuración de la tarea Control de inicio de aplicaciones. Para simplificar el control de inicio en situaciones de distribución de software, puede usar el subsistema de Control de distribución de software.

Un *paquete de distribución de software* (en adelante, denominado "paquete") representa una aplicación de software que se instala en un dispositivo protegido. Cada paquete contiene al menos una aplicación, y también puede contener archivos individuales, actualizaciones o hasta un comando individuales, además de las aplicaciones, en particular cuando se instala una aplicación o una actualización de software.

El subsistema de Control de distribución de software se implementa como lista de exclusiones adicional. Cuando se agrega un paquete de instalación a la lista, el mismo se convierte en paquete de confianza. El desempaquetado de paquetes de confianza está permitido, y se permite también que las aplicaciones instaladas o actualizadas desde paquetes de confianza se inicien automáticamente. Los archivos extraídos pueden heredar el atributo de confianza de un paquete de distribución principal. Un *paquete de distribución principal* es un paquete que el usuario agregó a la lista de exclusiones de Control de distribución de software y se convirtió en un paquete de confianza.

Kaspersky Embedded Systems Security para Windows controla solo los ciclos completos de distribución de software. La aplicación no puede procesar correctamente el inicio de archivos modificados por un paquete de confianza si, cuando el paquete se inicia por primera vez, se desactiva el control de distribución de software o no se instala el componente Control de inicio de aplicaciones.

El Control de distribución de software no está disponible si se desactiva la casilla de verificación **Aplicar reglas a archivos ejecutables** en la configuración de la tarea Control de inicio de aplicaciones.

Caché de distribución del software

Kaspersky Embedded Systems Security para Windows utiliza una caché de distribución de software generado dinámicamente ("caché de distribución") para establecer la relación entre paquetes de confianza y archivos creados durante la distribución del software. Cuando un paquete se inicia por primera vez, Kaspersky Embedded Systems Security para Windows detecta todos los archivos creados por el paquete durante el proceso de distribución del software y almacena sumas de control del archivo y rutas en el caché de distribución. Entonces se permite a todos los archivos en el caché de distribución iniciarse de forma predeterminada.

No puede revisar, limpiar ni modificar manualmente el caché de distribución mediante la interfaz de usuario. Kaspersky Embedded Systems Security para Windows completa y controla el caché.

Puede exportar el caché de distribución a un archivo de configuración (en formato XML) y borrar el caché con opciones de la línea de comandos.

Para exportar el caché de distribución a un archivo de configuración, ejecute el siguiente comando:

```
kavshell appcontrol /config /savetofile:<ruta de acceso completa> /sdc
```

Para borrar el caché de distribución, ejecute el siguiente comando:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security para Windows actualiza el caché de distribución cada 24 horas. Si la suma de control de un archivo anteriormente permitido se cambia, la aplicación elimina el registro de este archivo desde el caché de distribución. Si la tarea Control de inicio de aplicaciones se inicia en un modo Activo, los intentos posteriores de iniciar este archivo se bloquearán. Si se cambia la ruta completa al archivo anteriormente permitido, los intentos subsecuentes de iniciar este archivo no se bloquearán, porque la suma de control se almacena dentro del caché de distribución.

Procesamiento de los archivos extraídos

Todos los archivos extraídos de un paquete de confianza heredan el atributo de confianza sobre el primer inicio del paquete. Si desactiva la casilla después del primer inicio, todos los archivos extraídos del paquete conservarán el atributo heredado. Para reiniciar el atributo heredado para todos los archivos extraídos, debe borrar el caché de distribución y desactivar la casilla de verificación **Permitir la distribución adicional de los programas creados desde este paquete de distribución** antes de volver a iniciar el paquete de distribución de confianza.

Los archivos extraídos y los paquetes creados por un paquete de distribución de confianza primario heredan el atributo de confianza cuando sus sumas de control se agregan a la caché de distribución al abrirse por primera vez el paquete de distribución de software de la lista de exclusiones. Por lo tanto, el propio paquete de distribución y todos los archivos extraídos de este paquete también serán de confianza. De forma predeterminada, la cantidad de niveles de la herencia del atributo de confianza es ilimitada.

Los archivos extraídos conservarán el atributo de confianza después de reiniciar el sistema operativo.

El procesamiento de archivos se define en la Configuración de Control de distribución de software mediante la selección o la desactivación de la casilla de verificación **Permitir la distribución adicional de los programas creados desde este paquete de distribución**.

Por ejemplo, si test.msi, un paquete que contiene varios paquetes y aplicaciones, se agrega a la lista de exclusiones y se selecciona esta casilla, todos los paquetes y aplicaciones contenidos en el paquete test.msi se podrán descomprimir y ejecutar, incluso si contienen otros archivos anidados. Esta situación funciona para archivos extraídos en todos los niveles anidados.

Si agrega un paquete test.msi a la lista de exclusiones y desactiva la casilla de verificación **Permitir la distribución adicional de los programas creados desde este paquete de distribución**, la aplicación asignará el atributo de confianza solo a los paquetes y archivos ejecutables extraídos directamente de un paquete de confianza principal (en el primer nivel de anidación). Las sumas de control de estos archivos se almacenan en el caché de distribución. Todos los archivos en el segundo nivel de anidación y superiores serán bloqueados por el principio de denegación predeterminada.

Trabajar con la lista de reglas de Control de inicio de aplicaciones

La lista de paquetes de confianza del subsistema de control de distribución de software es una lista de exclusiones que amplifica pero no reemplaza la lista general de reglas de Control de inicio de aplicaciones.

Las reglas de denegación de Control de inicio de aplicaciones tienen la prioridad más alta: se bloqueará la descompresión del paquete de confianza y el inicio de archivos nuevos o modificados si estos paquetes y archivos están afectados por las reglas de denegación de control del inicio de aplicaciones.

Las exclusiones de control de distribución de software se aplican tanto para paquetes de confianza como para archivos creados o modificados por estos paquetes si no se aplica ninguna regla de denegación en la lista de Control de inicio de aplicaciones para esos paquetes y archivos.

Uso de las conclusiones de KSN

Las conclusiones de KSN sobre la fiabilidad de los archivos tienen mayor prioridad que las exclusiones de Control de distribución de software. El desempaquetado de paquetes de confianza y la ejecución de archivos creados o modificados por paquetes de confianza se bloquearán si se recibe una conclusión de KSN que indique que se trata de archivos no confiables.

En ese momento, después de descomprimir los datos de un paquete de confianza, todos los archivos secundarios podrán ejecutarse independientemente del uso de KSN dentro del alcance del control de inicio de aplicaciones. En ese momento, los estados de las casillas de verificación **Denegar inicio de aplicaciones no confiables según KSN** y **Autorizar inicio de aplicaciones confiables según KSN** no afectan el funcionamiento de la casilla de verificación **Permitir la distribución adicional de los programas creados desde este paquete de distribución**.

Acerca del uso de KSN para la tarea Control de inicio de aplicaciones

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

Si los datos de KSN sobre la reputación de una aplicación se utilizan por la tarea Control de inicio de aplicaciones, la reputación de la aplicación de KSN se considera un criterio para permitir o denegar el inicio de esa aplicación. Si KSN informa a Kaspersky Embedded Systems Security para Windows que una aplicación no es confiable cuando el usuario intenta iniciar la aplicación, el inicio de la aplicación se denegará. Si KSN informa a Kaspersky Embedded Systems Security para Windows que una aplicación es confiable cuando el usuario intenta iniciar la aplicación, el inicio de aplicación se autorizará. KSN puede usarse junto con las reglas de Control de inicio de aplicaciones o como un criterio independiente para denegar el inicio de aplicaciones.

Uso de conclusiones de KSN como criterio independiente para denegar el inicio de aplicaciones

Este escenario le permite controlar de manera segura el inicio de aplicaciones en el dispositivo protegido sin la necesidad de la configuración avanzada de la lista de reglas.

Puede aplicar conclusiones KSN para Kaspersky Embedded Systems Security para Windows simultáneamente con la única regla especificada. La aplicación solo permitirá el inicio de aplicaciones que son de confianza en KSN o que están habilitadas por una regla especificada.

Para esta situación, le recomendamos definir una regla de autorización de inicio de aplicaciones basada en un certificado digital.

Se deniega el inicio del resto de las aplicaciones de acuerdo con la directiva Denegar por defecto. La utilización de KSN cuando no hay ninguna regla aplicada protege a un dispositivo de aplicaciones que KSN considera como amenaza.

Uso de conclusiones de KSN simultáneamente con reglas de Control de inicio de aplicaciones

Cuando se usan las conclusiones de KSN simultáneamente con el Control de inicio de aplicaciones, se aplican las siguientes condiciones:

- Kaspersky Embedded Systems Security para Windows siempre deniega el inicio de una aplicación si se incluye en alcance de al menos una regla de denegación. Si KSN considera que la aplicación es de confianza, la conclusión correspondiente tiene una prioridad inferior y no se considera; el inicio de la aplicación seguirá denegándose. Esto le permite expandir la lista de aplicaciones bloqueadas.

- Kaspersky Embedded Systems Security para Windows siempre bloquea el inicio de aplicaciones si este está prohibido para aplicaciones que no sean de confianza en KSN y la aplicación no es de confianza en KSN. Si se define una regla de autorización para la aplicación, tiene una prioridad inferior y no se considera; el inicio de la aplicación seguirá denegándose. Esto protege al dispositivo de aplicaciones que KSN considera una amenaza, pero no se consideraron durante la configuración inicial de las reglas.

Acerca del Generador de reglas de control de inicio de aplicaciones

Puede crear listas de reglas de Control de inicio de aplicaciones usando tareas y directivas de Kaspersky Security Center simultáneamente para todos los dispositivos protegidos y los grupos de dispositivos protegidos en la red corporativa. Se recomiendan los siguientes escenarios si la red corporativa no tiene una máquina de referencia y no puede crear una lista de reglas de autorización basadas en las aplicaciones instaladas en la máquina modelo.

Puede ejecutar localmente la tarea del Generador de reglas de control de inicio de aplicaciones a través de la Consola de la aplicación para crear una lista de reglas basadas en las aplicaciones que se ejecutan en un solo dispositivo protegido.

El componente Control de inicio de aplicaciones se instala con dos reglas de permiso preestablecidas:

- Regla de autorización para scripts y paquetes de Windows Installer con un certificado de confianza para el sistema operativo.
- Regla de autorización para archivos ejecutables con un certificado de confianza para el sistema operativo.

Puede crear listas de reglas de Control de inicio de aplicaciones del lado de Kaspersky Security Center en uno de dos modos:

- Utilizando la tarea de grupo del Generador de reglas de Control de inicio de aplicaciones.

  En este escenario, una tarea de grupo genera su propia lista de reglas de Control de inicio de aplicaciones para cada dispositivo protegido en la red y guarda esas listas a un archivo XML en la carpeta compartida especificada. El archivo XML generado por la tarea Generador de reglas de control de inicio de aplicaciones contiene las reglas de autorización especificadas en la configuración de la tarea antes de que se inicie la tarea. No se crearán reglas para aplicaciones cuya ejecución no se haya permitido en la configuración especificada para la tarea. El inicio de tales aplicaciones se rechaza de forma predeterminada. Luego, puede importar manualmente la lista creada de reglas en la tarea de Control de inicio de aplicaciones para la directiva de Kaspersky Security Center.

  Puede configurar que las reglas generadas se importen automáticamente en la lista de reglas para la tarea Control de inicio de aplicaciones.

  Este escenario se recomienda cuando tiene que crear listas de reglas de Control de inicio de aplicaciones rápidamente. Recomendamos configurar el inicio programado de la tarea de Generador de reglas de Control de inicio de aplicaciones solo si el área de aplicación de las reglas de autorización incluye carpetas y archivos que usted sabe son seguros.

  Antes de usar la tarea de Control de inicio de aplicaciones en la red, asegúrese de que todos los dispositivos protegidos puedan acceder a una carpeta compartida. Si la política de la organización no permite utilizar una carpeta compartida en la red, recomendamos que inicie la tarea Generador de reglas de control de inicio de aplicaciones en un dispositivo protegido del grupo de dispositivos protegidos de prueba o en una máquina de referencia.

- Según un informe de los eventos de tareas generadas en Kaspersky Security Center por la tarea de Control de inicio de aplicaciones ejecutada en el modo **Solo estadísticas**.

  En este escenario, Kaspersky Embedded Systems Security para Windows no deniega el inicio de aplicaciones. En cambio, con el Control de inicio de aplicaciones que se ejecuta en el modo **Solo estadísticas**, informa todos los inicios de aplicaciones autorizados y denegados en todos los dispositivos protegidos de red en la pestaña **Eventos** del espacio de trabajo del nodo Servidor de administración de Kaspersky Security Center. Kaspersky Security Center utiliza los registros para generar una sola lista de eventos en los cuales se haya rechazado el inicio de la aplicación.

Debe configurar el periodo de ejecución de tareas de modo que se realicen durante el periodo especificado todos los escenarios posibles de dispositivos protegidos y grupos de dispositivos protegidos y, al menos, un reinicio del dispositivo protegido. Luego de que finalice el periodo de ejecución de la tarea, puede importar los datos de inicio de aplicaciones desde el informe de eventos de Kaspersky Security Center guardado (formato TXT) y generar reglas de autorización de Control de inicio de aplicaciones para tales aplicaciones según estos datos.

Esta acción se recomienda si una red empresarial tiene una gran cantidad de dispositivos protegidos de diferentes tipos (con un software diferente instalado).

- Según los eventos de inicios de aplicaciones denegados que se recibieron a través de Kaspersky Security Center, sin crear ni importar un archivo de configuración.

  Para usar esta función, la tarea Control de Inicio de aplicaciones en el dispositivo protegido se debe ejecutar bajo una directiva de Kaspersky Security Center activa. En este caso, todos los eventos en el dispositivo protegido se envían al Servidor de administración.

Le recomendamos actualizar la lista de reglas cuando el conjunto de aplicaciones instaladas en dispositivos protegidos de red cambia (por ejemplo, cuando se instalan actualizaciones o se reinstalan sistemas operativos). Le recomendamos generar una lista actualizada de reglas ejecutando la tarea de Generador de reglas de Control de inicio de aplicaciones o la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** en dispositivos protegidos del grupo de administración de prueba. El grupo de administración de prueba incluye los dispositivos protegidos requeridos para evaluar el inicio de aplicaciones nuevas antes de que se instalen en dispositivos protegidos de red.

Los archivos XML que contienen listas de reglas de autorización se crean según un análisis de las tareas iniciadas en el dispositivo protegido. Para agrupar todas las aplicaciones utilizadas en la red al generar listas de reglas, le aconsejamos iniciar la tarea de Generador de reglas de control de inicio de aplicaciones y la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** en una máquina modelo.

Antes de generar las reglas de autorización sobre la base de aplicaciones iniciadas en una máquina de referencia, asegúrese de que la máquina modelo sea segura y no tenga malware.

Antes de agregar reglas de autorización, seleccione uno de los modos de aplicación de la regla disponibles. La lista de reglas de la directiva de Kaspersky Security Center muestra solo las reglas especificadas por la directiva, sin tener en cuenta el modo de aplicación de la regla. La lista de reglas locales incluye todas las reglas aplicadas, tanto reglas locales como reglas agregadas a través de una directiva.

Configuración predeterminada de la tarea Control de inicio de aplicaciones

De forma predeterminada, la tarea de Control de inicio de aplicaciones tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea Control de inicio de aplicaciones

Configuración	Valor predeterminado	Descripción
Modo de la tarea.	**Solo estadísticas**. Los registros de la tarea denegar eventos de inicio y autorizaron eventos de inicio según las reglas establecidas. El inicio de aplicaciones no se rechaza.	Puede seleccionar el modo **Activo** después de que se genera la lista final de reglas.

Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo	No aplicado	Puede repetir las acciones realizadas durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo.
Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar	No aplicado.	Puede impedir el inicio de intérpretes de comandos si no tienen ningún comando para ejecutar.
Administración de reglas	**Agregar reglas de la directiva a las reglas locales**	Puede seleccionar un modo en el cual las reglas especificadas en una directiva se apliquen junto con las reglas del dispositivo protegido.
Área de aplicación de la regla	La tarea controla el inicio de los archivos ejecutables, los scripts y los paquetes MSI. También controla la carga de módulos DLL.	Puede especificar los tipos de archivos cuyo inicio está controlado por reglas.
Uso de KSN	Los datos de la reputación de la aplicación en KSN no se utilizan.	Puede usar los datos de la reputación de la aplicación en KSN al ejecutar una tarea de Control de inicio de aplicaciones.
Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista	No aplicado.	Puede permitir la distribución de software usando los instaladores y las aplicaciones especificadas en la configuración. De forma predeterminada, la distribución de software solo se permite cuando se usa el servicio de Windows Installer.
Permitir siempre la distribución de software a través de Windows Installer	Aplicado. Puede cambiarse solo si se ha habilitado la opción **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.	Puede autorizar cualquier instalación o actualización del software si las operaciones se realizan mediante Windows Installer.
Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service	No aplicado. Puede cambiarse solo si se ha habilitado la opción **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.	Puede activar o desactivar la distribución automática del software mediante el Administrador de configuración del Centro del sistema.
Inicio de la tarea	La primera ejecución no está programada.	La tarea de Control de inicio de aplicaciones no se inicia automáticamente cuando se inicia de Kaspersky Embedded Systems Security para Windows. Puede iniciar la tarea manualmente o configurar un inicio programado.

Configuración predeterminada de la tarea de Generador de reglas de Control de inicio de aplicaciones

Configuración	Valor predeterminado	Descripción
Prefijo para nombres de	Idéntico al nombre del dispositivo protegido en el cual se instala	Puede cambiar el prefijo por nombres de reglas de autorización.

reglas de autorización	Kaspersky Embedded Systems Security para Windows.	
Área de aplicación de las reglas de autorización	De forma predeterminada, el área de aplicación de las reglas de autorización incluye las siguientes categorías de archivos: • Archivos con la extensión EXE ubicados en las carpetas C:\Windows, C:\Program Files (x86) y C:\Program Files • Paquetes MSI almacenados en la carpeta C:\Windows • Scripts almacenados en la carpeta C:\Windows La tarea también crea reglas para todas las aplicaciones en ejecución, sin tener en cuenta su ubicación ni formato.	Puede cambiar el área de protección al agregar o eliminar rutas de carpeta y al especificar los tipos de archivo que estarán autorizados a iniciarse según las reglas generadas automáticamente. Además, puede ignorar aplicaciones en ejecución al crear reglas de autorización.
Criterios para generación de reglas de autorización	Se utilizan el asunto y la huella del certificado digital; se generan reglas para todos los usuarios y los grupos de usuarios.	Puede usar el Hash SHA256 al generar reglas de autorización. Puede seleccionar un usuario y grupo de usuarios para los cuales las reglas de autorización se deben generar automáticamente.
Acciones después de la finalización de la tarea	Las reglas de autorización se agregan a la lista de reglas de Control de inicio de aplicaciones; las reglas nuevas se fusionan con las reglas existentes y las reglas duplicadas se eliminan.	Puede agregar reglas a las reglas existentes sin fusionarlas y sin eliminar las reglas duplicadas; reemplazar las reglas existentes con reglas de autorización nuevas; o configurar la exportación de reglas de autorización a un archivo.
Configuración del inicio de tareas con permisos	La tarea se inicia con una cuenta de sistema.	Puede autorizar a la tarea de Generador de reglas de Control de inicio de aplicaciones a iniciarse en una cuenta de sistema o utilizando los permisos de un usuario especificado.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Generador de reglas de Control de inicio de aplicaciones no se inicia automáticamente cuando se inicia Kaspersky Embedded Systems Security para Windows. Puede iniciar la tarea manualmente o configurar un inicio programado.

Gestión del Control de inicio de aplicaciones a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración de la tarea para uno o todos los dispositivos protegidos en la red.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la directiva para la tarea Control de inicio de aplicaciones

Para abrir la configuración de la tarea Control de inicio de aplicaciones a través de la directiva de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configuración** en la subsección **Control de inicio de aplicaciones**.

   Se abre la ventana **Control de inicio de aplicaciones**.

Configure la directiva según sea necesario.

Cómo abrir la lista de reglas de Control de inicio de aplicaciones

Para abrir la lista de reglas de Control de inicio de aplicaciones a través de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configuración** en la subsección **Control de inicio de aplicaciones**.

   Se abre la ventana **Control de inicio de aplicaciones**.
7. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de Control de inicio de aplicaciones**.

Configure la lista de reglas como sea necesario.

Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas de Control de inicio de aplicaciones

Para empezar a crear la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Abra la pestaña **Tareas**.
4. Haga clic en el botón **Nueva tarea**.

   Se abre la ventana **Nuevo asistente de tarea**.
5. Seleccione la tarea **Generador de reglas de control de inicio de aplicaciones**.
6. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración**.

Para configurar la tarea Generador de reglas de Control de inicio de aplicaciones:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Abra la pestaña **Tareas**.
4. Haga doble clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **Propiedades: Generador de reglas de control de inicio de aplicaciones**.

Consulte la sección Configuración de la tarea de Generador de reglas de control de inicio de aplicaciones para obtener más información sobre la configuración de la tarea.

Configuración de la tarea Control de inicio de aplicaciones

Para ajustar la configuración general de la tarea Control de inicio de aplicaciones:

1. Abra la ventana **Control de inicio de aplicaciones**.
2. En la pestaña **General**, seleccione la configuración siguiente en la sección **Modo de la tarea**:
   - En la lista desplegable **Modo de la tarea**, especifique el modo de la tarea.
   - Desactive o seleccione la casilla de verificación **Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo**.
   - Desactive o seleccione la opción **Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar**.

3. En el bloque **Administración de reglas**, configure las opciones para aplicar reglas:

   a. Haga clic en el botón **Lista de reglas** para agregar reglas de autorización a la tarea de Control de inicio de aplicaciones.

   > Kaspersky Embedded Systems Security para Windows no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") para escribir la ruta de acceso correctamente.

   b. Seleccione el modo para aplicar reglas:

   - **Reemplazar las reglas locales con reglas de las directivas**

     La aplicación aplica la lista de reglas especificada en la directiva para el control de inicio de aplicaciones centralizado de un grupo de dispositivos protegidos. Las listas de reglas locales no se pueden crear, modificar ni aplicar.

   - **Agregar reglas de la directiva a las reglas locales**

     La aplicación aplica la lista de reglas especificada en una directiva junto con listas de reglas locales. Puede modificar las listas de reglas locales usando la tarea del Generador de reglas de Control de inicio de aplicaciones.

4. En la sección **Área de aplicación de la regla**, especifique la siguiente configuración:

   - Aplicar reglas a archivos ejecutables.
   - Supervisar la carga de módulos DLL.

     > El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.

   - Aplicar reglas a scripts y paquetes MSI.

5. En la casilla de grupo **Uso de KSN**, configure las siguientes opciones de inicio de aplicaciones:

   - Denegar inicio de aplicaciones no confiables según KSN.
   - Autorizar inicio de aplicaciones confiables según KSN.
   - Usuarios o grupos de usuarios con permiso para iniciar aplicaciones que KSN considera de confianza:

     a. En el menú contextual del botón **Editar**, seleccione el método para agregar usuarios.

     Se abre la ventana **Seleccionar usuario o grupo de usuarios**.

     b. Seleccione un usuario o un grupo de usuarios.

     c. Haga clic en el botón **Aceptar**.

6. En la pestaña **Control de distribución de software**, configure las opciones para control de distribución de software.

7. En la pestaña **Administración de tareas**, configure la programación de inicio de la tarea.

8. Haga clic en el botón **Aceptar** de la ventana **Control de inicio de aplicaciones**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración del Control de distribución de software

Para agregar un paquete de distribución de confianza a través del Complemento de administración:

1. Abra la ventana **Control de inicio de aplicaciones**.
2. En la pestaña **Control de distribución de software**, seleccione la casilla de verificación **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.

   Puede seleccionar **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**, si la casilla de verificación **Control de inicio de aplicaciones** en la pestaña **Aplicar reglas a archivos ejecutables** está seleccionada en la configuración de la tarea **General**.

3. Desactive la casilla de verificación **Permitir siempre la distribución de software a través de Windows Installer** si es necesario.

   Solo se recomienda desactivar la casilla **Permitir siempre la distribución de software a través de Windows Installer** si es absolutamente necesario. Desactivar esta función puede causar errores al actualizar archivos del sistema operativo y también impedir el inicio de archivos extraídos de un paquete de distribución.

4. Si es necesario, seleccione la casilla de verificación **Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service**.

   La aplicación controla el ciclo de distribución del software en el dispositivo protegido; desde la entrega del paquete hasta la instalación o actualización. La aplicación no controla procesos si alguna etapa de distribución se realizara antes de la instalación de la aplicación en el dispositivo protegido.

5. Para crear la lista de autorizados o editar la lista existente de paquetes de distribución de confianza, haga clic en **Modificar la lista de paquetes** y seleccione uno de los siguientes métodos en la ventana que se abre:

   - **Agregar un paquete de distribución**.

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

     b. Seleccione el archivo ejecutable o el paquete de distribución.

     El bloque **Criterios de confianza** se completa automáticamente con datos sobre el archivo seleccionado.

     c. Desactive o seleccione la casilla de verificación **Permitir la distribución adicional de los programas creados desde este paquete de distribución**.

     d. Seleccione una de dos opciones disponibles para criterios para usar para determinar si un archivo o el paquete de distribución es de confianza:

     - **Usar certificado digital**

- Usar hash SHA256

- **Agregar varios paquetes por hash**

  Puede seleccionar un número ilimitado de archivos de ejecutables y paquetes de distribución, y agregarlos a la lista al mismo tiempo. Kaspersky Embedded Systems Security para Windows examina el hash y permite que el sistema operativo inicie los archivos especificados.

- **Cambiar el paquete seleccionado**

  Use esta opción para seleccionar otro archivo de inicio o paquete de distribución, o bien para cambiar los criterios de confianza.

- Importar lista de paquetes de distribución desde el archivo.

  En la ventana **Abrir**, especifique el archivo de configuración que contiene una lista de paquetes de distribución de confianza.

Si crea un paquete de distribución de confianza basado en un archivo ejecutable luego de agregar, en la configuración de la Zona de confianza, un proceso basado en ese mismo archivo ejecutable que luego designó como de confianza para la tarea Control de inicio de aplicaciones, la configuración de la Zona de confianza tendrá mayor prioridad. Kaspersky Embedded Systems Security para Windows no permitirá iniciar el archivo ejecutable, pero considerará que el proceso de dicho archivo es de confianza.

6. Si desea eliminar una aplicación o un paquete de distribución anteriormente agregados a la lista de confianza, haga clic en el botón **Eliminar paquetes de distribución**. Se podrán ejecutar los archivos extraídos.

Para impedir que los archivos extraídos se inicien, desinstale la aplicación en el dispositivo protegido o cree una regla de denegación en la configuración de la tarea Control de inicio de aplicaciones.

7. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada.

Configuración de una tarea de Generador de reglas de Control de inicio de aplicaciones

Para configurar la tarea Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana Propiedades: Generador de reglas de control de inicio de aplicaciones.

2. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

3. En la sección **Configuración**, puede establecer la siguiente configuración:

- Especifique el prefijo que se usará para los nombres de las reglas.
- Seleccione cómo crear reglas de autorización:
  - Crear reglas de autorización para las aplicaciones en ejecución
  - Crear reglas de autorización para las aplicaciones de las siguientes carpetas

4. En la sección **Opciones**, puede especificar las acciones que desea realizar mientras crea reglas de autorización de Control de inicio de aplicaciones:
   - Usar certificado digital
   - Usar sujeto y huella digital del certificado digital
   - De no haber un certificado, usar
     - **Hash SHA256**. El valor de la suma de control del archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.
     - **ruta de acceso al archivo**. La ruta de acceso al archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas especificada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas** en la sección **Configuración**.
   - Usar hash SHA256
   - Generar reglas para este usuario o grupo de usuarios.

   Puede configurar ajustes para los archivos de configuración con listas de reglas de autorización para Control de dispositivos y Control de inicio de aplicaciones. Kaspersky Embedded Systems Security para Windows crea estas listas cuando se completa la tarea.
5. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
6. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.
7. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.
8. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

   Se guardan las opciones de la tarea de grupo recientemente configuradas.

Configuración de las reglas de Control de inicio de aplicaciones a través de Kaspersky Security Center

Aprenda a generar una lista de reglas según distintos criterios o a crear manualmente reglas de autorización o denegación utilizando la tarea Control de inicio de aplicaciones.

Adición de una regla de Control de inicio de aplicaciones

Para agregar una regla de Control de inicio de aplicaciones mediante el Complemento de administración:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Agregar una regla**.

   Se abre la ventana **Configuración de la regla**.
4. Especifique la siguiente configuración:
   a. En el campo **Nombre**, ingrese el nombre de la regla.
   b. En la lista desplegable **Tipo**, seleccione el tipo de regla:
      - **De autorización**, si desea que la regla autorice el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de la regla.
      - **De denegación**, si desea que la regla bloquee el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de la regla.
   c. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
      - **Archivos ejecutables**, si desea que la regla controle el inicio de archivos ejecutables.
      - **Scripts y paquetes MSI**, si desea que la regla controle el inicio de scripts y paquetes MSI.
   d. En el campo **Usuario o grupo de usuarios**, indique los usuarios que podrán o no iniciar aplicaciones, dependiendo del tipo de regla.
      1. En el menú contextual del botón **Examinar**, seleccione el método que desee usar para agregar usuarios de confianza.

         Se abre la ventana **Selección de usuario o grupo de usuarios**.
      2. Seleccione un usuario o un grupo de usuarios.
      3. Haga clic en el botón **Aceptar**.
   e. Si desea tomar los valores de los criterios de activación de la regla enumerados en el bloque **Criterio de activación de la regla** de un archivo, haga lo siguiente:
      1. Haga clic en el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**.

         Se abre la ventana estándar **Abrir** de Microsoft Windows.
      2. Seleccione el archivo.
      3. Haga clic en el botón **Abrir**.

El valor de los criterios contenidos en el archivo se muestra en los campos del bloque **Criterio de activación de la regla**. El criterio para el cual están disponibles los datos en las propiedades del archivo se selecciona de forma predeterminada.

f. En el cuadro de grupo **Criterio de activación de la regla**, seleccione una o varias de las siguientes opciones aplicables:

- **Certificado digital**, si desea que la regla controle el inicio de aplicaciones que se ejecuten utilizando archivos firmados con un certificado digital:
  - Seleccione la casilla de verificación **Usar sujeto** si desea que la regla controle el inicio de archivos firmados con un certificado digital que tengan el sujeto especificado.
  - Seleccione la casilla de verificación **Usar huella** si desea que la regla controle solo el inicio de archivos firmados con un certificado digital con la huella especificada.
- **hash SHA256**, si desea que la regla controle el inicio de aplicaciones que se inicien utilizando archivos cuya suma de control coincida con la especificada.
- **Ruta de acceso al archivo**, si desea que la regla controle el inicio de aplicaciones que se inicien utilizando archivos almacenados en la ruta especificada.
  - **Línea de comandos** si desea que la regla controle el inicio de los programas que se ejecutan utilizando los argumentos especificados en el campo de la línea de comandos. El campo se habilita después de que seleccione la opción **Ruta al archivo**. Puede usar los caracteres ? y * como una máscara al especificar los argumentos de la línea de comandos para los procesos iniciados como criterio.

Kaspersky Embedded Systems Security para Windows no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") para escribir la ruta de acceso correctamente.

Al especificar los objetos, puede usar los caracteres ? y * como máscaras de archivo.

Debe seleccionar al menos una opción. De lo contrario, no se agrega la regla Control de inicio de aplicaciones.

g. Si desea agregar exclusiones de la regla, realice lo siguiente:

1. En la sección **Exclusiones de la regla**, haga clic en el botón **Agregar**.

   Se abre la ventana **Exclusión de la regla**.

2. En el campo **Nombre**, ingrese el nombre de la exclusión.

3. Especifique la configuración para la exclusión de archivos de la aplicación de la regla de Control de inicio de aplicaciones. Puede llenar los campos de la configuración desde las propiedades del archivo si hace clic en el botón **Establecer exclusión a partir de las propiedades de un archivo**.

   - Certificado digital
   - Usar sujeto
   - Usar huella
   - hash SHA256

- Ruta de acceso al archivo

4. Haga clic en el botón **Aceptar**.

5. Si es necesario, repita los pasos (i) al (iv) para agregar exclusiones adicionales.

5. Haga clic en el botón **Aceptar** de la ventana **Configuración de la regla**.

La regla creada se mostrará en la lista de la ventana **Reglas de Control de inicio de aplicaciones**.

Habilitación del modo Habilitación predeterminada

El modo Habilitación predeterminada permite que todas las aplicaciones se inicien si no están bloqueados por reglas o por una conclusión de KSN de que no son confiables. Para activar el modo Habilitación predeterminada, agregue reglas de permiso específicas. Puede activar Habilitación predeterminada solo para scripts o para todos los archivos ejecutables.

Para agregar una regla de Habilitación predeterminada:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.

2. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Agregar una regla**.
   Se abre la ventana **Configuración de la regla**.

3. En el campo **Nombre**, ingrese el nombre de la regla.

4. En la lista desplegable **Tipo**, seleccione el tipo de regla **De autorización**.

5. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:

   - **Archivos ejecutables**, si desea que la regla controle el inicio de archivos ejecutables.
   - **Scripts y paquetes MSI**, si desea que la regla controle el inicio de scripts y paquetes MSI.

6. En el cuadro de grupo **Criterio de activación de la regla**, seleccione la opción **Ruta de acceso al archivo**.

7. Escriba la siguiente máscara: `?:\`

8. Haga clic en el botón **Configuración de la regla** de la ventana **Aceptar**.

Kaspersky Embedded Systems Security para Windows aplica el modo de Habilitación predeterminada.

Creación de reglas de autorización para Control de inicio de aplicaciones con los eventos de Kaspersky Security Center

Para crear reglas de autorización para Control de inicio de aplicaciones con los eventos de Kaspersky Security Center:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.

2. Haga clic en el botón **Agregar**.

3. En el menú contextual del botón, seleccione **Crear reglas de autorización para los eventos de Kaspersky Security Center**.

4. Seleccione el principio para agregar las reglas a la lista de reglas de Control de inicio de aplicaciones creadas previamente:

   - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.
   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

   Se abre la ventana **Generar reglas de Control de inicio de aplicaciones**.

5. Seleccione los tipos de eventos que la aplicación usará para crear las reglas de control de inicio de aplicaciones:

   - **Modo Solo estadísticas: inicio de aplicación denegado**.
   - **Inicio de la aplicación denegado**.

6. Seleccione un periodo en la lista desplegable **Solicitar eventos generados dentro del periodo**.

7. De ser necesario, en el campo **Usar eventos generados para un grupo de dispositivos administrados**, ingrese el nombre (o un fragmento del nombre) del grupo de dispositivos administrados por Kaspersky Security Center cuyos eventos se usarán de base para crear las reglas de control de inicio de aplicaciones.

8. Seleccione o desactive la casilla **Priorizar el uso del hash al generar reglas**.

   Si la casilla está seleccionada, Kaspersky Embedded Systems Security para Windows usa la suma de control del archivo para generar la regla cuando tanto la suma de control como el certificado del archivo están disponibles.

   Si la casilla está desactivada, Kaspersky Embedded Systems Security para Windows usa el certificado digital del archivo para generar la regla cuando tanto la suma de control como el certificado del archivo están disponibles.

9. Haga clic en el botón **Generar reglas**.

10. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de inicio de aplicaciones**.

    La lista de reglas en la tarea de Control de inicio de aplicaciones se completará con reglas nuevas generadas según un dato de sistema del dispositivo protegido con la Consola de administración de Kaspersky Security Center instalada.

    Las reglas con el mismo hash no se agregan, ya que todas las reglas de la lista deben ser únicas.

Importación de reglas desde el informe de Kaspersky Security Center sobre aplicaciones bloqueadas

Puede importar datos de inicios de la aplicación bloqueada desde el informe generado en Kaspersky Security Center después de la ejecución de la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** y usar estos datos para generar una lista de reglas de autorización de Control de inicio de aplicaciones en la directiva configurada.

Al generar un informe sobre eventos que ocurren durante la tarea de Control de inicio de aplicaciones, puede hacer un seguimiento de las aplicaciones cuyo inicio se bloquea.

Al importar datos de un informe sobre aplicaciones bloqueadas en la configuración de la directiva, asegúrese de que la lista que está usando solo contenga aplicaciones cuyo inicio desea autorizar.

Para especificar reglas de autorización de Control de inicio de aplicaciones para un grupo de dispositivos protegidos según un informe de aplicaciones bloqueadas de Kaspersky Security Center:

1. Abra la ventana **Control de inicio de aplicaciones**.
2. En el bloque **Modo de la tarea**, seleccione el modo **Solo estadísticas**.
3. En las propiedades de la directiva, en la sección **Notificación de eventos**, asegúrese de que:
   - Para eventos con nivel de importancia **Crítico**, el periodo por el que se conservarán los eventos **Inicio de la aplicación denegado** en el registro de tareas sea superior al periodo por el que planee ejecutar la tarea en modo **Solo estadísticas** (el valor predeterminado es de 30 días).
   - Para eventos con un nivel de importancia de **Advertencia**, el período de retención del registro de tareas para eventos de **Modo Solo estadísticas: inicio de aplicación denegado** supere el período planeado para ejecutar la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).

     Cuando el periodo de retención de eventos se agota, la información sobre los eventos registrados se elimina y no se refleja en el archivo del informe. Antes de ejecutar la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas**, asegúrese de que el tiempo de ejecución de la tarea no supere el período configurado para los eventos especificados.
4. Cuando la tarea haya finalizado, exporte los eventos registrados a un archivo TXT:
   a. En el espacio de trabajo del nodo **Servidor de administración** en Kaspersky Security Center, seleccione la pestaña **Eventos**.
   b. Haga clic en el nodo **Crear una selección** crear una selección de eventos basada en el criterio Bloqueado para ver las aplicaciones cuyo inicio bloqueará la tarea Control de inicio de aplicaciones.
   c. En el panel de resultados de la selección, haga clic en **Exportar eventos a archivo** para guardar el informe sobre inicios de la aplicación bloqueados en un archivo TXT.

   Antes de importar y aplicar el informe generado en una directiva, asegúrese de que el informe solo contenga datos sobre las aplicaciones cuyo inicio desea autorizar.
5. Importe datos sobre inicios de aplicación bloqueados en la tarea de Control de inicio de aplicaciones. Para hacerlo, en las propiedades de la directiva en la configuración de la tarea de Control de inicio de aplicaciones, realice lo siguiente:
   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

Se abre la ventana **Reglas de Control de inicio de aplicaciones**.

b. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Importar datos sobre aplicaciones bloqueadas del informe de Kaspersky Security Center**.

c. Seleccione el principio para agregar reglas desde la lista creada según el informe de Kaspersky Security Center a la lista de reglas de Control de inicio de aplicaciones configuradas anteriormente:

- **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.
- **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.

a. **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas. En la ventana estándar de Microsoft Windows que se abre, seleccione el archivo TXT al cual se exportaron los eventos del informe de inicios de aplicación bloqueados.

b. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de inicio de aplicaciones**.

Las reglas creadas a partir del informe de Kaspersky Security Center sobre aplicaciones bloqueadas se agregan a la lista de reglas de Control de inicio de aplicaciones.

Importación de reglas de Control de inicio de aplicaciones desde un archivo XML

Puede importar informes generados por la tarea de grupo de Generador de reglas de Control de inicio de aplicaciones y aplicarlos como una lista de reglas de autorización en la directiva que está configurando.

Cuando la tarea de grupo de Generador de reglas de Control de inicio de aplicaciones finaliza, la aplicación exporta las reglas de autorización creadas a archivos XML guardados en la carpeta compartida especificada. Cada archivo con una lista de reglas se crea analizando los archivos ejecutados y las aplicaciones iniciadas en cada dispositivo protegido independiente en la red corporativa. Las listas contienen reglas de autorización para archivos y aplicaciones cuyo tipo coincide con el tipo especificado en la tarea de grupo de Generador de reglas de Control de inicio de aplicaciones.

Para especificar las reglas de autorización del Control de inicio de aplicaciones para un grupo de dispositivos protegidos según una lista de reglas de autorización generada automáticamente:

1. En la pestaña **Tareas**, en el panel de detalles del grupo de dispositivos protegidos que está configurando, cree una tarea de grupo de Generador de reglas de control de inicio de aplicaciones o seleccione una tarea existente.

2. En las propiedades de la tarea de grupo de Generador de reglas de Control de inicio de aplicaciones creada o en el asistente de tareas, especifique la siguiente configuración:

   - En la sección **Notificación**, configure las opciones para guardar el informe de ejecución de la tarea.

     Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

   - En la sección **Configuración**, especifique los tipos de aplicaciones cuyo inicio será autorizado por las reglas que se crean. Puede modificar el conjunto de las carpetas que contienen aplicaciones autorizadas: excluya

carpetas predeterminadas del área de la tarea o agregue carpetas nuevas manualmente.

- En la sección **Opciones**, especifique las operaciones que deberá realizar la tarea mientras se esté ejecutando y después de que finalice. Especifique el criterio de generación de la regla y el nombre del archivo al cual se exportarán las reglas generadas.
- En la sección **Programación**, configure las opciones de programación de inicio de tareas.
- En la sección **Cuenta**, especifique la cuenta de usuario conforme a la cual se ejecutará la tarea.
- En la sección **Exclusiones del área de la tarea**, especifique los grupos de dispositivos protegidos que deben excluirse del área de la tarea.

  Kaspersky Embedded Systems Security para Windows no crea reglas de autorización para las aplicaciones iniciadas en los dispositivos protegidos excluidos.

3. En la pestaña **Tareas** en el panel de detalles del grupo de dispositivos protegidos configurados, en la lista de tareas de grupo, seleccione la tarea Generador de reglas de control de inicio de aplicaciones que creó y haga clic en el botón **Iniciar** para iniciar la tarea.

   Cuando la tarea termine, las listas de reglas de autorización generadas automáticamente se guardan en archivos de XML en una carpeta compartida.

   Antes de usar la tarea de Control de inicio de aplicaciones en la red, asegúrese de que todos los dispositivos protegidos puedan acceder a una carpeta compartida. Si la directiva de la organización no asegura el uso de una carpeta compartida en la red, le recomendamos iniciar la tarea Generador de reglas de Control de inicio de aplicaciones en un dispositivo protegido del grupo de dispositivos protegidos de prueba o en una máquina de referencia.

4. Para agregar las listas de reglas de autorización generadas a la tarea de Control de inicio de aplicaciones:

   a. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.

   b. Haga clic en el botón **Agregar** y, en la lista que se abre, seleccione **Importar reglas desde archivo XML**.

   c. Seleccione el principio para agregar las reglas de autorización generadas automáticamente a la lista de reglas de Control de inicio de aplicaciones creadas anteriormente:

   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.
   - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
     - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

   a. En la ventana estándar de Microsoft Windows que se abre, seleccione archivos de XML creados después de la finalización de la tarea de grupo de Generador de reglas de Control de inicio de aplicaciones.

   b. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de inicio de aplicaciones**.

5. Si desea aplicar las reglas creadas para controlar el inicio de aplicaciones, en la directiva en las propiedades de la tarea de Control de inicio de aplicaciones, seleccione el modo **Activo** para la tarea.

Las reglas de autorización generadas automáticamente según ejecuciones de la tarea en cada dispositivo protegido independiente se aplican a todos los dispositivos protegidos de red abarcados por la directiva configurada. En estos dispositivos protegidos, la aplicación solo permitirá el inicio de las aplicaciones para las cuales se crearon reglas de autorización.

Comprobación del inicio de aplicaciones

Antes de aplicar las reglas de Control de inicio de aplicaciones configuradas, puede probar cualquier aplicación para determinar qué reglas de Control de inicio de aplicaciones son provocadas por esa aplicación.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows deniega el inicio de las aplicaciones cuyo inicio no está autorizado por una sola regla. Para evitar la denegación del inicio de aplicaciones importantes, debe crear reglas de autorización para ellas.

Si el inicio de una aplicación está controlado por varias reglas de distintos tipos, se da prioridad a las reglas de denegación: el inicio de una aplicación se rechazará si corresponde a tan solo una regla de denegación.

Para evaluar las reglas de Control de inicio de aplicaciones:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. En la ventana que se abre, haga clic en el vínculo **Mostrar reglas del archivo**.

   Se abre la ventana de Microsoft Windows estándar.
3. Seleccione el archivo cuyo control de inicio desea evaluar.

   La ruta de acceso al archivo especificado se muestra en el campo de búsqueda. La lista contiene todas las reglas que se activarán cuando se inicie el archivo seleccionado.

Creación de la tarea Generador de reglas de control de inicio de aplicaciones

Para crear y configurar la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana **Configuración** en el Asistente de nueva tarea.
2. Configure las siguientes opciones:
   - Especifique un Prefijo para reglas.
   - Configure el área de aplicación de las reglas de autorización.
3. Haga clic en el botón **Siguiente**.
4. Especifique las acciones que Kaspersky Embedded Systems Security para Windows debe realizar:
   - durante la generación de las reglas de autorización
   - cuando se complete la tarea
5. En la sección **Programación**, configure el inicio programado de la tarea.

6. Haga clic en el botón **Siguiente**.
7. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desea utilizar.
8. Haga clic en el botón **Siguiente**.
9. Especifique el nombre de la tarea.
10. Haga clic en el botón **Siguiente**.

    El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos: " * < > & \ : |

    Se abre la ventana **Finalizar la creación de la tarea**.
11. Puede ejecutar la tarea opcionalmente después de que el Asistente finalice, seleccionando la casilla **Ejecutar tarea después de que finalice el asistente**.
12. Haga clic en **Finalizar** para terminar de crear la tarea.

Para configurar una regla existente en Kaspersky Security Center,

Abra la ventana **Propiedades: Generador de reglas de control de inicio de aplicaciones** y ajuste la configuración siguiendo las instrucciones de arriba.

La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Restricción del alcance de uso de la tarea

Para restringir el área de la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana **Propiedades:Generador de reglas de control de inicio de aplicaciones.**
2. Seleccione cómo crear reglas de autorización:
   - **Crear reglas de autorización para las aplicaciones en ejecución**
   - **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**
3. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada.

Acciones a realizar durante la generación de reglas automáticas

Para configurar las acciones que Kaspersky Embedded Systems Security para Windows debe realizar durante la ejecución de la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana **Propiedades: Generador de reglas de control de inicio de aplicaciones**.
2. Abra la pestaña **Opciones**.
3. En el bloque **Durante la generación de reglas de autorización**, configure las siguientes opciones:
   - **Usar certificado digital**
   - **Usar sujeto y huella digital del certificado digital**
   - **De no haber un certificado, usar**
     - **Hash SHA256**. El valor de la suma de control del archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.
     - **ruta de acceso al archivo**. La ruta de acceso al archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas especificada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas** en la sección **Configuración**.
   - **Usar hash SHA256**
   - **Generar reglas para este usuario o grupo de usuarios**.
4. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada.

Acciones a realizar después de la finalización de la generación de reglas automáticas

Para configurar las acciones que realizará Kaspersky Embedded Systems Security para Windows después de que finalice la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana **Propiedades: Generador de reglas de control de inicio de aplicaciones**.
2. Abra la pestaña **Opciones**.
3. En la sección **Después de completada la tarea**, configure las siguientes opciones:
   - **Agregar reglas de autorización a la lista de reglas de Control de inicio de aplicaciones**.
   - **Principio de adición**.
   - **Exportar reglas de autorización a archivo**.
   - **Agregar detalles del dispositivo protegido al nombre del archivo**.
4. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada.

Gestión de Control de inicio de aplicaciones a través de la Consola de la aplicación

En esta sección, aprenderá a navegar por la interfaz de la Consola de la aplicación y a definir la configuración de la tarea en un dispositivo protegido.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la tarea Control de inicio de aplicaciones

Para abrir la configuración de la tarea general de Control de inicio de aplicaciones a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de inicio de aplicaciones**.
3. En el panel de detalles del nodo secundario de **Control de inicio de aplicaciones**, haga clic en el vínculo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

Cómo abrir la ventana de las reglas de Control de inicio de aplicaciones

Para abrir la lista de reglas de Control de inicio de aplicaciones a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de inicio de aplicaciones**.
3. En el panel de resultados del nodo **Control de inicio de aplicaciones**, haga clic en el vínculo **Reglas de Control de inicio de aplicaciones**.

   Se abre la ventana **Reglas de Control de inicio de aplicaciones**.
4. Configure la lista de reglas como sea necesario.

Cómo abrir la configuración de la tarea Generador de reglas de Control de inicio de aplicaciones

Para configurar la tarea Generador de reglas de Control de inicio de aplicaciones:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Generadores automatizados de reglas**.
2. Seleccione el nodo secundario **Generador de reglas de control de inicio de aplicaciones**.
3. En el panel de resultados del nodo secundario **Generador de reglas de control de inicio de aplicaciones**, haga clic en el vínculo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
4. Configure la tarea como sea necesario.

Configuración de la tarea Control de inicio de aplicaciones

Para ajustar la configuración general de la tarea Control de inicio de aplicaciones:

1. Abra la ventana **Configuración de tareas**.
2. Defina los siguientes valores de configuración de tarea:
   - En la pestaña **General**:
     - Modo de la tarea Control de inicio de aplicaciones.
     - El área de aplicación de la regla en la tarea.
     - Uso de KSN.
   - La configuración de Control de distribución de software en la pestaña **Control de distribución de software**.
   - La configuración de la programación de inicio de tareas en las pestañas **Programación** y **Avanzado**.
3. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

   La configuración modificada se guarda.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Selección del modo de la tarea Control de inicio de aplicaciones

Para configurar el modo de la tarea de Control de inicio de aplicaciones:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **General**, en la lista desplegable **Modo de la tarea**, especifique el modo de la tarea.
3. Desactive o seleccione la casilla de verificación **Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo**.

Kaspersky Embedded Systems Security para Windows crea una nueva lista de eventos en caché cada vez que se modifica la configuración de la tarea de Control de inicio de aplicaciones. Esto significa que el Control de inicio de aplicaciones se realiza según la configuración de seguridad actual.

4. Desactive o seleccione la opción **Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar**.
5. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Todos los intentos de iniciar aplicaciones se registran en el registro de tareas.

Configuración del área de la tarea de Control de inicio de aplicaciones

Para definir el área de la tarea de Control de inicio de aplicaciones:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **General**, en el bloque **Área de aplicación de la regla**, defina los siguientes ajustes:
   - **Aplicar reglas a archivos ejecutables**
   - **Supervisar la carga de módulos DLL**

     El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.

   - **Aplicar reglas a scripts y paquetes MSI**
3. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Configuración del uso de KSN

Para configurar los servicios de uso de KSN para la tarea de Control de inicio de aplicaciones:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **General**, en el bloque **Uso de KSN**, defina los ajustes que controlan el uso de los servicios de KSN:
   - Si es necesario, seleccione la casilla de verificación **Denegar inicio de aplicaciones no confiables según KSN**.
   - Si es necesario, seleccione la casilla de verificación **Autorizar inicio de aplicaciones confiables según KSN**.

- Si se la casilla de verificación **Autorizar inicio de aplicaciones confiables según KSN** está seleccionada, indique los usuarios o los grupos de usuarios que pueden iniciar las aplicaciones de confianza en KSN. Para ello, realice las siguientes acciones:

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

  Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.

  > De forma predeterminada, el acceso a los programas de confianza en KSN está permitido para todos los usuarios.

  b. Especifique la lista de usuarios o grupos de usuarios.

  c. Haga clic en el botón **Aceptar**.

3. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Configuración del Control de distribución de software

Para agregar un paquete de distribución de confianza a través de la Consola de la aplicación:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **Control de distribución de software**, seleccione la casilla de verificación **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**.

   > Puede seleccionar **Permitir la distribución automática de software mediante las aplicaciones y los paquetes de la lista**, si la casilla de verificación **Control de inicio de aplicaciones** en la pestaña **Aplicar reglas a archivos ejecutables** está seleccionada en la configuración de la tarea **General**.

3. Desactive la casilla de verificación **Permitir siempre la distribución de software a través de Windows Installer** si es necesario.

   > Solo se recomienda desactivar la casilla **Permitir siempre la distribución de software a través de Windows Installer** si es absolutamente necesario. Desactivar esta función puede causar errores al actualizar archivos del sistema operativo y también impedir el inicio de archivos extraídos de un paquete de distribución.

4. Si es necesario, seleccione la casilla de verificación **Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service**.

   > La aplicación controla el ciclo de distribución del software en el dispositivo protegido; desde la entrega del paquete hasta la instalación o actualización. La aplicación no controla procesos si alguna etapa de distribución se realizara antes de la instalación de la aplicación en el dispositivo protegido.

5. Para crear la lista de autorizados o editar la lista existente de paquetes de distribución de confianza, haga clic en **Modificar la lista de paquetes** y seleccione uno de los siguientes métodos en la ventana que se abre:

- **Agregar un paquete de distribución**.

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

  b. Seleccione el archivo ejecutable o el paquete de distribución.

  El bloque **Criterios de confianza** se completa automáticamente con datos sobre el archivo seleccionado.

  c. Desactive o seleccione la casilla de verificación **Permitir la distribución adicional de los programas creados desde este paquete de distribución**.

  d. Seleccione una de dos opciones disponibles para criterios para usar para determinar si un archivo o el paquete de distribución es de confianza:

  - **Usar certificado digital**
  - **Usar hash SHA256**

- **Agregar varios paquetes por hash**

  Puede seleccionar un número ilimitado de archivos de ejecutables y paquetes de distribución, y agregarlos a la lista al mismo tiempo. Kaspersky Embedded Systems Security para Windows examina el hash y permite que el sistema operativo inicie los archivos especificados.

- **Cambiar el paquete seleccionado**

  Use esta opción para seleccionar otro archivo de inicio o paquete de distribución, o bien para cambiar los criterios de confianza.

- Importar lista de paquetes de distribución desde el archivo.

  En la ventana **Abrir**, especifique el archivo de configuración que contiene una lista de paquetes de distribución de confianza.

Si crea un paquete de distribución de confianza basado en un archivo ejecutable luego de agregar, en la configuración de la Zona de confianza, un proceso basado en ese mismo archivo ejecutable que luego designó como de confianza para la tarea Control de inicio de aplicaciones, la configuración de la Zona de confianza tendrá mayor prioridad. Kaspersky Embedded Systems Security para Windows no permitirá iniciar el archivo ejecutable, pero considerará que el proceso de dicho archivo es de confianza.

6. Si desea eliminar una aplicación o un paquete de distribución anteriormente agregados a la lista de confianza, haga clic en el botón **Eliminar paquetes de distribución**. Se podrán ejecutar los archivos extraídos.

Para impedir que los archivos extraídos se inicien, desinstale la aplicación en el dispositivo protegido o cree una regla de denegación en la configuración de la tarea Control de inicio de aplicaciones.

7. Haga clic en el botón **Aceptar**.

Se guarda la configuración especificada.

Configuración de las reglas de Control de inicio de aplicaciones

Aprenda cómo generar, importar y exportar una lista de reglas o crear manualmente reglas de autorización o denegación utilizando la tarea de Control de inicio de aplicaciones.

Adición de una regla de Control de inicio de aplicaciones

Para agregar una regla de Control de inicio de aplicaciones mediante la Consola de la aplicación:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Agregar una regla**.

   Se abre la ventana **Configuración de la regla**.
4. Especifique la siguiente configuración:
   a. En el campo **Nombre**, ingrese el nombre de la regla.
   b. En la lista desplegable **Tipo**, seleccione el tipo de regla:
      - **De autorización**, si desea que la regla autorice el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de la regla.
      - **De denegación**, si desea que la regla bloquee el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de la regla.
   c. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
      - **Archivos ejecutables**, si desea que la regla controle el inicio de archivos ejecutables.
      - **Scripts y paquetes MSI**, si desea que la regla controle el inicio de scripts y paquetes MSI.
   d. En el campo **Usuario o grupo de usuarios**, indique los usuarios que podrán o no iniciar aplicaciones, dependiendo del tipo de regla.
      1. En el menú contextual del botón **Examinar**, seleccione el método que desee usar para agregar usuarios de confianza.

         Se abre la ventana **Selección de usuario o grupo de usuarios**.
      2. Seleccione un usuario o un grupo de usuarios.
      3. Haga clic en el botón **Aceptar**.
   e. Si desea tomar los valores de los criterios de activación de la regla enumerados en el bloque **Criterio de activación de la regla** de un archivo, haga lo siguiente:
      1. Haga clic en el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**.

Se abre la ventana estándar **Abrir** de Microsoft Windows.

2. Seleccione el archivo.

3. Haga clic en el botón **Abrir**.

   El valor de los criterios contenidos en el archivo se muestra en los campos del bloque **Criterio de activación de la regla**. El criterio para el cual están disponibles los datos en las propiedades del archivo se selecciona de forma predeterminada.

f. En el cuadro de grupo **Criterio de activación de la regla**, seleccione una o varias de las siguientes opciones aplicables:

- **Certificado digital**, si desea que la regla controle el inicio de aplicaciones que se ejecuten utilizando archivos firmados con un certificado digital:
  - Seleccione la casilla de verificación **Usar sujeto** si desea que la regla controle el inicio de archivos firmados con un certificado digital que tengan el sujeto especificado.
  - Seleccione la casilla de verificación **Usar huella** si desea que la regla controle solo el inicio de archivos firmados con un certificado digital con la huella especificada.
- **hash SHA256**, si desea que la regla controle el inicio de aplicaciones que se inicien utilizando archivos cuya suma de control coincida con la especificada.
- **Ruta de acceso al archivo**, si desea que la regla controle el inicio de aplicaciones que se inicien utilizando archivos almacenados en la ruta especificada.
  - **Línea de comandos** si desea que la regla controle el inicio de los programas que se ejecutan utilizando los argumentos especificados en el campo de la línea de comandos. El campo se habilita después de que seleccione la opción **Ruta al archivo**. Puede usar los caracteres ? y * como una máscara al especificar los argumentos de la línea de comandos para los procesos iniciados como criterio.

> Kaspersky Embedded Systems Security para Windows no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida ("\") para escribir la ruta de acceso correctamente.

> Al especificar los objetos, puede usar los caracteres ? y * como máscaras de archivo.

Debe seleccionar al menos una opción. De lo contrario, no se agrega la regla Control de inicio de aplicaciones.

g. Si desea agregar exclusiones de la regla, realice lo siguiente:

1. En la sección **Exclusiones de la regla**, haga clic en el botón **Agregar**.

   Se abre la ventana **Exclusión de la regla**.

2. En el campo **Nombre**, ingrese el nombre de la exclusión.

3. Especifique la configuración para la exclusión de archivos de la aplicación de la regla de Control de inicio de aplicaciones. Puede llenar los campos de la configuración desde las propiedades del archivo si hace clic en el botón **Establecer exclusión a partir de las propiedades de un archivo**.

   - Certificado digital

- Usar sujeto
- Usar huella
- hash SHA256
- Ruta de acceso al archivo

4. Haga clic en el botón **Aceptar**.
5. Si es necesario, repita los pasos (i) al (iv) para agregar exclusiones adicionales.

5. Haga clic en el botón **Aceptar** de la ventana **Configuración de la regla**.

La regla creada se mostrará en la lista de la ventana **Reglas de Control de inicio de aplicaciones**.

Habilitación del modo Habilitación predeterminada

El modo Habilitación predeterminada permite que todas las aplicaciones se inicien si no están bloqueados por reglas o por una conclusión de KSN de que no son confiables. Para activar el modo Habilitación predeterminada, agregue reglas de permiso específicas. Puede activar Habilitación predeterminada solo para scripts o para todos los archivos ejecutables.

Para agregar una regla de Habilitación predeterminada:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Agregar una regla**.
   Se abre la ventana **Configuración de la regla**.
4. En el campo **Nombre**, ingrese el nombre de la regla.
5. En la lista desplegable **Tipo**, seleccione el tipo de regla **De autorización**.
6. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
   - **Archivos ejecutables**, si desea que la regla controle el inicio de archivos ejecutables.
   - **Scripts y paquetes MSI**, si desea que la regla controle el inicio de scripts y paquetes MSI.
7. En el cuadro de grupo **Criterio de activación de la regla**, seleccione la opción **Ruta de acceso al archivo**.
8. Escriba la siguiente máscara: `?:\`
9. Haga clic en el botón **Configuración de la regla** de la ventana **Aceptar**.

Kaspersky Embedded Systems Security para Windows aplica el modo de Habilitación predeterminada.

Creación de reglas de autorización desde eventos de la tarea de Control de inicio de aplicaciones

Para crear un archivo de configuración que contenga reglas de autorización generadas desde eventos de la tarea de Control de inicio de aplicaciones:

1. Inicie la tarea Control de inicio de aplicaciones en el modo **Solo estadísticas** para que, en el registro de tareas, se guarde información sobre todos los inicios de aplicaciones que sucedan en un dispositivo protegido.

2. Una vez que la tarea complete su ejecución en modo **Solo estadísticas**, abra el registro de tareas. Para ello, haga clic en el botón **Abrir el registro de tareas** en el bloque **Administración** del panel de detalles del nodo **Control de inicio de aplicaciones**.

3. En la ventana **Registros**, haga clic en **Generar reglas basadas en los eventos**.

   Kaspersky Embedded Systems Security para Windows generará un archivo XML de configuración que contendrá la lista de reglas según los eventos de la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas**. Puede aplicar esta lista de reglas en la tarea Control de inicio de aplicaciones.

Antes de aplicar la lista de reglas generada desde los eventos de la tarea registrados, le recomendamos que revise y procese manualmente la lista para estar seguro que el inicio de archivos críticos (por ejemplo, archivos de sistema) esté autorizado por las reglas especificadas.

Todos los eventos de la tarea se registran en el registro de tareas sin tener en cuenta el modo de la tarea. Puede generar un archivo de configuración con una lista de reglas basado en el registro creado para la tarea que se ejecuta en el modo **Activo**. Este escenario no se recomienda excepto en casos urgentes, porque se debe generar una lista de la regla final antes de que la tarea se ejecute en el modo **Activo** para que sea eficaz.

Exportación de Reglas de Control de inicio de aplicaciones

Para exportar reglas de Control de inicio de aplicaciones a un archivo de configuración:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.

2. Haga clic el botón **Exportar a archivo**.

   Se abre la ventana de Microsoft Windows estándar.

3. En la ventana que se abre, especifique el archivo al cual desea exportar las reglas. Si no existe tal archivo, este se creará. Si ya existe un archivo con el nombre especificado, su contenido se sobrescribirá cuando se exporten las reglas.

4. Haga clic en el botón **Guardar**.

   La configuración de la regla se exportará al archivo especificado.

Importación de reglas de Control de inicio de aplicaciones desde un archivo XML

Para importar las reglas de Control de inicio de aplicaciones:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.

2. Haga clic en el botón **Agregar**.

3. En el menú contextual del botón, seleccione **Importar reglas desde archivo XML**.

4. Especifique el método para agregar reglas importadas. Para hacerlo, seleccione una de las opciones del menú contextual del botón **Importar reglas desde archivo XML**:

   - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.
   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

   Se abre la ventana estándar **Abrir** de Microsoft Windows.

5. En la ventana **Abrir**, seleccione el archivo XML que contiene las reglas de Control de inicio de aplicaciones.

6. Haga clic en el botón **Abrir**.

Las reglas importadas se mostrarán en la lista en la ventana **Reglas de Control de inicio de aplicaciones**.

Eliminación de Reglas de Control de inicio de aplicaciones

Para eliminar las Reglas de Control de inicio de aplicaciones:

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.

2. En la lista, seleccione una o más reglas que desee eliminar.

3. Haga clic en el botón **Eliminar seleccionadas**.

4. Haga clic en el botón **Guardar**.

Las Reglas de Control de inicio de aplicaciones seleccionadas se eliminan.

Configuración de una tarea de Generador de reglas de Control de inicio de aplicaciones

Para configurar los ajustes de la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana Configuración de tareas en la tarea **Generador de reglas de control de inicio de aplicaciones**.

2. Configure las siguientes opciones:

   - En la pestaña **General**:
     - Especifique un **Prefijo para reglas**.
     - Configure el área de aplicación de las reglas de autorización.

- En la pestaña **Acciones**, especifique las acciones que Kaspersky Embedded Systems Security para Windows debe realizar.
- En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de la tarea.
- En la pestaña **Ejecutar como**, configure las Opciones de inicio de tareas con permisos de la cuenta.

3. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación.

Restricción del alcance de uso de la tarea

Para restringir el área de la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana **Configuración de tareas** en la tarea **Generador de reglas de control de inicio de aplicaciones**.
2. Seleccione cómo crear reglas de autorización:
   - **Crear reglas de autorización para las aplicaciones en ejecución**.
   - **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**.
3. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Acciones a realizar durante la generación de reglas automáticas

Para configurar las acciones de Kaspersky Embedded Systems Security para Windows durante la ejecución y tras la finalización de la tarea Generador de reglas de control de inicio de aplicaciones, realice lo siguiente:

1. Abra la ventana **Configuración de tareas** en la tarea **Generador de reglas de control de inicio de aplicaciones**.
2. Abra la pestaña **Opciones**.
3. En el bloque **Durante la generación de reglas de autorización**, configure las siguientes opciones:
   - **Usar certificado digital**
   - **Usar sujeto y huella digital del certificado digital**
   - **De no haber un certificado, usar**
     - **Hash SHA256**. El valor de la suma de control del archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.

- **ruta de acceso al archivo**. La ruta de acceso al archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas especificada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas** en la sección **Configuración**.

- Usar hash SHA256.
- Generar reglas para este usuario o grupo de usuarios.

4. En la sección **Después de completada la tarea**, configure las siguientes opciones:
   - Agregar reglas de autorización a la lista de reglas de Control de inicio de aplicaciones.
   - Principio de adición.
   - **Exportar reglas de autorización a archivo**.
   - Agregar detalles del dispositivo protegido al nombre del archivo.
5. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Acciones a realizar después de la finalización de la generación de reglas automáticas

Para configurar las acciones que realizará Kaspersky Embedded Systems Security para Windows después de que finalice la tarea de Generador de reglas de Control de inicio de aplicaciones:

1. Abra la ventana Configuración de tareas en la tarea **Generador de reglas de control de inicio de aplicaciones**.
2. Abra la pestaña **Opciones**.
3. En la sección **Después de completada la tarea**, configure las siguientes opciones:
   - Agregar reglas de autorización a la lista de reglas de Control de inicio de aplicaciones.
   - Principio de adición.
   - **Exportar reglas de autorización a archivo**.
   - Agregar detalles del dispositivo protegido al nombre del archivo.
4. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Administración del Control de inicio de aplicaciones a través del Complemento web

Para configurar las tareas de Control de inicio de aplicaciones a través del Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Control de actividad local**.
5. Haga clic en el botón **Configuración** en la subsección **Control de inicio de aplicaciones**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de la tarea Control de inicio de aplicaciones

Configuración	Descripción
Modo de la tarea.	En esta lista desplegable, puede seleccionar el modo de la tarea Control de inicio de aplicaciones: • **Activo**. Kaspersky Embedded Systems Security para Windows utiliza las reglas especificadas para controlar el inicio de cualquier aplicación. • **Solo estadísticas**. Kaspersky Embedded Systems Security para Windows no utiliza las reglas de Control de inicio de aplicaciones. Solo guarda información sobre el inicio de las aplicaciones en el registro de la tarea. Se permite el inicio de todas las aplicaciones. Puede usar este modo para generar una lista de Reglas de Control de inicio de aplicaciones sobre la base de la información sobre los inicios de aplicaciones denegados en el registro de tareas. De forma predeterminada, la tarea Control de inicio de aplicaciones se ejecuta en el modo **Solo estadísticas**.
Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo	La casilla de verificación habilita o deshabilita el control del inicio para los intentos segundos y subsecuentes de iniciar aplicaciones sobre la base de la información sobre eventos almacenada en el caché. Si la casilla está activada, Kaspersky Embedded Systems Security para Windows permite o impide que se ejecute una aplicación basándose en la conclusión a la que arriba la tarea en el primer inicio de la aplicación. Por ejemplo, si las reglas autorizaron el primer inicio de la aplicación, la información sobre esta decisión se almacenará en el caché, y el segundo inicio y todos los inicios subsecuentes también se autorizarán, sin volver a comprobarlo. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows analiza una aplicación cada vez que se intenta el inicio. De forma predeterminada, la casilla no está activada.
Denegar el inicio de los intérpretes de comando si no tienen ningún comando que ejecutar	Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security para Windows deniega el inicio del intérprete de línea de comando aunque el inicio del intérprete esté permitido. Para que se permita el inicio de un intérprete de comandos sin comando, deben cumplirse las dos siguientes condiciones: • El inicio del intérprete de línea de comando está autorizado. • El comando para ejecutar está autorizado.

	Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security para Windows solo considera las reglas de autorización para el inicio de un intérprete de línea de comando. El inicio se deniega si no se aplica ninguna regla de autorización o el proceso ejecutable no es de confianza para KSN. Si se aplica una regla de autorización o el proceso es de confianza para KSN, se puede iniciar un intérprete de línea de comando con o sin comando para ejecutar. Kaspersky Embedded Systems Security para Windows reconoce los siguientes intérpretes de línea de comandos: • cmd.exe • powershell.exe • python.exe • perl.exe De forma predeterminada, la casilla no está activada.
Aplicar reglas a archivos ejecutables	La casilla activa o desactiva el control de inicio de archivos ejecutables. Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows autoriza o bloquea el inicio de archivos ejecutables mediante las reglas especificadas cuya configuración especifica **Archivos ejecutables** como alcance. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no controla el inicio de los archivos ejecutables utilizando las reglas especificadas. Se autoriza el inicio de archivos ejecutables. De forma predeterminada, la casilla está activada.
Supervisar la carga de módulos DLL	La casilla activa o desactiva el control de la carga de módulos DLL. Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows autoriza o bloquea las cargas de módulos DLL mediante las reglas especificadas cuya configuración especifica **Archivos ejecutables** como alcance. Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no controla la carga de módulos DLL mediante las reglas especificadas. Se autoriza la carga de módulos DLL. La casilla de verificación está activa si la casilla de verificación **Aplicar reglas a archivos ejecutables** está seleccionada. De forma predeterminada, la casilla está activada.
Aplicar reglas a scripts y paquetes MSI	La casilla de verificación habilita o deshabilita el inicio de scripts y paquetes MSI. Si esta casilla de verificación está activada, Kaspersky Embedded Systems Security para Windows permite o impide la ejecución de scripts y paquetes MSI basándose en las reglas especificadas que tengan la opción **Scripts y paquetes MSI** configurada como área. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no controla el inicio de scripts y paquetes MSI mediante las reglas especificadas. Se autoriza el inicio de scripts y paquetes MSI. De forma predeterminada, la casilla está activada.
Denegar inicio de aplicaciones no confiables según KSN	La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según los datos de reputación de la aplicación en KSN.

	Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows bloquea la ejecución de cualquier aplicación si no es de confianza en KSN. Las reglas de autorización de Control de inicio de aplicaciones que se aplican a aplicaciones que no son de confianza en KSN no se iniciarán. Si selecciona la casilla de verificación, se proporciona protección adicional contra el malware. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no toma en cuenta la reputación de aplicaciones que no son de confianza en KSN y autoriza o bloquea el inicio de acuerdo con las reglas que se aplican a tales aplicaciones. De forma predeterminada, la casilla no está activada.
Autorizar inicio de aplicaciones confiables según KSN	La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según los datos de reputación de la aplicación en KSN. Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security para Windows permite que las aplicaciones se ejecuten si son de confianza en KSN. Las reglas de Control de inicio de aplicaciones que realizan una acción de bloqueo y que afectan a las aplicaciones que KSN considera de confianza tienen mayor prioridad: si los servicios de KSN consideran que una aplicación es de confianza, el inicio de dicha aplicación se bloqueará. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security para Windows no toma en cuenta la reputación de aplicaciones de confianza en KSN y autoriza o deniega el inicio de acuerdo con las reglas que se aplican a tales aplicaciones. De forma predeterminada, la casilla no está activada.
Usuarios o grupos de usuarios que podrán ejecutar aplicaciones confiables según KSN	Si la casilla de verificación **Autorizar inicio de aplicaciones confiables según KSN** está seleccionada, aquí puede especificar usuarios y grupos de usuarios autorizados para iniciar aplicaciones en las que confía KSN. De forma predeterminada, se especifican los siguientes usuarios: **Todos** y **NT AUTHORITY\SYSTEM**.
Reglas	Configure las reglas de autorización o denegación para la tarea Control de inicio de aplicaciones.
Control de distribución de software	Puede agregar paquetes de distribución de confianza.
Administración de tareas	Puede configurar las opciones para iniciar la tarea en base a una programación.

Control de dispositivos

Esta sección contiene información acerca de la tarea Control de dispositivos y cómo configurarla.

Acerca de la tarea Control de dispositivos

Kaspersky Embedded Systems Security para Windows controla el registro y el uso de dispositivos externos y unidades de CD/DVD para proteger el dispositivo contra las amenazas a la seguridad informática asociadas al intercambio de archivos con unidades flash u otros tipos de dispositivos externos conectados mediante USB.

Kaspersky Embedded Systems Security para Windows controla las siguientes conexiones de dispositivos externos de USB:

- Unidades flash USB, incluidas las que son compatibles con UAS
- Unidades de CD/DVD ROM
- Unidades de discos flexibles conectadas mediante USB
- Adaptadores de red conectados mediante USB
- Dispositivos móviles MTP conectados mediante USB

Kaspersky Embedded Systems Security para Windows le informa sobre todos los dispositivos conectados mediante USB con el correspondiente evento en los registros de tareas y eventos. Los detalles de los eventos incluyen el tipo de dispositivo y la ruta de acceso de la conexión. Cuando se inicia la tarea de control de dispositivos, Kaspersky Embedded Systems Security para Windows comprueba y enumera todos los dispositivos conectados mediante USB. Puede configurar las notificaciones en la sección de configuración de notificaciones de Kaspersky Security Center.

La tarea Control de dispositivos supervisa todos los intentos de conexiones de dispositivos externos a un dispositivo protegido mediante USB y bloquea la conexión si no hay reglas de autorización para tales dispositivos. Después de que se bloquea la conexión, el dispositivo no está disponible.

La aplicación asigna uno de los siguientes estados a cada dispositivo externo conectado:

- *Confiable*. Dispositivo para el cual desea permitir el intercambio de archivos. Después de la generación de la lista de reglas, el valor de la *Ruta de acceso a la instancia del dispositivo* se incluye en el alcance de uso para al menos una regla.
- *Dudoso*. Dispositivo para el cual desea restringir el intercambio de archivos. La ruta de acceso a la instancia del dispositivo no se incluye en ninguna área de aplicación de las reglas de autorización.

Puede crear reglas de autorización para que el dispositivo externo autorice el intercambio de datos a través del uso de la tarea de Generador de reglas para Control de dispositivos. También puede ampliar el área de aplicación de las reglas de autorización que ya haya creado. No puede crear reglas de autorización manualmente.

Kaspersky Embedded Systems Security para Windows identifica dispositivos externos registrados en el sistema con el valor Ruta de acceso a la instancia del dispositivo. La ruta de acceso a la instancia del dispositivo es una función predeterminada especificada únicamente para cada dispositivo externo. El valor de la ruta de acceso a la instancia del dispositivo aparece en las propiedades de Windows de cada dispositivo externo. Kaspersky Embedded Systems Security para Windows determina cuál es este valor automáticamente durante la generación de reglas.

La tarea de Control de dispositivos puede funcionar en dos modos:

- **Activar**. Kaspersky Embedded Systems Security para Windows aplica reglas para controlar la conexión de unidades flash y otros dispositivos externos, y autoriza o bloquea el uso de todos los dispositivos según el principio de denegación predeterminada y las reglas de autorización especificadas. Se autoriza el uso de dispositivos externos de confianza. El uso de dispositivos externos dudosos sea bloquea de forma predeterminada.

  Si un dispositivo externo que se considera dudoso se conecta a un dispositivo protegido antes de que la tarea Control de dispositivos comience a ejecutarse en modo **Activar**, la aplicación no bloqueará el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el dispositivo protegido. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.

- **Solo estadísticas**. Kaspersky Embedded Systems Security para Windows no controla la conexión de unidades flash ni otros dispositivos externos, sino que solo registra la información sobre la conexión y el registro de dispositivos externos en un dispositivo protegido y sobre las reglas de autorización de Control de dispositivos que activan los dispositivos conectados. Se autoriza el uso de todos los dispositivos externos. Este modo está configurado de forma predeterminada.

  Puede aplicar este modo para la generación de reglas según la información sobre bloqueos de dispositivos registrada durante la ejecución de la tarea.

Acerca de las Reglas de Control de dispositivos

Kaspersky Embedded Systems Security para Windows no aplica reglas de autorización para dispositivos móviles conectados a MTP.

Las reglas se generan de manera única para cada dispositivo conectado en ese momento o que se haya conectado alguna vez a un dispositivo protegido si la información sobre este dispositivo se almacena en el registro del sistema.

Para generar reglas de autorización para el control de dispositivos:

- Aplicar la tarea de Generador de reglas para Control de dispositivos.
- Ejecute la tarea Control de dispositivos en el modo Solo estadísticas.
- Aplique la información del sistema sobre dispositivos conectados anteriormente.
- Ampliar el área de aplicación de la regla ya especificadas.

Kaspersky Embedded Systems Security para Windows admite una cantidad máxima cantidad de 3072 reglas de control de dispositivos.

Las reglas de control de dispositivos se describen a continuación.

Tipo de regla

El tipo de regla siempre es *de autorización*. De forma predeterminada, la tarea Control de dispositivos bloquea todas las conexiones de unidades flash y de otros dispositivos externos si estos dispositivos no se incluyen en ninguna área de aplicación de las reglas de autorización.

Criterio de activación y área de aplicación de la regla

Las reglas de Control de dispositivos identifican las unidades flash y otros dispositivos externos según la *Ruta de acceso a la instancia del dispositivo*. La ruta de acceso a la instancia del dispositivo es un criterio único que el sistema asigna a un dispositivo cuando este se conecta y se registra como dispositivo externo o unidad de CD/DVD (por ejemplo, IDE o SCSI).

Kaspersky Embedded Systems Security para Windows controla la conexión de unidades de CD/DVD externas sin tener en cuenta el bus usado para la conexión. Al montar el dispositivo mediante USB, el sistema operativo registra dos valores de ruta de acceso a la instancia del dispositivo: uno para el dispositivo externo y otro para la unidad de CD/DVD (por ejemplo, IDE o SCSI). Para conectar estos dispositivos correctamente, se deben configurar las reglas de autorización para cada valor de ruta de acceso a la instancia.

Kaspersky Embedded Systems Security para Windows define automáticamente la ruta de acceso a la instancia del dispositivo y analiza el valor obtenido en los elementos siguientes:

- fabricante del dispositivo (VID);
- tipo de controlador del dispositivo (PID);
- número de serie del dispositivo.

No puede configurar la ruta de acceso a la instancia del dispositivo manualmente. Los criterios de activación de la regla de autorización definen el área de aplicación de la regla. De manera predeterminada, cuando se crea una regla de autorización, su área de aplicación se limita al dispositivo inicial al que corresponden las propiedades con las que Kaspersky Embedded Systems Security para Windows generó la regla. Puede configurar los valores en la configuración de la regla creada usando una máscara para ampliar el área de aplicación de la regla.

Valores iniciales del dispositivo

Propiedades del dispositivo que Kaspersky Embedded Systems Security para Windows usó para la generación de reglas de autorización y que se muestran en el Administrador de dispositivos de Windows para cada dispositivo conectado.

Los valores iniciales del dispositivo contienen la siguiente información:

- **Ruta de acceso a la instancia del dispositivo**. Kaspersky Embedded Systems Security para Windows utiliza esta propiedad para definir los criterios de activación de las reglas y completar los campos **Fabricante (VID)**, **Tipo de controlador (PID)** y **Número de serie** en el bloque **Área de aplicación de la regla** de la ventana **Propiedades de la regla**.
- **Nombre descriptivo**. Nombre del dispositivo que está configurado en las propiedades del dispositivo por su fabricante.

Kaspersky Embedded Systems Security para Windows automáticamente define valores iniciales del dispositivo cuando la regla se está generando. Más tarde, puede usar estos valores para reconocer el dispositivo que se utilizó como base para la generación de la regla. Los valores iniciales del dispositivo no están disponibles para su modificación.

Descripción

Puede agregar información adicional para cada regla de Control de dispositivos creada en el campo **Descripción**; por ejemplo, puede anotar el nombre de la unidad de memoria conectada o el nombre de su propietario. El comentario se mostrará en el campo correspondiente de la ventana **Reglas de Control de dispositivos**.

La descripción y los valores iniciales del dispositivo no tienen permitida la activación de reglas y se asignan solo para simplificar la identificación del dispositivo por parte del usuario.

Acerca del Generador de reglas para Control de dispositivos

Puede importar reglas de autorización de control de dispositivos de los archivos XML que se generaron automáticamente durante la ejecución de las tareas de Control de dispositivos o de Generador de reglas para Control de dispositivos.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows no permite conectar ninguna unidad de memoria flash ni ningún otro dispositivo externo que no se haya incluido en el área de aplicación de las reglas de control de dispositivos especificadas.

Propósitos y escenarios para generar reglas de control de dispositivos

Escenario de generación de reglas	Objetivo
Tarea de Generador de reglas para Control de dispositivos	• Agregue reglas de autorización de dispositivos de confianza conectados anteriormente antes del primer inicio de la tarea de Control de dispositivos. • Genere una lista de reglas para dispositivos de confianza en la red de dispositivos protegidos.
Generación de reglas según datos de sistema	Agregue reglas de autorización para uno o varios dispositivos externos, cuyos datos se hayan almacenado en el sistema.
Generación de reglas basadas en datos sobre los dispositivos conectados actualmente	Renueve una lista de reglas ya especificada cuando es necesario confiar en una cantidad pequeña de dispositivos externos nuevos.
La tarea Control de dispositivos en el modo **Solo estadísticas**	Genere reglas de autorización para un gran número de dispositivos de confianza.

Uso de la tarea de Generador de reglas para control de dispositivos

El archivo XML, generado después de la finalización de la tarea de Generador de reglas para Control de dispositivos, contiene reglas de autorización para las unidades flash y otros dispositivos externos cuyos datos se han almacenado en un registro del sistema.

Utilice este escenario durante el proceso de generación de reglas para tener en cuenta todos los dispositivos externos que se hayan conectado alguna vez y que estén registrados por los sistemas en todos los dispositivos protegidos en la red o para considerar solo los datos sobre los dispositivos actualmente conectados a todos los dispositivos protegidos en la red. La tarea también autoriza todos los dispositivos externos que están conectados en el momento de ejecución de la tarea. Después de la finalización de la tarea de grupo, Kaspersky Embedded Systems Security para Windows genera listas de reglas de autorización para todos los dispositivos externos registrados en la red y guarda estas listas en un archivo XML en una carpeta especificada. Luego, puede importar manualmente las reglas generadas en la configuración de la tarea de control de dispositivos. A diferencia de una tarea en un dispositivo protegido, la directiva no permite configurar la adición automática de las reglas creadas a la lista de reglas de Control de dispositivos cuando se completa la tarea de grupo del Generador de reglas para Control de dispositivos.

Este escenario se recomienda para generar la lista de reglas de autorización antes del primer inicio de la tarea de Control de dispositivos, de modo que las reglas de autorización generadas abarquen todos los dispositivos externos de confianza que se utilicen en un dispositivo protegido.

Uso de datos de sistema sobre todos los dispositivos conectados

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security para Windows recibe datos del sistema sobre todos los dispositivos externos que se hayan conectado alguna vez o estén conectados en ese momento a un dispositivo protegido y muestra los dispositivos detectados en la lista de la ventana **Generar reglas basadas en información del sistema**.

Para cada dispositivo detectado, Kaspersky Embedded Systems Security para Windows analiza los valores de fabricante (VID), el tipo de controlador (PID), el nombre descriptivo, el número de serie y la ruta de acceso a la instancia del dispositivo. Puede generar reglas de autorización para cualquier dispositivo externo cuyos datos se hayan almacenado en el sistema, y agregar directamente reglas creadas recientemente a la lista de las reglas de control de dispositivos.

Según este escenario, Kaspersky Embedded Systems Security para Windows genera reglas de autorización para los dispositivos externos que alguna vez se hayan conectado o que estén conectados en ese momento a un dispositivo protegido con Kaspersky Security Center instalado.

Este escenario se recomienda para renovar una lista de reglas ya especificada cuando es necesario confiar en una cantidad pequeña de dispositivos externos nuevos.

Uso de datos sobre los dispositivos conectados actualmente

En esta situación, Kaspersky Embedded Systems Security para Windows genera reglas de autorización solo para dispositivos externos actualmente conectados. Puede seleccionar uno o varios dispositivos externos para los que desea generar reglas de autorización.

Uso de la tarea Control de dispositivos en el modo Solo estadísticas

El archivo XML recibido después de la finalización de la tarea de Control de dispositivos en el modo **Solo estadísticas** se genera según el registro de tareas.

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security para Windows registra información sobre todas las conexiones de unidades flash y otros dispositivos externos a un dispositivo protegido. Puede generar reglas de autorización según eventos de la tarea y exportarlas a un archivo XML. Antes de iniciar la tarea en el modo **Solo estadísticas**, se recomienda configurar el periodo de ejecución de la tarea, de modo que, durante el periodo especificado, se realicen todas las conexiones de dispositivos externos posibles con un dispositivo protegido.

Este escenario se recomienda para renovar una lista de reglas ya generada si se debe autorizar un gran número de dispositivos externos nuevos.

Si la generación de la lista de reglas según este escenario se realiza en una máquina modelo, puede aplicar una lista de reglas de autorización generadas al configurar la tarea de Control de dispositivos mediante Kaspersky Security Center. De esta manera, podrá autorizar el uso de dispositivos externos conectados a una máquina modelo en todos los dispositivos protegidos.

Acerca de la tarea de Generador de reglas para Control de dispositivos

La tarea de Generador de reglas para Control de dispositivos puede crear automáticamente una lista de reglas de autorización para unidades flash conectadas y otros dispositivos externos según los datos de sistema sobre todos los dispositivos externos que se hayan conectado alguna vez a un dispositivo protegido.

Después de la finalización de la tarea, Kaspersky Embedded Systems Security para Windows crea un archivo XML de configuración que contiene la lista de reglas de autorización para todos los dispositivos externos detectados, o directamente agrega reglas generadas en la tarea de Control de dispositivos según la configuración del Generador de reglas para Control de dispositivos. La aplicación autorizará posteriormente los dispositivos para los cuales se generaron reglas de autorización automáticamente.

Las reglas generadas y agregadas en la tarea se muestran en la ventana **Reglas de Control de dispositivos**.

Configuración predeterminada de la tarea de control de dispositivos

De forma predeterminada, la tarea de Control de dispositivos tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea de control de dispositivos

Configuración	Valor predeterminado	Descripción
Modo de la tarea.	**Solo estadísticas**	La tarea registra información sobre dispositivos externos que se bloquearon o se autorizaron según las reglas especificadas. Los dispositivos externos, en realidad, no se bloquean. Puede seleccionar el modo **Activar** para que la protección del dispositivo bloquee realmente el uso de dispositivos externos.
Permitir el uso de todos los dispositivos externos cuando la tarea Control de dispositivos no se esté ejecutando	No aplicado	Kaspersky Embedded Systems Security para Windows bloquea el uso de dispositivos externos sin tener en cuenta el estado de la tarea de Control de dispositivos. Esto proporciona el nivel de máxima protección contra las amenazas de seguridad informática que surgen al intercambiar archivos con dispositivos externos. Puede ajustar el parámetro de modo que Kaspersky Embedded Systems Security para Windows autorice el uso de todos los dispositivos externos cuando la tarea de Control de dispositivos no está en ejecución.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Control de dispositivos no se inicia automáticamente al inicio de Kaspersky Embedded Systems Security para Windows. Puede configurar la programación de inicio de tareas.

Configuración predeterminada de la tarea de Generador de reglas para Control de dispositivos

Configuración	Valor predeterminado	Descripción

Modo de la tarea.	**Tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado**	El modo de operación de la tarea. Puede seleccionar el modo de tarea **Tener en cuenta solo los dispositivos externos conectados actualmente**.
Acciones después de la finalización de la tarea	Las reglas de autorización se agregan a la lista de reglas de Control de dispositivos, las reglas nuevas se fusionan con las existentes y las reglas duplicadas se eliminan.	Puede agregar reglas a las existentes sin fusionarlas y sin eliminar las reglas duplicadas; reemplazar las reglas existentes con reglas de autorización nuevas; o configurar la exportación de reglas de autorización a un archivo.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Generador de reglas para Control de dispositivos no se inicia automáticamente al inicio de Kaspersky Embedded Systems Security para Windows. Puede iniciar la tarea manualmente o configurar un inicio programado.

Gestión del Control de dispositivos a través del Complemento de administración

En esta sección, aprenda cómo navegar a través de la interfaz del Complemento de administración y gestionar las conexiones de cualquier dispositivo externo a todos los dispositivos protegidos en la red generando listas de reglas a través de Kaspersky Security Center para los grupos de dispositivos protegidos.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la directiva para la tarea de Control de dispositivos

Para abrir la configuración de la tarea de Control de dispositivos a través de la directiva de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configuración** en la subsección **Control de dispositivos**.

   Se abre la ventana **Control de dispositivos**.

7. Configure la directiva según sea necesario.

Cómo abrir la lista de reglas de Control de dispositivos

Para abrir la lista de reglas de Control de dispositivos a través de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configuración** en la subsección **Control de dispositivos**.

   Se abre la ventana **Control de dispositivos**.
7. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de Control de dispositivos**.
8. Configure la directiva según sea necesario.

Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de dispositivos

Para iniciar la creación de una tarea de Generador de reglas para Control de dispositivos:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Abra la pestaña **Tareas**.
4. Haga clic en el botón **Nueva tarea**.

   Se abre la ventana **Nuevo asistente de tarea**.
5. Seleccione la tarea **Generador de reglas para Control de dispositivos**.
6. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración**.

Para configurar la tarea Generador de reglas para Control de dispositivos:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Abra la pestaña **Tareas**.
4. Haga doble clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **Propiedades: Generador de reglas para Control de dispositivos**.

Consulte la sección Configuración de la tarea Generador de reglas para Control de dispositivos para obtener más información sobre la configuración de la tarea.

Configuración de la tarea de Control de dispositivos

Para ajustar la configuración de la tarea Control de dispositivos:

1. Abra la ventana **Control de dispositivos**.
2. En la pestaña **General**, configure la siguiente configuración de tarea:
   - En la sección **Modo de la tarea**, seleccione uno de los modos de la tarea:
     - Activo.

       Si un dispositivo externo que se considera dudoso se conecta a un dispositivo protegido antes de que la tarea Control de dispositivos se inicie en modo Activo, la aplicación no bloqueará el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el dispositivo protegido. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.

     - **Solo estadísticas**.
   - Seleccione o desactive la casilla de verificación **Permitir el uso de todos los dispositivos externos cuando la tarea Control de dispositivos no se esté ejecutando**.
3. Haga clic el botón **Lista de reglas** para modificar la lista de reglas del Control de dispositivos.
4. De ser necesario, configure la programación de inicio de la tarea en la pestaña **Administración de tareas**.
5. Haga clic en el botón **Aceptar** de la ventana **Control de dispositivos**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración de la tarea Generador de reglas para Control de dispositivos

Para configurar la tarea Generador de reglas para Control de dispositivos:

1. Abra la ventana **Propiedades: Generador de reglas para Control de dispositivos**.

2. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

3. En la sección **Configuración**, puede establecer la siguiente configuración:

   - Seleccione el modo de operación: tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado o tener en cuenta solo los dispositivos externos conectados actualmente.
   - Ajuste la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security para Windows crea después de la finalización de la tarea.

4. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).

5. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.

6. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

7. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

   Se guardan las opciones de la tarea de grupo recientemente configuradas.

Configuración de reglas de Control de dispositivos mediante Kaspersky Security Center

Aprenda cómo generar una lista de reglas según distintos criterios o crear manualmente las reglas de autorización o denegación utilizando la tarea de Control de dispositivos.

Creación de reglas de autorización a partir de datos de sistema en una directiva de Kaspersky Security Center

*Para especificar reglas de autorización utilizando la opción **Generar reglas basadas en datos del sistema** en la tarea de Control de dispositivos:*

1. Si es necesario, conecte un dispositivo externo nuevo que desee que sea de confianza para un dispositivo protegido con la Consola de administración de Kaspersky Security Center instalada.

2. Abra la ventana **Reglas de Control de dispositivos**.

3. Haga clic en el botón **Agregar** y, en el menú contextual que se abre, seleccione la opción **Generar reglas basadas en datos del sistema**.

4. Seleccione un dispositivo de la lista de dispositivos que figura en la ventana **Generar reglas basadas en información del sistema**.

5. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.

6. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.

La lista de reglas en la tarea de Control de dispositivos se completará con reglas nuevas generadas según los datos de sistema del dispositivo protegido con la Consola de administración de Kaspersky Security Center instalada.

Generación de reglas para dispositivos conectados

*Para especificar reglas de autorización con la opción **Generar reglas basadas en los dispositivos conectados** en la tarea de Control de dispositivos:*

1. Abra la ventana Reglas de Control de dispositivos.

2. Haga clic en el botón **Agregar** y, en el menú contextual, seleccione **Generar reglas basadas en los dispositivos conectados**.

   Se abre la ventana **Generar reglas basadas en información del sistema**.

3. En la lista de dispositivos detectados conectados al dispositivo protegido, seleccione los dispositivos para los cuales desea generar reglas de autorización.

4. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.

5. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.

La lista de reglas en la tarea de Control de dispositivos se completará con reglas nuevas generadas según los datos de sistema del dispositivo protegido con la Consola de administración de Kaspersky Security Center instalada.

Generación de reglas basadas en el registro de Kaspersky Security Center

*Para especificar reglas de autorización utilizando la opción **Generar reglas basadas en los dispositivos conectados** en la tarea Control de dispositivos:*

1. Abra la ventana Reglas de Control de dispositivos.

2. Haga clic en el botón **Agregar** y, en el menú contextual, seleccione **Generar reglas basadas en los dispositivos conectados**.

   Se abre la ventana **Generar reglas basadas en información del sistema**.

3. Haga clic en **Actualizar la lista** para obtener la lista de dispositivos disponibles y seleccione los dispositivos para los que desee generar reglas de autorización. Además, puede especificar el **nombre descriptivo** en el campo de **búsqueda** para filtrar los dispositivos y acelerar la selección.

4. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.

5. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.

La lista de reglas en la tarea Control de dispositivos se completará con nuevas reglas generadas en función del registro de Kaspersky Security Center.

Visualización de las propiedades de las reglas de Control de dispositivos

Para ver las propiedades de las reglas de **Control de dispositivos**, realice lo siguiente:

1. Abra la ventana **Control de dispositivos**.
2. En la pestaña **General**, haga clic en el botón **Lista de reglas** y doble clic en la regla seleccionada.

   Aparece la ventana **Propiedades de la regla**.

Propiedades de las reglas de Control de dispositivos

Propiedad	Descripción
Aplicar regla	Utilice esta opción para habilitar o deshabilitar la aplicación de reglas.
Fabricante (VID)	Puede especificar el VID completo del fabricante del dispositivo o usar el carácter * como máscara. El carácter * se utiliza para identificar a cualquier fabricante. Si la casilla Usar máscara está seleccionada para el campo Fabricante (VID), los datos de los campos con la casilla de verificación seleccionada se sustituyen con el carácter * y no se tienen en cuenta cuando la regla se aplica.
Tipo de controlador del dispositivo (PID)	Puede especificar el PID completo del controlador o usar el carácter * como máscara. El carácter * se utiliza para indicar cualquier tipo de controlador. Si la casilla Usar máscara está seleccionada para el campo Tipo de controlador del dispositivo (PID), los datos de los campos con la casilla de verificación seleccionada se sustituyen con el carácter * y no se tienen en cuenta cuando la regla se aplica.
Número de serie	Puede especificar el número de serie completo del dispositivo o usar los caracteres * y ? como máscaras. El carácter * representa cualquier secuencia de caracteres, incluida una secuencia vacía. El carácter ? representa carácter individual en la secuencia. Si la casilla Usar máscara está seleccionada en el campo Número de serie, los datos del campo con la casilla de verificación seleccionada se sustituyen con el signo * y no se tienen en cuenta cuando la regla se aplica. Si seleccionó la opción **Usar máscara**, pero no ingresó ningún carácter en el campo **Número de serie**, guardó la configuración y cerró la ventana, la aplicación utiliza * como máscara para la propiedad **Número de serie** y no considera el campo cuando se aplica la regla.
Ruta de acceso a la instancia del dispositivo	Identificador del dispositivo conectado. No puede modificar la propiedad. El campo solo tiene fines informativos. La aplicación no utiliza el campo para el control de dispositivos.
Nombre descriptivo	Nombre del dispositivo que estableció el fabricante. No puede modificar la propiedad. El campo solo tiene fines informativos. La aplicación no utiliza el campo para el control de dispositivos.
Usuario o grupo de usuarios	Hay distintas opciones para indicar qué cuenta de usuario o qué grupo de usuarios tendrán acceso a los dispositivos USB seleccionados: • usar Active Directory Domain Services • usar la lista de usuarios y grupos de usuarios del Servidor de administración • agregar los usuarios y grupos de usuarios manualmente

	El sistema operativo muestra todos los dispositivos USB conectados. Solo puede acceder a las unidades USB para las que tiene los derechos de acceso respectivos.
Descripción	Descripción del dispositivo predeterminada. Si es necesario, especifique información adicional sobre la regla en el campo Descripción. Por ejemplo, especifique los dispositivos afectados por la regla.

Importación de reglas desde el informe de Kaspersky Security Center sobre dispositivos bloqueados

Tras ejecutar la tarea Control de dispositivos en modo **Solo estadísticas**, puede importar los datos del informe de Kaspersky Security Center sobre las conexiones de dispositivos que se hayan bloqueado y generar, con esos datos, una lista de reglas de autorización de Control de dispositivos en la directiva que esté configurando.

Al generar el informe sobre eventos que ocurren durante la tarea de Control de dispositivos, puede hacer un seguimiento de los dispositivos cuya conexión se restringe.

Para especificar reglas de autorización para la conexión de dispositivos para un grupo de dispositivos protegidos según el informe de Kaspersky Security Center sobre dispositivos bloqueados:

1. En las propiedades de la directiva, en la sección **Notificación de eventos**, asegúrese de que:

   - para el nivel de importancia **Eventos críticos**, el periodo por el que se mantendrá almacenado el evento Dispositivo externo no confiable detectado y bloqueado en el registro de tareas sea superior al periodo por el que se planea utilizar el modo **Solo estadísticas** (el valor predeterminado es de 30 días);

   - para el nivel de importancia **Advertencia**, el periodo por el que se mantendrá almacenado el evento Solo estadísticas: dispositivo externo no confiable detectado en el registro de tareas sea superior al periodo por el que se planea utilizar el modo **Solo estadísticas** (el valor predeterminado es de 30 días).

   Cuando el periodo para almacenar eventos se agota, la información sobre los eventos registrados se elimina y no se refleja en el archivo del informe. Antes de ejecutar la tarea de Control de dispositivos en modo **Solo estadísticas**, asegúrese de que el tiempo de ejecución de la tarea no supere el tiempo de almacenamiento configurado para los eventos especificados.

2. Inicie la tarea de Control de dispositivos en modo **Solo estadísticas**.

   a. En el espacio de trabajo del nodo **Servidor de administración** en Kaspersky Security Center, seleccione la pestaña **Eventos**.

   b. Haga clic en el botón **Crear selección** y cree una selección de eventos basada en el criterio Dispositivo externo no confiable detectado y bloqueado. Vea las conexiones de los dispositivos bloqueados por la tarea Control de dispositivos.

   c. En el panel de resultados de la selección, haga clic en el vínculo **Exportar eventos a archivo** para guardar el informe sobre conexiones restringidas en un archivo TXT.

Antes de importar y aplicar el informe generado en una directiva, asegúrese de que el informe solo contenga datos de los dispositivos cuya conexión desea autorizar.

3. Importe datos sobre conexiones de dispositivos restringidos a la tarea de Control de dispositivos:

a. Abra la ventana **Reglas de Control de dispositivos**.

b. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Importar datos sobre dispositivos bloqueados del informe de Kaspersky Security Center**.

c. Seleccione el principio para agregar reglas desde la lista creada sobre la base del informe de Kaspersky Security Center a la lista de reglas de Control de dispositivos configuradas anteriormente:

- **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.
- **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
  - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

a. En la ventana estándar de Microsoft Windows que se abre, seleccione el archivo TXT al cual se exportaron los eventos del informe sobre dispositivos restringidos.

b. Haga clic en el botón **Guardar** de la ventana **Reglas de Control de dispositivos**.

4. Haga clic en el botón **Aceptar** de la ventana **Control de dispositivos**.

Las reglas creadas sobre la base del informe de Kaspersky Security Center sobre los dispositivos restringidos se agregan a la lista de reglas de Control de dispositivos.

Creación de reglas con la tarea Generador de reglas para Control de dispositivos

Para especificar reglas de control de dispositivos para un grupo de dispositivos protegidos mediante la tarea de Generador de reglas para Control de dispositivos:

1. Abra la ventana **Configuración** en el Asistente de nueva tarea.

2. Configure las siguientes opciones:

- En el bloque **Modo**:
  - **Tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado**
  - **Tener en cuenta solo los dispositivos externos conectados actualmente**
- En el bloque **Después de completada la tarea**:
  - Agregar reglas de autorización a la lista de reglas de Control de dispositivos.
  - **Principio de adición**.
  - **Exportar reglas de autorización a archivo**.
  - **Agregar detalles del dispositivo protegido al nombre del archivo**.

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

4. En la sección **Programación**, configure el inicio programado de la tarea.
5. Haga clic en el botón **Siguiente**.
6. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desea utilizar.
7. Haga clic en el botón **Siguiente**.
8. Especifique el nombre de la tarea.
9. Haga clic en el botón **Siguiente**.

   El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos: " * < > & \ : |

   Se abre la ventana **Finalizar la creación de la tarea**.
10. Puede ejecutar la tarea opcionalmente después de que el Asistente finalice, seleccionando la casilla **Ejecutar tarea después de que finalice el asistente**.
11. Haga clic en **Finalizar** para terminar de crear la tarea.
12. En la pestaña **Tareas** en el espacio de trabajo del grupo de dispositivos protegidos configurados, en la lista de tareas de grupo, seleccione el Generador de reglas para Control de dispositivos que creó.
13. Haga clic en el botón **Inicio** para iniciar la tarea.

    Cuando la tarea se completa, las listas de reglas de autorización generadas automáticamente se guardan en una carpeta compartida en archivos XML.

    Antes de usar la directiva de Control de dispositivos en la red, asegúrese de que todos los dispositivos protegidos puedan acceder a una carpeta de red compartida. Si la política de la organización no contempla el uso de una carpeta compartida en la red, recomendamos iniciar la tarea Generador de reglas para Control de dispositivos para las reglas de control del dispositivo protegido en el grupo de dispositivos protegidos de prueba o en una máquina modelo.

Agregar reglas generadas a la lista de reglas de Control de dispositivos

Para agregar las listas de reglas de autorización generadas a la tarea de Control de dispositivos:

1. Abra la ventana **Reglas de Control de dispositivos**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón **Agregar**, seleccione la opción **Importar reglas desde archivo XML**.
4. Seleccione el principio para agregar las reglas de autorización generadas automáticamente a la lista de reglas de Control de dispositivos creadas anteriormente:

   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.

- **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.

5. **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas. En la ventana estándar de Microsoft Windows que se abre, seleccione archivos XML creados después de la finalización de la tarea de grupo de Generador de reglas para Control de dispositivos.

6. Haga clic en el botón **Abrir**.

   Todas las reglas generadas desde el archivo XML se agregan a la lista según el principio seleccionado.

7. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.

8. Si desea aplicar las reglas de Control de dispositivos generadas, seleccione el modo de la tarea **Control de dispositivos** en los ajustes de **Activo** dentro de la directiva.

Las reglas de autorización generadas automáticamente según datos del sistema en cada dispositivo protegido independiente se aplican a todos los dispositivos protegidos de red abarcados por la directiva configurada. En estos dispositivos protegidos, la aplicación permitirá la conexión de solo los dispositivos para los cuales se crearon reglas de autorización.

Gestión del Control de dispositivos a través de la Consola de la aplicación

En esta sección, aprenderá a navegar por la interfaz de la Consola de la aplicación y a definir la configuración de la tarea en un dispositivo protegido.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la tarea de Control de dispositivos

Para abrir la configuración de la tarea de Control de dispositivos a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.

2. Seleccione el nodo secundario **Control de dispositivos**.

3. En el panel de detalles del nodo secundario **Control de dispositivos**, haga clic en el vínculo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

4. Configure la tarea como sea necesario.

Cómo abrir la ventana Reglas de control de dispositivos

Para abrir la lista de reglas de Control de dispositivos a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de dispositivos**.
3. En el panel de resultados del nodo **Control de dispositivos**, haga clic en el vínculo **Reglas de Control de dispositivos**.

   Se abre la ventana **Reglas de Control de dispositivos**.
4. Configure la lista de reglas como sea necesario.

Cómo abrir la configuración de la tarea de Generador de reglas para Control de dispositivos

Para configurar la tarea Generador de reglas para Control de dispositivos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Generadores automatizados de reglas**.
2. Seleccione el nodo secundario **Generador de reglas para Control de dispositivos**.
3. En el panel de resultados del nodo secundario **Generador de reglas para Control de dispositivos**, haga clic en el vínculo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
4. Configure la tarea como sea necesario.

Configuración de la tarea Control de dispositivos

Para ajustar la configuración de la tarea Control de dispositivos:

1. Abra la ventana **Configuración de tareas**.
2. En la pestaña **General**, configure la siguiente configuración de tarea:
   - En la sección **Modo de la tarea**, seleccione uno de los modos de la tarea:
     - Activar.

       Si un dispositivo externo que se considera dudoso se conecta a un dispositivo protegido antes de que la tarea Control de dispositivos se inicie en modo Activo, la aplicación no bloqueará el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el dispositivo protegido. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.
     - **Solo estadísticas**.
   - Seleccione o desactive la casilla de verificación **Permitir el uso de todos los dispositivos externos cuando la tarea Control de dispositivos no se esté ejecutando**.

3. Si es necesario, en las pestañas **Programación** y **Avanzado**, configure las opciones de inicio de tareas programadas.

4. Para modificar la lista de reglas de control de dispositivos, haga clic en el vínculo **Reglas de Control de dispositivos** en la parte inferior del panel de resultados del nodo **Control de dispositivos**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración de las reglas de Control de dispositivos

Aprenda cómo generar, importar y exportar una lista de reglas o crear manualmente las reglas de autorización o denegación utilizando la tarea del Control de dispositivos.

Importación de Reglas de Control de dispositivos desde un archivo XML

Para importar las reglas de Control de dispositivos:

1. Abra la ventana **Reglas de Control de dispositivos**.

2. Haga clic en el botón **Agregar**.

3. En el menú contextual del botón, seleccione **Importar reglas desde archivo XML**.

4. Especifique el método para agregar reglas importadas. Para hacerlo, seleccione una de las opciones del menú contextual del botón **Importar reglas desde archivo XML**:

   - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.

   - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

   Se abre la ventana estándar **Abrir** de Microsoft Windows.

5. En la ventana **Abrir**, seleccione el archivo XML que contiene la configuración de las Reglas de Control de dispositivos.

6. Haga clic en el botón **Abrir**.

Las reglas importadas se mostrarán en la lista de la ventana **Reglas de Control de dispositivos**.

Llenado de la lista de reglas según los eventos de la tarea Control de dispositivos

Para crear un archivo de configuración que contenga listas de reglas de Control de dispositivos según los eventos de la tarea Control de dispositivos:

1. Inicie la tarea Control de dispositivos en modo **Solo estadísticas** para registrar todas las conexiones de unidades flash y otros dispositivos externos a un dispositivo protegido.

2. Después de la finalización de la tarea en el modo **Solo estadísticas**, abra el registro de tareas con un clic en el botón **Abrir el registro de tareas** en la sección **Administración** del panel de resultados del nodo **Control de dispositivos**.

3. En la ventana **Registros**, haga clic en **Generar reglas basadas en los eventos**.

   Kaspersky Embedded Systems Security para Windows creará un archivo XML de configuración que contendrá una lista de reglas generada según los eventos de la tarea de Control de dispositivos en el modo **Solo estadísticas**. Puede aplicar esta lista en la tarea Control de dispositivos.

Antes de aplicar una lista de reglas generada según los eventos de la tarea, se recomienda revisar y, luego, procesar manualmente la lista de reglas para asegurarse de que no haya dispositivos dudosos autorizados por las reglas especificadas.

Durante la conversión de un archivo XML con los eventos de la tarea a una lista de reglas de control de dispositivos, la aplicación genera reglas de autorización para todos los eventos registrados, incluidas las restricciones de dispositivos.

Todos los eventos de la tarea se registran en el registro de tareas sin tener en cuenta el modo de la tarea. Puede crear un archivo de configuración con una lista de reglas que se base en los eventos de la tarea en el modo **Activar**. Este método no se recomienda, excepto en casos urgentes en los que la eficacia de la tarea requiera la generación de una versión final de la lista de reglas antes de que la tarea se ejecute en el modo activo.

Cómo agregar una regla de autorización para uno o varios dispositivos externos

La tarea de Control de dispositivos no admite la función de adición manual de reglas de a una. Sin embargo, en casos donde debe agregar reglas para uno o varios dispositivos externos nuevos, puede usar la opción **Generar reglas basadas en datos del sistema**. Si se aplica este escenario, la aplicación usa los datos de Windows sobre todos los dispositivos externos que se hayan conectado alguna vez y también autoriza a los dispositivos conectados en ese momento para el relleno de una lista de reglas de autorización.

Para agregar una regla de autorización para uno o varios dispositivos externos que están conectados actualmente:

1. Abra la ventana **Reglas de Control de dispositivos**.

2. Haga clic en el botón **Agregar**.

3. En el menú contextual que se abre, seleccione la opción **Generar reglas basadas en datos del sistema**.

4. En la ventana que se abre, revise la lista de dispositivos detectados y seleccione un solo dispositivo o varios en los que desee confiar en un dispositivo protegido.

5. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.

   Se generarán y se agregarán reglas nuevas a la lista de reglas de Control de dispositivos.

Eliminación de Reglas de Control de dispositivos

Para eliminar las Reglas de Control de dispositivos:

1. Abra la ventana **Reglas de Control de dispositivos**.
2. En la lista, seleccione una o varias reglas que desee eliminar.
3. Haga clic en el botón **Eliminar seleccionadas**.
4. Haga clic en el botón **Guardar**.

Las reglas de Control de dispositivos seleccionadas se eliminarán.

Exportación de Reglas de Control de dispositivos

Para exportar Reglas del Control de dispositivos a un archivo de configuración:

1. Abra la ventana **Reglas de Control de dispositivos**.
2. Haga clic el botón **Exportar a archivo**.

   Se abre la ventana de Microsoft Windows estándar.
3. En la ventana que se abre, especifique el archivo al cual desea exportar las reglas. Si no existe tal archivo, este se creará. Si ya existe un archivo con el nombre especificado, su contenido se volverá a escribir después de que las reglas se exporten.
4. Haga clic en el botón **Guardar**.

La regla y su configuración se exportarán al archivo especificado.

Habilitación y deshabilitación de Reglas de Control de dispositivos

Puede habilitar y deshabilitar las reglas de autorización de Control de dispositivos creadas sin eliminarlas.

Para activar o desactivar una regla de control de dispositivos creada:

1. Abra la ventana **Reglas de Control de dispositivos**.
2. En la lista de reglas especificadas, abra la ventana **Propiedades de la regla** con un clic doble en la regla cuyas propiedades desea configurar.
3. En la ventana que se abre, seleccione o desactive la casilla de verificación **Aplicar regla**.
4. Haga clic en el botón **Aceptar**.

El estado de aplicación de regla se guardará y se mostrará para la regla especificada.

Ampliación del área de aplicación de las Reglas de Control de dispositivos

Cada regla de Control de dispositivos generada automáticamente abarca un solo dispositivo externo. Si desea ampliar el área de aplicación de una regla de control de dispositivos, puede hacerlo definiendo la máscara de la ruta de acceso a la instancia del dispositivo en las propiedades de la regla.

Utilizar una máscara de ruta de instancia de dispositivo permite reducir el número total de reglas de autorización de Control de dispositivos y simplifica el procesamiento de las reglas. Sin embargo, la ampliación de un área de aplicación de la regla puede provocar la disminución de la eficacia del control de dispositivos externos.

Para aplicar una máscara a la ruta de acceso a la instancia del dispositivo en las propiedades de la regla de control de dispositivos:

1. Abra la ventana **Reglas de Control de dispositivos**.
2. En la ventana que se abre, seleccione una regla para usar sus propiedades en la aplicación de la máscara.
3. Abra la ventana **Propiedades de la regla** con un doble clic en una regla de control de dispositivos seleccionada.
4. En la ventana que se abre, realice las siguientes operaciones:
   - Seleccione la casilla de verificación **Usar máscara** al lado del campo **Fabricante (VID)** si desea que la regla seleccionada autorice conexiones para todos los dispositivos externos que coincidan con la información especificada sobre el fabricante del dispositivo.
   - Seleccione la casilla de verificación **Usar máscara** al lado del campo **Tipo de controlador (PID)** si desea que la regla seleccionada autorice conexiones para todos los dispositivos externos que coincidan con la información especificada sobre el tipo de controlador.
   - Seleccione la casilla de verificación **Usar máscara** al lado del campo **Número de serie** si desea que la regla seleccionada autorice conexiones para todos los dispositivos externos que coincidan con la información especificada sobre el número de serie del dispositivo.

   Si la casilla **Usar máscara** está seleccionada en al menos uno de los campos, los datos de los campos con la casilla de verificación seleccionada se sustituyen con el carácter * y no se tienen en cuenta cuando la regla se aplica.
5. Especifique una cuenta de usuario o un grupo de usuarios que tengan acceso a los dispositivos USB seleccionados. El sistema operativo muestra todos los dispositivos USB conectados. Solo puede acceder a los dispositivos USB para los que tiene los derechos de acceso respectivos.
6. Si es necesario, ingrese información adicional sobre la regla en el campo **Usuario o grupo de usuarios**. Por ejemplo, especifique los dispositivos afectados por la regla.
7. Haga clic en el botón **Aceptar**.

Se guardarán las propiedades de la regla configuradas recientemente. El área de aplicación de la regla se ampliará según la máscara de la ruta de acceso a la instancia del dispositivo especificada.

Configuración de la tarea Generador de reglas para Control de dispositivos

Para configurar la tarea Generador de reglas para Control de dispositivos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Generadores automatizados de reglas**.
2. Seleccione el nodo secundario **Generador de reglas para Control de dispositivos**.
3. En el panel de resultados del nodo secundario **Propiedades**, haga clic en el vínculo **Generador de reglas para Control de dispositivos**.

   Aparece la ventana **Configuración de tareas**.
4. En la pestaña **General**, dentro del bloque **Modo de la tarea**, seleccione el modo de la tarea:
   - **Tener en cuenta los datos del sistema sobre todos los dispositivos externos que se hayan conectado**
   - **Tener en cuenta solo los dispositivos externos conectados actualmente**
5. En la sección **Después de completada la tarea**, especifique las acciones que Kaspersky Embedded Systems Security para Windows debe realizar después de la finalización de la tarea:
   - Agregar reglas de autorización a la lista de reglas de Control de dispositivos.
   - Principio de adición.
   - Exportar reglas de autorización a archivo.
   - Agregar detalles del dispositivo protegido al nombre del archivo.
6. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas.
7. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

Kaspersky Embedded Systems Security para Windows aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Administración del Control de dispositivos a través del Complemento web de la Consola de la aplicación

En esta sección, aprenderá a navegar la interfaz del Complemento web y establecer la configuración de las tareas en un dispositivo protegido.

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Control de actividad local**.
5. Haga clic en el botón **Configuración** en la subsección **Control de dispositivos**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración	Descripción
Activo	Kaspersky Embedded Systems Security para Windows aplica reglas para controlar la conexión de unidades extraíbles y otros dispositivos externos, y autoriza o bloquea el uso de todos los dispositivos según el principio de denegación predeterminada y las reglas de autorización especificadas. Se autoriza el uso de dispositivos externos de confianza. El uso de dispositivos externos dudosos sea bloquea de forma predeterminada.
Solo estadísticas	Kaspersky Embedded Systems Security para Windows no controla la conexión de unidades extraíbles ni otros dispositivos externos, sino que solo registra la información sobre la conexión y el registro de dispositivos externos en un dispositivo protegido y sobre las reglas de autorización de Control de dispositivos que activan los dispositivos conectados. Se autoriza el uso de todos los dispositivos externos. Este modo está configurado de forma predeterminada.
Permitir el uso de todos los dispositivos externos cuando la tarea Control de dispositivos no se esté ejecutando	La casilla de verificación permite autorizar o bloquear el uso de dispositivos externos cuando la tarea Control de dispositivos no se está ejecutando. Si la casilla está seleccionada y la tarea Control de dispositivos no se está ejecutando, Kaspersky Embedded Systems Security para Windows permite usar cualquier dispositivo externo en un dispositivo protegido. Si la casilla de verificación está desactivada, la aplicación bloquea el uso de dispositivos externos no confiables en un dispositivo protegido en los siguientes casos: la tarea Control de dispositivos no se está ejecutando o el servicio de Kaspersky Security está desactivado. Esta opción se recomienda para maximizar el nivel de protección contra las amenazas de seguridad informática que surgen al intercambiar archivos con dispositivos externos. De forma predeterminada, la casilla no está activada.
Reglas de Control de dispositivos	Puede editar la lista de reglas de Control de dispositivos.
Administración de tareas	Puede configurar las opciones para iniciar la tarea en base a una programación.

Administración de firewall

Esta sección contiene información acerca de la tarea Administración de firewall y cómo configurarla.

Acerca de la tarea Administración de firewall

Si el firewall de Windows está desactivado durante la instalación de Kaspersky Embedded Systems Security para Windows, la tarea de administración del firewall no se ejecutará después de que finalice la instalación. Si el Firewall de Windows está activado durante la instalación, la tarea Administración de firewall se ejecutará cuando finalice la instalación.

Si el firewall de Windows está controlado por una directiva de grupo de Kaspersky Security Center, la tarea de Administración de firewall no se puede iniciar.

La tarea Administración de firewall no filtra el tráfico de red de forma independiente, pero permite administrar el Firewall de Windows a través de la interfaz gráfica de Kaspersky Embedded Systems Security para Windows.

La tarea entra en contacto con el Firewall de Windows a intervalos regulares. De forma predeterminada, se establece contacto cada un minuto y el intervalo no se puede cambiar.

Mientras la tarea Administración de firewall está en ejecución, Kaspersky Embedded Systems Security para Windows realiza las acciones definidas por el modo de interacción con el firewall de Windows:

- **Observar el estado de Windows Firewall**. La aplicación solo observa el estado del firewall de Windows y envía un evento de advertencia a Kaspersky Security Center si el firewall de Windows no se ha iniciado.
- **Controlar la operación de Windows Firewall**. La aplicación controla el funcionamiento de Firewall de Windows en la medida determinada por las siguientes funciones:
  - Mantener el estado de Firewall de Windows

    Esta función habilita o deshabilita el mantenimiento de Firewall de Windows en el estado **Habilitado/Deshabilitado** a través de la lista desplegable.

    Cuando se habilita esta función, la aplicación realiza las siguientes acciones:

    - Entra en contacto con el Firewall de Windows a intervalos de un minuto.
    - Lee el estado del Firewall de Windows.
    - Cuando el estado está definido en **Habilitado**, habilita el Firewall de Windows si está deshabilitado.
    - Cuando el estado está definido en **Deshabilitado**, deshabilita el Firewall de Windows si está habilitado.

    Esta función no se puede deshabilitar si la función **Administrar los ajustes y reglas de Firewall de Windows** está deshabilitada.

    De manera predeterminada, la función está habilitada y la opción **Habilitado** está seleccionada.

- Administrar los ajustes y reglas de Firewall de Windows.

  Esta función habilita o deshabilita la administración de los ajustes y las reglas de Firewall de Windows.

  Cuando se habilita esta función, la aplicación realiza las siguientes acciones:

  - Entra en contacto con el Firewall de Windows a intervalos de un minuto.
  - Lee y copia los ajustes y las reglas de Firewall de Windows.
  - Asigna a los ajustes de Firewall de Windows los valores definidos en la tarea Administración de firewall.
  - Crea una lista de reglas de firewall en el grupo "Kaspersky Security Group" dentro del complemento del Firewall de Windows. Este conjunto contiene todas las reglas de firewall de la tarea Administración de firewall.

    Posteriormente, cuando entra en contacto con Firewall de Windows, la aplicación no sincroniza la lista de reglas de firewall del grupo "Kaspersky Security Group" con la lista de reglas de la tarea Administración de firewall. Para sincronizar las listas de reglas de firewall, reinicie la tarea Administración de firewall.
  - Restringe la capacidad de editar los ajustes y las reglas de Firewall de Windows a través de herramientas de terceros o directamente con el complemento (wf.msc). Si se modifican los ajustes o las reglas de Firewall de Windows, en el lapso de un minuto, la aplicación revierte los valores a aquellos que se hayan definido con la tarea Administración de firewall.

  Si se deshabilita esta función, la aplicación revierte los ajustes y las reglas de Firewall de Windows a los valores guardados por la aplicación en su primer contacto con Firewall de Windows y deja de administrar los ajustes y las reglas de Firewall de Windows.

  Esta función no se puede deshabilitar si la función **Mantener el estado de Firewall de Windows** está deshabilitada.

  De forma predeterminada, esta función está habilitada.

Acerca de las reglas de firewall

Si el modo de interacción con Firewall de Windows se establece en **Controlar la operación de Windows Firewall**, la tarea Administración de Firewall filtra el tráfico de red a través de Firewall de Windows mediante el uso de reglas de firewall.

Las reglas de firewall para aplicaciones controlan las conexiones de red de aplicaciones específicas. El criterio de activación para estas reglas se basa en la ruta de acceso al archivo ejecutable de la aplicación.

Las reglas de firewall para puertos controlan las conexiones de red en las que se utilizan puertos y protocolos (TCP/UDP) puntuales. Los criterios de activación para tales reglas son el puerto o intervalo de puertos y el tipo de protocolo.

Las reglas de puerto involucran un área de aplicación más amplia que la de las reglas de aplicación. Al permitir las conexiones de red a través de reglas de puertos, se reduce el nivel de seguridad del dispositivo protegido.

Puede realizar las siguientes acciones administrativas con las reglas de firewall:

- crear y eliminar reglas de firewall
- cambiar la configuración de las reglas de firewall
- habilitar y deshabilitar reglas específicas

Reglas de firewall creadas por defecto

Durante la instalación, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas de autorización para evitar que se bloqueen las aplicaciones instaladas junto con Kaspersky Embedded Systems Security para Windows. Encontrará los detalles y las limitaciones más abajo.

Cuando se instala en un dispositivo con cualquiera de las versiones de Windows compatibles, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para conexiones de red entrantes:

- Reglas de autorización para la Consola de Kaspersky Embedded Systems Security para Windows (kavfsgt.exe), ubicada en la carpeta de instalación de la aplicación. Estado: habilitado. Alcance de la regla: todas las direcciones. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el puerto local 15000 si el Agente de red de Kaspersky Security Center está instalado en el dispositivo. Estado: habilitado. Alcance de la regla: todas las direcciones. Protocolos: TCP y UDP, una regla por protocolo.

Cuando se instala en un dispositivo con Windows 7 o una versión posterior, Kaspersky Embedded Systems Security para Windows crea un conjunto de reglas para conexiones de red salientes:

- Reglas de autorización para la Consola de Kaspersky Embedded Systems Security para Windows (kavfsgt.exe), ubicada en la carpeta de instalación de la aplicación. Estado: habilitado. Alcance de la regla: todas las direcciones. Protocolos: TCP y UDP, una regla por protocolo.
- Reglas de autorización para Kaspersky Embedded Systems Security para Windows (kavfswp.exe), cuyo archivo se encuentra en la carpeta de instalación de la aplicación. Estado: habilitado. Alcance de la regla: todas las direcciones. Protocolos: TCP y UDP, una regla por protocolo.
- Dos reglas de autorización para el puerto local 13000 si el Agente de red de Kaspersky Security Center está instalado en el dispositivo. Estado: habilitado. Alcance de la regla: todas las direcciones. Protocolos: TCP y UDP, una regla por protocolo.

Si desinstala Kaspersky Embedded Systems Security para Windows, la aplicación eliminará todas las reglas de firewall creadas, excepto las reglas creadas por el Agente de red de Kaspersky Security Center, como "Kaspersky Security Center WDS" y "Kaspersky Administration Kit". La aplicación también eliminará las reglas creadas para ICMPv4 e ICMPv6 para Windows 7 y versiones posteriores.

Cuando se desinstala Kaspersky Embedded Systems Security para Windows, la aplicación permite todas las conexiones ICMP para sistemas operativos anteriores a Windows 7.

Configuración predeterminada de la tarea de Administración de Firewall

La tarea de Administración de Firewall utiliza la configuración predeterminada que se describe en la tabla a continuación. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea de Administración de Firewall

Configuración	Valor predeterminado	Descripción

Modo de interacción entre Kaspersky Embedded Systems Security para Windows y Firewall de Windows	**Observar el estado de Windows Firewall**	La aplicación solo observa el estado de Firewall de Windows y envía una notificación a Kaspersky Security Center si detecta que Firewall de Windows está deshabilitado.
Conexiones entrantes	**Bloquear**	Puede crear y configurar reglas de firewall de entrada para bloquear o permitir las conexiones entrantes.
Conexiones salientes	**Autorizar**	Puede crear y configurar reglas de firewall de salida para bloquear o permitir conexiones salientes.
Permitir conexiones ICMP	**Deshabilitado**	Este ajuste permite las conexiones entrantes y salientes a través los protocolos ICMPv4 e ICMPv6 independientemente de los ajustes definidos en la tarea para las conexiones entrantes y salientes.
Programación de inicio de tareas	N/D	La tarea de Administración de Firewall no se inicia automáticamente al inicio de Kaspersky Embedded Systems Security para Windows. Puede configurar la programación de inicio de tareas.

Configuración de la tarea Administración de firewall mediante el Complemento de administración

En esta sección, se brindan instrucciones para configurar los ajustes generales de la tarea Administración de firewall y para crear y configurar reglas de firewall a través del Complemento de administración.

Configuración de los ajustes generales de la tarea Administración de firewall

Para configurar los ajustes generales de la tarea Administración de firewall mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Control de actividad de red**, dentro de la sección **Administración de firewall**, haga clic en el botón **Configuración**.

   Se abre la ventana **Administración de firewall**.
5. En la pestaña **General**, en el bloque **Integración con Firewall de Windows**, seleccione el modo de interacción entre Kaspersky Embedded Systems Security para Windows y el firewall de Windows:

- **Observar el estado de Windows Firewall**. Si selecciona esta opción, la aplicación solo observará el estado del firewall de Windows y enviará un evento de advertencia a Kaspersky Security Center si el firewall de Windows no se ha iniciado.

  Si selecciona esta opción para reemplazar la opción **Controlar la operación de Windows Firewall**, la aplicación restaurará la configuración interna del Firewall de Windows la siguiente vez que se inicie el sistema operativo del dispositivo protegido.

- **Controlar la operación de Windows Firewall**. Si selecciona esta opción, la aplicación monitoreará el Firewall de Windows en la medida en que lo determinan las siguientes opciones:

  - Mantener el estado de Firewall de Windows.
  - Administrar los ajustes y reglas de Firewall de Windows.
  - Permitir conexiones ICMP.

6. En el bloque **Conexiones entrantes**, configure los ajustes para las conexiones de red entrantes:

   - Use la lista desplegable **Acción para conexiones entrantes** para especificar la acción que Firewall de Windows realizará para todas las conexiones de red entrantes, a menos que haya reglas de Firewall para conexiones entrantes que definan lo contrario.
   - De ser necesario, agregue reglas de Firewall para conexiones entrantes.

     Las reglas que defina para las conexiones entrantes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de autorización para conexiones de red entrantes y selecciona **Bloquear** en la lista desplegable **Acción para conexiones entrantes**, Firewall de Windows permitirá las conexiones de red entrantes que coincidan con los criterios de la regla.

7. En el bloque **Conexiones salientes**, configure los ajustes para las conexiones de red salientes:

   - Use la lista desplegable **Acción para conexiones salientes** para especificar la acción que Firewall de Windows realizará para todas las conexiones de red salientes, a menos que haya reglas de Firewall para conexiones salientes que definan lo contrario.
   - De ser necesario, agregue reglas de Firewall para conexiones salientes.

     Las reglas que defina para las conexiones salientes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de bloqueo para conexiones de red salientes y selecciona **Autorizar** en la lista desplegable **Acción para conexiones salientes**, Firewall de Windows bloqueará las conexiones de red salientes que coincidan con los criterios de la regla.

8. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Creación y configuración de reglas de firewall

Para crear y configurar reglas de firewall mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Control de actividad de red**, dentro de la sección **Administración de firewall**, haga clic en el botón **Configuración**.

   Se abre la ventana **Administración de firewall**.

5. En la pestaña **General**, en la sección **Conexiones entrantes**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de firewall para conexiones entrantes**.

6. Cree y configure sus reglas de firewall para conexiones entrantes.

1. Haga clic en el botón **Agregar** de la pestaña **Aplicaciones**.

   Se abre la ventana **Regla de firewall para la aplicación**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red entrantes.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para la aplicación.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para la aplicación.

   c. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

   d. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo puede usar direcciones de tipo IPv4.

   e. Haga clic en el botón **Aceptar** para guardar la regla.

3. Haga clic en el botón **Agregar** de la pestaña **Puertos**.

   Se abre la ventana **Regla de firewall para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para los puertos.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para los puertos.

   c. En el bloque **Puertos locales**, ingrese un puerto o un intervalo de puertos.

   d. Seleccione el tipo de protocolo (TCP/UDP) para el cual se controlarán las conexiones entrantes.

   e. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

Solo puede usar direcciones de tipo IPv4.

f. Haga clic en el botón **Aceptar** para guardar la regla.

5. En la ventana **Reglas de firewall para conexiones entrantes**, haga clic en el botón **Aceptar**.

7. En la pestaña **General**, en el bloque **Conexiones salientes**, haga clic en el botón **Lista de reglas**.
   Se abre la ventana **Reglas de firewall para conexiones salientes**.

8. Cree y configure sus reglas de firewall para conexiones salientes.

1. Haga clic en el botón **Agregar** de la pestaña **Aplicaciones**.

   Se abre la ventana **Regla de firewall para la aplicación**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

   c. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

   d. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo puede usar direcciones de tipo IPv4.

   e. Haga clic en el botón **Aceptar** para guardar la regla.

3. Haga clic en el botón **Agregar** de la pestaña **Puertos**.

   Se abre la ventana **Regla de firewall para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
   - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

   c. En el bloque **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   d. Seleccione el tipo de protocolo (TCP/UDP) para el cual se controlarán las conexiones salientes.

   e. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la

regla.

Solo puede usar direcciones de tipo IPv4.

f. Haga clic en el botón **Aceptar** para guardar la regla.

5. En la ventana **Reglas de firewall para conexiones salientes**, haga clic en el botón **Aceptar**.

9. Haga clic en el botón **Aceptar** de la ventana **Administración de firewall**.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Habilitación y deshabilitación de Reglas de firewall

Para habilitar o deshabilitar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Control de actividad de red**, haga clic en el botón **Configuración** en la subsección **Administración de firewall**.
5. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Reglas de firewall para conexiones entrantes**.
6. Según el tipo de regla cuyo estado desee modificar, haga clic en los vínculos **Entrante** o **Saliente** y seleccione las pestañas **Aplicaciones** o **Puertos**.
7. En la lista de reglas, seleccione la regla cuyo estado desee modificar y realice una de las acciones siguientes:
   - Si desea habilitar una regla deshabilitada, seleccione la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se habilitará.
   - Si desea deshabilitar una regla habilitada, desactive la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se deshabilitará.
8. Haga clic en el botón **Aceptar** de la ventana **Reglas de firewall para conexiones entrantes**.

9. Haga clic en el botón **Aceptar** de la ventana **Administración de firewall**.

10. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la direciva>**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Eliminación de reglas de firewall

Solo puede eliminar reglas de puerto y de aplicación. No puede eliminar reglas de grupo existentes.

Para eliminar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Control de actividad de red**, haga clic en el botón **Configuración** en la subsección **Administración de firewall**.

5. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Reglas de firewall para conexiones entrantes**.

6. Según el tipo de regla cuyo estado desee modificar, seleccione la pestaña **Aplicaciones** o **Puertos**.

7. En la lista de reglas, seleccione la regla que desee eliminar.

8. Haga clic en el botón **Eliminar**.

   La regla seleccionada se elimina.

9. Haga clic en el botón **Aceptar** de la ventana **Reglas de firewall para conexiones entrantes**.

10. Haga clic en el botón **Aceptar** de la ventana **Administración de firewall**.

11. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la directiva>**.

Se guardará la configuración especificada para la tarea de Administración de firewall. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Configuración de la tarea Administración de firewall mediante la Consola de la aplicación

En esta sección, se brindan instrucciones para configurar los ajustes generales de la tarea Administración de firewall y para crear y configurar reglas de firewall mediante la interfaz de la Consola de la aplicación.

Configuración de los ajustes generales de la tarea Administración de firewall

Algunos de los ajustes de las reglas de firewall para conexiones entrantes y salientes podrían no estar disponibles si la Consola de la aplicación se conecta al host local (es decir, al host en el que se la inicia) y el sistema operativo del host no es compatible con dicho ajuste.

Para configurar los ajustes generales de la tarea Administración del firewall mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Parámetros** en el panel de detalles del nodo **Administración de firewall**.

   Se abre la ventana **Configuración de tareas**.
4. En la pestaña **General**, en el bloque **Filtrado de tráfico de red**, seleccione la opción de interacción entre Kaspersky Embedded Systems Security para Windows y el firewall de Windows:

   - **Observar el estado de Windows Firewall**. Si selecciona esta opción, la aplicación solo observará el estado del firewall de Windows y enviará un evento de advertencia a Kaspersky Security Center si el firewall de Windows no se ha iniciado.

     Si selecciona esta opción para reemplazar la opción **Controlar la operación de Windows Firewall**, la aplicación restaurará la configuración interna del Firewall de Windows la siguiente vez que se inicie el sistema operativo del dispositivo protegido.

   - **Controlar la operación de Windows Firewall**. Si selecciona esta opción, la aplicación monitoreará el Firewall de Windows en la medida en que lo determinan las siguientes opciones:

     - Mantener el estado de Firewall de Windows.
     - Administrar los ajustes y reglas de Firewall de Windows.
     - Permitir conexiones ICMP.
5. En el bloque **El programa controla la operación de Firewall de Windows de acuerdo con los siguientes ajustes**, configure los siguientes ajustes:

   - Use la lista desplegable **Acción para conexiones entrantes** para especificar la acción que Firewall de Windows realizará para todas las conexiones de red entrantes, a menos que haya reglas de Firewall para conexiones entrantes que definan lo contrario.
   - De ser necesario, agregue reglas de Firewall para conexiones entrantes.

     Las reglas que defina para las conexiones entrantes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de autorización para conexiones de red entrantes y selecciona **Bloquear** en la lista desplegable **Acción para conexiones entrantes**, Firewall de Windows permitirá las conexiones de red entrantes que coincidan con los criterios de la regla.
   - Use la lista desplegable **Acción para conexiones salientes** para especificar la acción que Firewall de Windows realizará para todas las conexiones de red salientes, a menos que haya reglas de Firewall para

conexiones salientes que definan lo contrario.

- De ser necesario, agregue reglas de Firewall para conexiones salientes.

  Las reglas que defina para las conexiones salientes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de bloqueo para conexiones de red salientes y selecciona **Autorizar** en la lista desplegable **Acción para conexiones salientes**, Firewall de Windows bloqueará las conexiones de red salientes que coincidan con los criterios de la regla.

6. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Creación y configuración de reglas de firewall

Para crear y configurar reglas de firewall mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Entrantes** en el panel de detalles del nodo **Administración de firewall**.

   Se abre la ventana **Reglas de firewall para conexiones entrantes**.
4. Cree y configure sus reglas de firewall para conexiones entrantes.

1. Haga clic en el botón **Agregar** de la pestaña **Aplicaciones**.

   Se abre la ventana **Regla de firewall para la aplicación**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red entrantes.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para la aplicación.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para la aplicación.

   c. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

   d. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo puede usar direcciones de tipo IPv4.

   e. Haga clic en el botón **Aceptar** para guardar la regla.

3. Haga clic en el botón **Agregar** de la pestaña **Puertos**.

   Se abre la ventana **Regla de firewall para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para los puertos.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para los puertos.

   c. En el bloque **Puertos locales**, ingrese un puerto o un intervalo de puertos.

   d. Seleccione el tipo de protocolo (TCP/UDP) para el cual se controlarán las conexiones entrantes.

   e. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

Solo puede usar direcciones de tipo IPv4.

f. Haga clic en el botón **Aceptar** para guardar la regla.

5. En la ventana **Reglas de firewall para conexiones entrantes**, haga clic en el botón **Aceptar**.

5. Haga clic en el vínculo **Conexiones salientes** en el panel de detalles del nodo **Administración de firewall**.
   Se abre la ventana **Reglas de firewall para conexiones salientes**.

6. Cree y configure sus reglas de firewall para conexiones salientes.

1. Haga clic en el botón **Agregar** de la pestaña **Aplicaciones**.

   Se abre la ventana **Regla de firewall para la aplicación**.

2. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   > El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
   - **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

   c. En el campo **Ruta de la aplicación**, ingrese la ruta al archivo ejecutable de la aplicación para la que está configurando la regla. Puede indicar la ruta manualmente o puede utilizar el botón **Examinar**.

   d. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

   > Solo puede usar direcciones de tipo IPv4.

   e. Haga clic en el botón **Aceptar** para guardar la regla.

3. Haga clic en el botón **Agregar** de la pestaña **Puertos**.

   Se abre la ventana **Regla de firewall para puertos**.

4. Configure los parámetros de la regla:

   a. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

   b. En la lista **Acción de la regla**, seleccione una de las opciones:

   - **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
   - **Bloquear**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

   c. En el bloque **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

   d. Seleccione el tipo de protocolo (TCP/UDP) para el cual se controlarán las conexiones salientes.

   e. En el campo **Acción de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la

regla.

Solo puede usar direcciones de tipo IPv4.

f. Haga clic en el botón **Aceptar** para guardar la regla.

5. En la ventana **Reglas de firewall para conexiones salientes**, haga clic en el botón **Aceptar**.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La fecha y la hora en que se modificó la configuración de la tarea se guardarán en el registro de auditoría del sistema.

Habilitación y deshabilitación de Reglas de firewall

Para habilitar o deshabilitar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Administración de firewall** en el panel de detalles del nodo **Reglas de firewall**.

   Se abre la ventana **Reglas de firewall**.
4. Según el tipo de regla cuyo estado desee modificar, haga clic en los vínculos **Entrante** o **Saliente** y seleccione las pestañas **Aplicaciones** o **Puertos**.
5. En la lista de reglas, seleccione la regla cuyo estado desee modificar y realice una de las acciones siguientes:

   - Si desea habilitar una regla deshabilitada, seleccione la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se habilitará.

   - Si desea deshabilitar una regla habilitada, desactive la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se deshabilitará.
6. Haga clic en el botón **Reglas de firewall** de la ventana **Guardar**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Eliminación de reglas de firewall

Solo puede eliminar reglas de puerto y de aplicación. No puede eliminar reglas de grupo existentes.

Para eliminar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Administración de firewall** en el panel de detalles del nodo **Reglas de firewall**.

   Se abre la ventana **Reglas de firewall**.
4. Según el tipo de regla cuyo estado desee modificar, seleccione la pestaña **Aplicaciones** o **Puertos**.
5. En la lista de reglas, seleccione la regla que desee eliminar.
6. Haga clic en el botón **Eliminar**.

   La regla seleccionada se elimina.
7. Haga clic en el botón **Reglas de firewall** de la ventana **Guardar**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Configuración de la tarea Administración de firewall mediante el Complemento web

En esta sección, se brindan instrucciones para configurar los ajustes generales de la tarea Administración de firewall y para crear y configurar reglas de firewall a través del Complemento web.

Configuración de los ajustes generales de la tarea Administración de firewall

Para configurar los ajustes generales de la tarea Administración de firewall mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Control de actividad de red**.
5. Haga clic en el botón **Configuración** de la ventana **Administración de firewall**.

   Se abre la ventana **Administración de firewall**.
6. En la pestaña **General**, en el bloque **Integración con Firewall de Windows**, seleccione la opción de interacción entre Kaspersky Embedded Systems Security para Windows y el firewall de Windows:

   - **Observar el estado de Firewall de Windows El programa solo observa el estado de Firewall de Windows**. Si selecciona esta opción, la aplicación solo observará el estado del firewall de Windows y enviará un evento de advertencia a Kaspersky Security Center si el firewall de Windows no se ha iniciado.

Si selecciona esta opción para reemplazar la opción **Controlar la operación de Firewall de Windows El programa controla la operación de Firewall de Windows de acuerdo con los siguientes ajustes**, la aplicación restaurará la configuración interna del Firewall de Windows la siguiente vez que se inicie el sistema operativo del dispositivo protegido.

- **Controlar la operación de Firewall de Windows El programa controla la operación de Firewall de Windows de acuerdo con los siguientes ajustes**. Si selecciona esta opción, la aplicación monitoreará el Firewall de Windows en la medida en que lo determinan las siguientes opciones:
  - Mantener el estado de Firewall de Windows.
  - Administrar los ajustes y reglas de Firewall de Windows.
  - Permitir conexiones ICMP.

7. En el bloque **Conexiones entrantes**, configure los ajustes para las conexiones de red entrantes:

- Use la lista desplegable **Acción para conexiones entrantes** para especificar la acción que Firewall de Windows realizará para todas las conexiones de red entrantes, a menos que haya reglas de Firewall para conexiones entrantes que definan lo contrario.
- De ser necesario, agregue reglas de Firewall para conexiones entrantes.

  Las reglas que defina para las conexiones entrantes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de autorización para conexiones de red entrantes y selecciona **Bloquear** en la lista desplegable **Acción para conexiones entrantes**, Firewall de Windows permitirá las conexiones de red entrantes que coincidan con los criterios de la regla.

8. En el bloque **Conexiones salientes**, configure los ajustes para las conexiones de red salientes:

- Use la lista desplegable **Acción para conexiones salientes** para especificar la acción que Firewall de Windows realizará para todas las conexiones de red salientes, a menos que haya reglas de Firewall para conexiones salientes que definan lo contrario.
- De ser necesario, agregue reglas de Firewall para conexiones salientes.

  Las reglas que defina para las conexiones salientes en Firewall actuarán como exclusiones. Por ejemplo, si configura una regla de bloqueo para conexiones de red salientes y selecciona **Autorizar** en la lista desplegable **Acción para conexiones salientes**, Firewall de Windows bloqueará las conexiones de red salientes que coincidan con los criterios de la regla.

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

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Configuración	Descripción
Reglas de firewall para aplicaciones	Puede administrar las reglas de aplicación. Este tipo de regla permite conexiones de red específicas para aplicaciones determinadas. El criterio de activación para estas reglas se basa en una ruta de acceso a un archivo ejecutable.
Reglas de firewall para puertos	Puede administrar las reglas de puerto. Este tipo de regla permite las conexiones de red para los puertos y los protocolos especificados (TCP/UDP). Los criterios de activación para estas reglas se basan en el número de puerto y en el tipo de protocolo.

Administración de tareas	Puede configurar las opciones para iniciar la tarea en base a una programación.

Creación y configuración de reglas de firewall

Para crear y configurar reglas de firewall mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Control de actividad de red**.
5. Haga clic en el botón **Configuración** en el bloque **Administración de firewall**.

   Se abre la ventana **Administración de firewall**.
6. Cree y configure una regla de firewall entrante para la aplicación.

a. Seleccione la pestaña **Aplicaciones (conexiones entrantes)**.

b. Haga clic en el botón **Agregar**.

c. En la parte derecha de la ventana, active la casilla **Usar la regla** para habilitar la regla.

d. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

> El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red entrantes para aplicaciones.

e. En la lista **Acción de la regla**, seleccione una de las opciones:

- **Autorizar.** Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para la aplicación.
- **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para la aplicación.

f. En el campo **Ruta de la aplicación**, ingrese manualmente la ruta al archivo ejecutable de la aplicación para la que está configurando la regla.

g. En el campo **Área de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

> Solo puede usar direcciones de tipo IPv4.

h. Haga clic en el botón **Aceptar** para guardar la regla.

7. Cree y configure una regla de firewall para conexiones entrantes a puertos.

a. Seleccione la pestaña **Puertos (conexiones entrantes)**.

b. Haga clic en el botón **Agregar**.

c. En la parte derecha de la ventana, active la casilla **Usar la regla** para habilitar la regla.

d. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

> El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red entrantes para puertos.

e. En la lista **Acción de la regla**, seleccione una de las opciones:

- **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red entrantes para los puertos.
- **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red entrantes para los puertos.

f. En el bloque **Puertos locales**, ingrese un puerto o un intervalo de puertos.

g. Seleccione el tipo de protocolo (TCP/UDP) para el cual se controlarán las conexiones entrantes.

h. En el campo **Área de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones entrantes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

> Solo puede usar direcciones de tipo IPv4.

i. Haga clic en el botón **Aceptar** para guardar la regla.

8. Cree y configure una regla de firewall saliente para la aplicación.

a. Seleccione la pestaña **Aplicaciones (conexiones salientes)**.

b. Haga clic en el botón **Agregar**.

c. En la parte derecha de la ventana, active la casilla **Usar la regla** para habilitar la regla.

d. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

> El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes para aplicaciones.

e. En la lista **Acción de la regla**, seleccione una de las opciones:

- **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes para la aplicación.
- **Bloquear**. Si selecciona esta opción, la aplicación bloqueará las conexiones de red salientes para la aplicación.

f. En el campo **Ruta de la aplicación**, ingrese manualmente la ruta al archivo ejecutable de la aplicación para la que está configurando la regla.

g. En el campo **Área de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que se originen en las direcciones de red especificadas siguiendo los ajustes de la regla.

> Solo puede usar direcciones de tipo IPv4.

h. Haga clic en el botón **Aceptar** para guardar la regla.

9. Cree y configure una regla de firewall saliente para puertos.

a. Seleccione la pestaña **Puertos (conexiones salientes)**.

b. Haga clic en el botón **Agregar**.

c. En la parte derecha de la ventana, active la casilla **Usar la regla** para habilitar la regla.

d. En el campo **Nombre de la regla**, ingrese el nombre de la regla modificada.

El nombre de la regla, independientemente de las mayúsculas y minúsculas que contenga, no debe coincidir con los nombres reservados "All", "ICMPv4" e "ICMPv6"; tampoco debe repetirse en la lista de reglas para conexiones de red salientes para puertos.

e. En la lista **Acción de la regla**, seleccione una de las opciones:

- **Autorizar**. Si selecciona esta opción, la aplicación permitirá las conexiones de red salientes a los puertos.
- **Bloquear**. Si se selecciona esta opción, la aplicación bloquea las conexiones de red salientes a los puertos.

f. En el bloque **Puertos remotos**, ingrese un puerto o un intervalo de puertos.

g. Seleccione el tipo de protocolo (TCP/UDP) para el cual se controlarán las conexiones entrantes.

h. En el campo **Área de aplicación de la regla**, ingrese direcciones de red. La aplicación controlará las conexiones salientes que tengan como destino las direcciones de red especificadas siguiendo los ajustes de la regla.

Solo puede usar direcciones de tipo IPv4.

i. Haga clic en el botón **Aceptar** para guardar la regla.

10. Haga clic en el botón **Aceptar** de la ventana **Administración de firewall**.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La fecha y la hora en que se modificó la configuración se guardarán en el registro de auditoría del sistema.

Habilitación y deshabilitación de Reglas de firewall

Para habilitar o deshabilitar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Elija la sección **Control de actividad de red**.
5. Haga clic en el botón **Configuración** de la subsección **Administración de firewall**.
6. Según el tipo de regla cuyo estado desee modificar, seleccione la pestaña **Reglas de firewall para puertos** o **Reglas de firewall para aplicaciones**.
7. En la lista de reglas, seleccione la regla cuyo estado desee modificar y realice una de las acciones siguientes:
   - Si desea habilitar una regla deshabilitada, presione el botón ubicado a la izquierda del nombre de la regla para activarlo.
   - Si desea deshabilitar una regla habilitada, presione el botón ubicado a la izquierda del nombre de la regla para desactivarlo.
8. Haga clic en el botón **Aceptar**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Eliminación de reglas de firewall

Solo puede eliminar reglas de puerto y de aplicación. No puede eliminar reglas de grupo existentes.

Para eliminar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Control de actividad de red**.
5. Haga clic en el botón **Configuración** de la subsección **Administración de firewall**.
6. Según el tipo de regla que desee eliminar, seleccione la pestaña **Reglas de firewall para puertos** o **Reglas de firewall para aplicaciones**.
7. En la lista de reglas, seleccione la regla que desee eliminar.
8. Haga clic en el botón **Eliminar**.

   La regla seleccionada se elimina.
9. Haga clic en el botón **Aceptar**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Monitor de integridad de archivos

Esta sección contiene información sobre el inicio y la configuración de la tarea Monitor de integridad de archivos.

Acerca de la tarea Monitor de integridad de archivos

La tarea Monitor de integridad de archivos está diseñada para realizar un seguimiento de las acciones realizadas con los archivos y las carpetas especificados en las áreas de aplicación que se especifican en la configuración de la tarea. Puede usar la tarea de detectar los cambios en el archivo que podrían indicar una violación de la seguridad en el dispositivo protegido. También puede configurar que se realice un seguimiento de los cambios en el archivo durante periodos en los cuales la supervisión se interrumpe.

Una *interrupción de supervisión* ocurre cuando el área de supervisión temporalmente queda fuera del área de la tarea, por ejemplo, si la tarea se detiene o si un dispositivo externo no está físicamente presente en un dispositivo protegido. Kaspersky Embedded Systems Security para Windows informa las operaciones de archivos detectadas en el área de supervisión tan pronto como un dispositivo externo se conecta de nuevo.

Si las tareas dejan de ejecutarse en el área de supervisión especificada debido a una nueva instalación del componente Monitor de integridad de archivos, esto no constituye una interrupción de supervisión. En este caso, la tarea Monitor de integridad de archivos no se ejecuta.

Requisitos en el entorno

Para iniciar la tarea Monitor de integridad de archivos, se deben cumplir las siguientes condiciones:

- Los sistemas de archivos ReFS o NTFS deben usarse en el dispositivo protegido.
- Se debe habilitar el diario de USN de Windows. El componente le solicita a este diario recibir la información sobre operaciones con archivos.

  Si habilita el diario de USN después de que una regla se haya creado para un volumen y la tarea Monitor de integridad de archivos se ha iniciado, la tarea se debe reiniciar. Si no, la regla no se aplicará durante la supervisión.

Áreas de supervisión excluidas

Puede crear áreas de supervisión excluidas. Las exclusiones se especifican para cada regla independiente y funcionan solo para el área de supervisión indicada. Puede especificar un número ilimitado de exclusiones para cada regla.

Las exclusiones tienen mayor prioridad que el área de supervisión y no son supervisadas por la tarea, aun si una carpeta o el archivo indicado están dentro del área de supervisión. Si la configuración para una de las reglas especifica un área de supervisión a un nivel inferior que una carpeta especificada en exclusiones, el área de supervisión no se considera cuando la tarea se ejecuta.

Para especificar exclusiones, puede usar las mismas máscaras que se usan para especificar áreas de supervisión.

Acerca de las reglas de supervisión de operaciones de archivos

La tarea Monitor de integridad de archivos funciona sobre la base de reglas de supervisión de operaciones de archivos. Puede usar criterios de activación de reglas para configurar las condiciones que harán que se active la tarea la tarea; también puede ajustar el nivel de importancia que se dará a los eventos de operaciones de archivos que se detecten y se hagan constar en el registro de tareas.

Cada área de supervisión está asociada a una regla de supervisión de operaciones de archivos.

Puede configurar los siguientes criterios de activación de la regla:

- Usuarios de confianza
- Marcadores de operaciones con archivos

Usuarios de confianza

De forma predeterminada, la aplicación trata todas las acciones del usuario como posible violación de la seguridad. La lista de usuarios de confianza está vacía. Puede crear una lista de usuarios de confianza en los ajustes de las reglas de supervisión de operaciones de archivos para configurar el nivel de importancia de los eventos.

Usuario que no es de confianza: es un estado asignado a cualquier usuario no indicado en la lista de usuarios de confianza en la configuración de la regla del área de supervisión. Si Kaspersky Embedded Systems Security para Windows detecta una operación de archivo realizada por un usuario que no es de confianza, la tarea Monitor de integridad de archivos registrará un Evento crítico en el registro de tareas.

Usuario de confianza: es un estado asignado a un usuario o el grupo de usuarios autorizados para realizar operaciones con archivos en el área de supervisión especificada. Si Kaspersky Embedded Systems Security para Windows detecta operaciones de archivos realizadas por un usuario de confianza, la tarea Monitor de integridad de archivos registrará un Evento informativo en el registro de tareas.

Kaspersky Embedded Systems Security para Windows no puede determinar a los usuarios que inician operaciones durante las interrupciones de la supervisión. En este caso, el estado del usuario está determinado como desconocido.

Usuario desconocido: es un estado que se asigna a un usuario si Kaspersky Embedded Systems Security para Windows no puede recibir la información sobre un usuario debido a una interrupción de la tarea o una omisión del controlador de sincronización de datos o un diario de USN. Si Kaspersky Embedded Systems Security para Windows detecta una operación de archivos realizada por un usuario desconocido, la tarea Monitor de integridad de archivos registrará un evento de *Advertencia* en el registro de tareas.

Marcadores de operaciones con archivos

Cuando la tarea Monitor de integridad de archivos se ejecuta, Kaspersky Embedded Systems Security para Windows usa marcadores de operaciones de archivos para decidir que una acción se ha realizado en un archivo.

Un marcador de operaciones con archivos es un descriptor único que puede caracterizar una operación con archivos.

Cada operación con archivos puede ser una sola acción o una cadena de acciones con archivos. Cada acción de esta clase se compara con un marcador de operaciones con archivos. Si el marcador que especifica como criterio de activación de la regla se detecta en una cadena de operaciones con archivos, la aplicación registra un evento que indica que la operación con archivos dada se realizó.

El nivel de importancia de los eventos registrados no depende de los marcadores de operaciones con archivos seleccionados o el número de eventos.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera todos los marcadores de operaciones con archivos disponibles. Puede seleccionar marcadores de operaciones con archivos manualmente en la configuración de la regla de la tarea.

Establecer Marcadores de operación de los archivos

ID de operación con archivos	Marcador de operaciones con archivos	Sistemas de archivos admitidos
BASIC_INFO_CHANGE	Los atributos o los marcadores del tiempo de un archivo o carpeta cambiaron.	NTFS, ReFS
COMPRESSION_CHANGE	La compresión de un archivo o carpeta cambió.	NTFS, ReFS
DATA_EXTEND	El tamaño de archivo o carpeta aumentó.	NTFS, ReFS
DATA_OVERWRITE	El dato en un archivo o carpeta se sobrescribió.	NTFS, ReFS
DATA_TRUNCATION	Archivo o carpeta truncados.	NTFS, ReFS
EA_CHANGE	Los atributos de la carpeta o el archivo ampliado cambiaron.	Solo NTFS
ENCRYPTION_CHANGE	El estado del cifrado del archivo o la carpeta cambió.	NTFS, ReFS
FILE_CREATE	Archivo o carpeta creada por primera vez	NTFS, ReFS
FILE_DELETE	El archivo o la carpeta eliminados de forma permanente con la combinación SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	Vínculo físico creado o eliminado del archivo o la carpeta	Solo NTFS
INDEXABLE_CHANGE	El estado del índice de archivo o carpeta cambió.	NTFS, ReFS
INTEGRITY_CHANGE	El atributo de integridad cambió para un determinado flujo de archivos.	Solo ReFS
NAMED_DATA_EXTEND	El tamaño de un determinado flujo de archivos aumentó.	NTFS, ReFS
NAMED_DATA_OVERWRITE	Determinado flujo de archivos sobrescrito	NTFS, ReFS
NAMED_DATA_TRUNCATION	Determinado flujo de archivos truncado	NTFS, ReFS
OBJECT_ID_CHANGE	El identificador de archivo o carpeta cambió.	NTFS, ReFS
RENAME_NEW_NAME	Nombre nuevo asignado a archivo o carpeta	NTFS, ReFS
REPARSE_POINT_CHANGE	Nuevo punto de reanálisis creado o existente cambiado para un archivo o carpeta	NTFS, ReFS
SECURITY_CHANGE	Los derechos de acceso del archivo o la carpeta cambiaron.	NTFS, ReFS
STREAM_CHANGE	Determinado flujo de archivos nuevo creado o flujo de archivos existentes modificado	NTFS, ReFS

TRANSACTED_CHANGE	Flujo de archivos determinado modificado por transacción TxF	Solo ReFS

Configuración de la tarea Monitor de integridad de archivos predeterminada

De forma predeterminada, la tarea Monitor de integridad de archivos tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de la configuración en los siguientes componentes:

- El Complemento de administración
- La Consola de la aplicación
- El Complemento web

Configuración de la tarea Monitor de integridad de archivos predeterminada

Configuración	Valor predeterminado	Descripción
Área de supervisión	No definido	Use esta opción para especificar las carpetas y los archivos para los cuales las acciones se supervisarán. Los eventos de supervisión se generarán para las carpetas y los archivos en el área de supervisión especificada.
Lista de **Usuarios de confianza**	No definido	Use esta opción para especificar a usuarios o grupos de usuarios cuyas acciones en las carpetas especificadas serán tratadas como seguras por el componente.
Registrar información de operaciones con archivos que aparezca durante el período de interrupción de la supervisión	Utilizado	Este ajuste de configuración se utiliza para habilitar o deshabilitar el registro de operaciones de archivos que ocurren en las áreas de supervisión especificadas durante los períodos en los que la tarea está inactiva. De forma predeterminada, se recopilan estadísticas sobre usuarios y objetos que son desconocidos y que no son de confianza.
Bloquear intentos de comprometer el registro de USN	Utilizado	Use esta opción para habilitar o deshabilitar la protección de cualquier registro de USN.
Detectar y bloquear todas las operaciones de archivos en el área seleccionada	Deshabilitado	Active o desactive la casilla **Detectar y bloquear todas las operaciones de archivos en el área seleccionada** si desea impedir todo cambio en el área de supervisión seleccionada.
Excluir las siguientes carpetas del control	No aplicado	Use esta opción para examinar el uso de exclusiones a fin de ver las carpetas donde las operaciones con archivos no se tienen que supervisar. Cuando se ejecute la tarea Monitor de integridad de archivos, Kaspersky Embedded Systems Security para Windows omite las áreas de supervisión especificadas como exclusiones.
Cálculo de la suma de control	No aplicado	Use esta opción para configurar el cálculo de la suma de control del archivo después de que se hayan realizado cambios en el archivo.
Marcadores de	Todos los	Use esta opción para especificar el grupo de marcadores de

operaciones con archivos	marcadores de operaciones con archivos disponibles se consideran.	operación de los archivos. Si una operación con archivos realizada en un área de supervisión es caracterizada por uno o varios marcadores especificados, Kaspersky Embedded Systems Security para Windows genera un evento de auditoría.
Programación de inicio de tareas	La primera ejecución no está programada.	Puede configurar las opciones para iniciar la tarea en base a una programación.

Administrar el Monitor de integridad de archivos mediante el Complemento de administración

En esta sección, aprenda cómo configurar la tarea Monitor de integridad de archivos mediante el Complemento de administración.

Configuración de la tarea Monitor de integridad de archivos

Para configurar los ajustes de la tarea Monitor de integridad de archivos mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Inspección del sistema**, dentro del bloque **Monitor de integridad de archivos**, haga clic en el botón **Configuración**.

   Se abre la ventana **Monitor de integridad de archivos**.
5. En la pestaña **Configuración de supervisión de operaciones de archivos**, configure los siguientes parámetros:
   - Seleccione o desactive la casilla de verificación **Registrar información de las operaciones con archivos que aparezca durante el período de interrupción de la supervisión**.

La casilla habilita o deshabilita la supervisión de las operaciones de archivos especificadas en la configuración de la tarea Monitor de integridad de archivos cuando la tarea no se está ejecutando por algún motivo (la remoción de un disco duro, la tarea fue detenida por usuario, error de software).

Si la casilla se selecciona, Kaspersky Embedded Systems Security para Windows registrará eventos en todos los alcances de supervisión cuando la tarea Monitor de integridad de archivos no se ejecute.

Si la casilla se desactiva, la aplicación no registrará las operaciones con archivos en las áreas de supervisión cuando la tarea no se esté ejecutando.

De forma predeterminada, la casilla está activada.

- Desactive o seleccione la casilla **Bloquear intentos de comprometer el registro de USN**.

  La casilla habilita o deshabilita la protección del registro de USN.

  Si la casilla está seleccionada, Kaspersky Embedded Systems Security para Windows bloqueará los intentos de eliminar el registro de USN o comprometer el contenido del registro de USN.

  Si la casilla está desactivada, la aplicación no supervisará los cambios realizados en el registro de USN.

  De forma predeterminada, la casilla está activada.

6. Agregue las reglas de supervisión de operaciones de archivos que determinarán el accionar de la tarea.
7. En la pestaña **Administración de tareas**, configure el inicio programado de la tarea.
8. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La información acerca de la fecha y hora de modificación de la configuración se guarda en el registro de auditoría del sistema.

Creación y configuración de una regla de supervisión de operaciones de archivos

Para crear y configurar una regla de supervisión de operaciones de archivos mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. Realice una de las siguientes opciones:

   - Si va a crear una regla de supervisión de operaciones de archivos en una directiva, en la sección **Inspección del sistema**, dentro del bloque **Monitor de integridad de archivos**, haga clic en el botón **Configuración**.

Se abre la **Configuración de supervisión de operaciones de archivos** de la ventana **Monitor de integridad de archivos**.

- Si va a crear una regla de supervisión de operaciones de archivos para una tarea local, en la ventana **Propiedades: Monitor de integridad de archivos**, vaya a la sección **Configuración**.

5. En el bloque **Área de supervisión**, haga clic en el botón **Agregar**.

   Aparece la ventana **Regla de supervisión de operaciones de archivos**.

6. Utilice uno de estos métodos para agregar un área de supervisión de operaciones de archivos:

   - Si desea seleccionar una carpeta o unidad a través del cuadro de diálogo estándar de Microsoft Windows:

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

        Aparece la ventana estándar **Buscar carpeta** de Microsoft Windows.

     b. Seleccione la carpeta cuyas operaciones de archivos desee supervisar.

     c. Haga clic en el botón **Aceptar**.

   - Si desea especificar un área de supervisión manualmente, agregue una ruta mediante una máscara admitida:

     - <*.ext>: todos los archivos con la extensión <ext>, sin tener en cuenta su ubicación
     - <*\name.ext>: todos los archivos con nombre <nombre> y extensión <ext>, sin tener en cuenta su ubicación
     - <\dir*> - todos los archivos en la carpeta <\dir>
     - <\dir*\name.ext>: todos los archivos con el nombre <nombre> y la extensión <ext> en la carpeta <\dir> y todas sus carpetas secundarias

   Al especificar un área de supervisión manualmente, asegúrese de que la ruta esté en el formato siguiente: <letra del volumen>:\<máscara> Si la letra del volumen falta, Kaspersky Embedded Systems Security para Windows no agregará el área de supervisión especificada.

7. Si es necesario, especifique usuarios de confianza:

   a. En la pestaña **Usuarios de confianza**, en el menú contextual del botón **Agregar**, seleccione el método que desee usar para agregar los usuarios de confianza.

      Se abre la ventana **Selección de usuario o grupo de usuarios**.

   b. Seleccione los usuarios o los grupos de usuarios que podrán realizar operaciones de archivos en el área de supervisión seleccionada.

   c. Haga clic en el botón **Aceptar**.

   De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera que no son de confianza todos aquellos usuarios que no figuran en la lista de usuarios de confianza y genera eventos críticos para ellos. Las estadísticas se compilan para los usuarios de confianza.

8. En la pestaña **Marcadores de operaciones con archivos**, de ser necesario, indique los marcadores de operaciones con archivos que desee monitorear:

a. Seleccione la opción **Detectar las operaciones de archivo en función de los siguientes marcadores**.

b. En la lista de operaciones con archivos disponibles, seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows atiende a todos los marcadores de operaciones con archivos disponibles. La opción **Detectar las operaciones de archivo en función de todos los marcadores reconocibles** está seleccionada.

9. Si desea bloquear todas las operaciones con archivos para el área seleccionada, active la casilla **Detectar y bloquear todas las operaciones de archivos en el área seleccionada**.

10. Si desea que la aplicación calcule la suma de control de un archivo que se ha modificado:

a. Seleccione la opción **Calcular la suma de control del archivo, si es posible. La suma de control se podrá visualizar en el informe de tareas**.

b. En la lista desplegable **Tipo de suma de control**, seleccione una de las opciones:

- **Hash MD5**
- **Hash SHA256**.

11. De ser necesario, agregue las carpetas o unidades que desee excluir del área de supervisión de operaciones de archivos seleccionada:

a. En la pestaña **Exclusiones**, active la casilla **Excluir las siguientes carpetas del control**.

b. Haga clic en el botón **Agregar**.

Se abre la ventana **Exclusión del área controlada**.

c. Haga clic en el botón **Examinar**.

Aparece la ventana estándar **Buscar carpeta** de Microsoft Windows.

d. Seleccione una carpeta o unidad.

e. Haga clic en el botón **Aceptar**.

La carpeta o unidad especificada se mostrará en la lista de exclusiones de la pestaña **Exclusiones**.

También puede agregar las áreas de supervisión que desee excluir manualmente, usando las mismas máscaras que se utilizan para definir las áreas de supervisión de operaciones de archivos.

12. Haga clic en el botón **Regla de supervisión de operaciones de archivos** en la ventana **Aceptar**.

La regla de supervisión de operaciones de archivos configurada se mostrará en las ventanas **Monitor de integridad de archivos** o **Propiedades: Monitor de integridad de archivos**, dentro del bloque **Área de supervisión**.

Exportación e importación de reglas de supervisión de operaciones de archivos

Puede exportar a un archivo XML las reglas de supervisión de operaciones de archivos que haya creado manualmente en las propiedades de la tarea Monitor de integridad de archivos.

Puede importar las reglas de supervisión de operaciones de archivos que haya exportado a un archivo XML a las propiedades de la tarea Monitor de integridad de archivos.

Para exportar o importar reglas de supervisión de operaciones de archivos mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. Realice una de las siguientes opciones:
   - Si desea importar o exportar las reglas de supervisión de operaciones de archivos definidas en una directiva, en la sección **Inspección del sistema**, dentro del bloque **Monitor de integridad de archivos**, haga clic en el botón **Configuración**.

     Se abre la pestaña **Monitor de integridad de archivos** de la ventana **Configuración de supervisión de operaciones de archivos**.
   - Si desea importar o exportar las reglas de supervisión de operaciones de archivos definidas en una tarea local, en la ventana **Propiedades: Monitor de integridad de archivos**, vaya a la sección **Configuración**.
5. Exporte o importe las reglas de supervisión de operaciones de archivos:
   - Cómo exportar reglas de supervisión de operaciones de archivos.

     1. En el bloque **Área de supervisión**, haga clic en el botón **Exportar**.

        Se abre la ventana **Guardar como** estándar de Microsoft Windows.
     2. Indique la ruta en la que desea guardar el archivo XML con la configuración de las reglas de supervisión de operaciones de archivos.
     3. Ingrese el nombre del archivo en el campo correspondiente.
     4. Haga clic en el botón **Guardar**.

        La aplicación guardará un archivo XML con la configuración de las reglas de supervisión de operaciones de archivos en la ruta especificada.

- Cómo importar reglas para las reglas de supervisión de operaciones de archivos.

  1. En el bloque **Área de supervisión**, haga clic en el botón **Importar**.
  2. En el menú contextual del botón **Importar**, seleccione uno de los valores posibles:
     - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.
     - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
     - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

     Se abre la ventana estándar **Abrir** de Microsoft Windows.
  3. Indique la ruta al archivo XML con la configuración de las reglas de supervisión de operaciones de archivos.
  4. Haga clic en el botón **Abrir**.

     Las reglas importadas se mostrarán en el bloque **Área de supervisión** de las ventanas **Monitor de integridad de archivos** o **Propiedades: Monitor de integridad de archivos**.

6. Haga clic en el botón **Guardar** para guardar los cambios.

Administrar el Monitor de integridad de archivos mediante la Consola de la aplicación

En esta sección, aprenda cómo configurar la tarea Monitor de integridad de archivos mediante la Consola de la aplicación.

Configuración de la tarea Monitor de integridad de archivos

Para configurar los ajustes generales de la tarea Monitor de integridad de archivos mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de integridad de archivos**.
3. Haga clic en el vínculo **Propiedades** en el panel de resultados del nodo **Monitor de integridad de archivos**.

   Aparece la ventana **Configuración de tareas**.
4. En la pestaña **General**, configure los siguientes ajustes:

a. Seleccione o desactive la casilla de verificación **Registrar información de operaciones con archivos que aparezca durante el período de interrupción de la supervisión**.

La casilla habilita o deshabilita la supervisión de las operaciones de archivos especificadas en la configuración de la tarea Monitor de integridad de archivos cuando la tarea no se está ejecutando por algún motivo (la remoción de un disco duro, la tarea fue detenida por usuario, error de software).

Si la casilla se selecciona, Kaspersky Embedded Systems Security para Windows registrará eventos en todos los alcances de supervisión cuando la tarea Monitor de integridad de archivos no se ejecute.

Si la casilla se desactiva, la aplicación no registrará las operaciones con archivos en las áreas de supervisión cuando la tarea no se esté ejecutando.

De forma predeterminada, la casilla está activada.

b. Desactive o seleccione la casilla **Bloquear intentos de comprometer el registro de USN**.

La casilla habilita o deshabilita la protección del registro de USN.

Si la casilla está seleccionada, Kaspersky Embedded Systems Security para Windows bloqueará los intentos de eliminar el registro de USN o comprometer el contenido del registro de USN.

Si la casilla está desactivada, la aplicación no supervisará los cambios realizados en el registro de USN.

De forma predeterminada, la casilla está activada.

5. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas.

6. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La información acerca de la fecha y hora de modificación de la configuración se guarda en el registro de auditoría del sistema.

Creación y configuración de una regla de supervisión de operaciones de archivos

Para crear y configurar una regla de supervisión de operaciones de archivos mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.

2. Seleccione el nodo secundario **Monitor de integridad de archivos**.

3. Haga clic en el vínculo **Monitor de integridad de archivos** en el panel de resultados del nodo **Reglas de supervisión de operaciones de archivos**.

   Aparece la ventana **Reglas de supervisión de operaciones de archivos**.

4. Utilice uno de estos métodos para definir la ruta del área supervisión de operaciones de archivos:

   - Si desea seleccionar una carpeta o unidad a través del cuadro de diálogo estándar de Microsoft Windows:

     a. En el lado izquierdo de la ventana, haga clic en el botón **Examinar**.

     Aparece la ventana estándar **Buscar carpeta** de Microsoft Windows.

     b. Seleccione la carpeta cuyas operaciones de archivos desee supervisar.

c. Haga clic en el botón **Aceptar**.

- Si desea especificar un área de supervisión manualmente, agregue una ruta mediante una máscara admitida:
  - <*.ext>: todos los archivos con la extensión <ext>, sin tener en cuenta su ubicación
  - <*\name.ext>: todos los archivos con nombre <nombre> y extensión <ext>, sin tener en cuenta su ubicación
  - <\dir*> - todos los archivos en la carpeta <\dir>
  - <\dir*\name.ext>: todos los archivos con el nombre <nombre> y la extensión <ext> en la carpeta <\dir> y todas sus carpetas secundarias

Al especificar un área de supervisión manualmente, asegúrese de que la ruta esté en el formato siguiente: <letra del volumen>:\<máscara> Si la letra del volumen falta, Kaspersky Embedded Systems Security para Windows no agregará el área de supervisión especificada.

5. Haga clic en el botón **Agregar**.

   El área de supervisión se mostrará en la lista ubicada en el lado izquierdo de la ventana **Reglas de supervisión de operaciones de archivos**.

6. Si es necesario, especifique usuarios de confianza:

   a. En la pestaña **Usuarios de confianza**, haga clic en el botón **Agregar**.

   Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.

   b. Seleccione los usuarios o grupos de usuarios a los que se les permitirá realizar operaciones con archivos en el área de supervisión seleccionada.

   c. Haga clic en el botón **Aceptar**.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera que no son de confianza todos aquellos usuarios que no figuran en la lista de usuarios de confianza y genera eventos críticos para ellos. Las estadísticas se compilan para los usuarios de confianza.

7. En la pestaña **Marcadores de operaciones con archivos**, de ser necesario, indique los marcadores de operaciones con archivos que desee monitorear:

   a. Seleccione la opción **Detectar las operaciones de archivo en función de los siguientes marcadores**.

   b. En la lista de operaciones con archivos disponibles, seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows atiende a todos los marcadores de operaciones con archivos disponibles. La opción **Detectar las operaciones de archivo en función de todos los marcadores reconocibles** está seleccionada.

8. Si desea bloquear todas las operaciones con archivos en el área de supervisión seleccionada, active la casilla **Detectar y bloquear todas las operaciones de archivos en el área seleccionada**.

9. Si desea que la aplicación calcule la suma de control de un archivo que se ha modificado:

a. En el bloque **Cálculo de la suma de control**, active la casilla **Calcular la suma de control de la versión final de un archivo luego de que este se haya modificado, si fuera posible. La suma de control se podrá ver en el registro de tareas**. **La suma de control se podrá visualizar en el registro de tareas**.

b. En la lista desplegable **Calcular la suma de control que usa el algoritmo**, seleccione una de las opciones:

- **Hash MD5**
- **Hash SHA256**.

10. De ser necesario, agregue carpetas o unidades que desee excluir de la supervisión de operaciones de archivos:

a. En la pestaña **Establecer exclusiones**, active la casilla **Tener en cuenta el área de supervisión excluida**.

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

Aparece la ventana estándar **Buscar carpeta** de Microsoft Windows.

c. Seleccione una carpeta o unidad.

d. Haga clic en el botón **Aceptar**.

e. Haga clic en el botón **Agregar**.

La carpeta o unidad especificada se mostrará en la lista de exclusiones.

> También puede agregar las áreas de supervisión que desee excluir manualmente, usando las mismas máscaras que se utilizan para definir las áreas de supervisión de operaciones de archivos.

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

Exportación e importación de reglas de supervisión de operaciones de archivos

Puede exportar a un archivo XML las reglas de supervisión de operaciones de archivos que haya creado manualmente en las propiedades de la tarea Monitor de integridad de archivos.

Puede importar las reglas de supervisión de operaciones de archivos que haya exportado a un archivo XML a las propiedades de la tarea Monitor de integridad de archivos.

Para exportar o importar reglas de supervisión de operaciones de archivos mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de integridad de archivos**.
3. Haga clic en el vínculo **Monitor de integridad de archivos** en el panel de resultados del nodo **Reglas de supervisión de operaciones de archivos**.

Aparece la ventana **Reglas de supervisión de operaciones de archivos**.

4. Exporte o importe las reglas de supervisión de operaciones de archivos:

- Cómo exportar reglas de supervisión de operaciones de archivos.

  1. En la parte izquierda de la ventana **Reglas de supervisión de operaciones de archivos**, haga clic en el botón **Exportar**.

     Se abre la ventana **Guardar como** estándar de Microsoft Windows.

  2. Indique la ruta en la que desea guardar el archivo XML con la configuración de las reglas de supervisión de operaciones de archivos.

  3. Ingrese el nombre del archivo en el campo correspondiente.

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

     La aplicación guardará un archivo XML con la configuración de las reglas de supervisión de operaciones de archivos en la ruta especificada.

- Cómo importar reglas para las reglas de supervisión de operaciones de archivos.

  1. En la parte izquierda de la ventana **Reglas de supervisión de operaciones de archivos**, haga clic en el botón **Importar**.

  2. En el menú contextual del botón **Importar**, seleccione uno de los valores posibles:

     - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica no se duplican. Si una regla tiene al menos un valor de configuración único, esa regla se agrega.
     - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
     - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

     Se abre la ventana estándar **Abrir** de Microsoft Windows.

  3. Indique la ruta al archivo XML con la configuración de las reglas de supervisión de acceso al registro.

  4. Haga clic en el botón **Abrir**.

     Las reglas importadas se mostrarán en la parte izquierda de la ventana **Reglas de supervisión de operaciones de archivos**.

5. Haga clic en el botón **Guardar** para guardar los cambios.

Administrar el Monitor de integridad de archivos mediante el Complemento web

En esta sección, aprenda cómo configurar la tarea Monitor de integridad de archivos mediante el Complemento web.

Configuración de la tarea Monitor de integridad de archivos

Para configurar la tarea Monitor de integridad de archivos mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Inspección del sistema**.
5. En la subsección **Monitor de integridad de archivos**, haga clic en el botón **Configuración**.

   Se abre la ventana **Monitor de integridad de archivos**.
6. En la pestaña **Configuración de supervisión de operaciones de archivos**, configure los siguientes parámetros:

   a. Seleccione o desactive la casilla de verificación **Registrar información de las operaciones sobre archivos que se realicen durante el período de interrupción de la supervisión**.

   La casilla habilita o deshabilita la supervisión de las operaciones de archivos especificadas en la configuración de la tarea Monitor de integridad de archivos cuando la tarea no se está ejecutando por algún motivo (la remoción de un disco duro, la tarea fue detenida por usuario, error de software).

   Si la casilla se selecciona, Kaspersky Embedded Systems Security para Windows registrará eventos en todos los alcances de supervisión cuando la tarea Monitor de integridad de archivos no se ejecute.

   Si la casilla se desactiva, la aplicación no registrará las operaciones con archivos en las áreas de supervisión cuando la tarea no se esté ejecutando.

   De forma predeterminada, la casilla está activada.

   b. Desactive o seleccione la casilla **Bloquear intentos de comprometer el registro de USN**.

   La casilla habilita o deshabilita la protección del registro de USN.

   Si la casilla está seleccionada, Kaspersky Embedded Systems Security para Windows bloqueará los intentos de eliminar el registro de USN o comprometer el contenido del registro de USN.

   Si la casilla está desactivada, la aplicación no supervisará los cambios realizados en el registro de USN.

   De forma predeterminada, la casilla está activada.
7. En la pestaña **Administración de tareas**, configure la programación de inicio de tareas.
8. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La información acerca de la fecha y hora de modificación de la configuración se guarda en el registro de auditoría del sistema.

Creación y configuración de una regla de supervisión de operaciones de archivos

Para crear y configurar una regla de supervisión de operaciones de archivos mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Inspección del sistema**.
5. En la subsección **Monitor de integridad de archivos**, haga clic en el botón **Configuración**.

   Se abre la pestaña **Monitor de integridad de archivos** de la ventana **Configuración de supervisión de operaciones de archivos**.
6. Haga clic en el botón **Agregar**.

   Aparece la ventana **Regla de supervisión de operaciones de archivos**.
7. En **Supervisar las operaciones de archivo en estas áreas**, indique una ruta utilizando alguna de las máscaras posibles:
   - <*.ext>: todos los archivos con la extensión <ext>, sin tener en cuenta su ubicación
   - <*\name.ext>: todos los archivos con nombre <nombre> y extensión <ext>, sin tener en cuenta su ubicación
   - <\dir*> - todos los archivos en la carpeta <\dir>
   - <\dir*\name.ext>: todos los archivos con el nombre <nombre> y la extensión <ext> en la carpeta <\dir> y todas sus carpetas secundarias

   Al especificar un área de supervisión manualmente, asegúrese de que la ruta esté en el formato siguiente: <letra del volumen>:\<máscara> Si la letra del volumen falta, Kaspersky Embedded Systems Security para Windows no agregará el área de supervisión especificada.
8. En la pestaña **Usuarios de confianza**, si es necesario, especifique los usuarios de confianza de una de las siguientes maneras:
   - Si desea utilizar el botón **Agregar**:
     a. Haga clic en el botón **Agregar**.
     b. En la ventana que se abre, en el campo **Nombre de usuario**, especifique el usuario o grupo de usuarios en formato SID.
     c. Haga clic en el botón **Aceptar**.
   - Si desea utilizar el botón **Agregar de la lista del Servidor de administración**:
     a. Haga clic en el botón **Agregar de la lista del Servidor de administración**.
     b. En la ventana que se abre, seleccione un usuario o grupo de usuarios de la lista.
     c. Haga clic en el botón **Aceptar**.

Los usuarios de confianza podrán operar con archivos del área de supervisión seleccionada.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera que no son de confianza todos aquellos usuarios que no figuran en la lista de usuarios de confianza y genera eventos críticos para ellos. Las estadísticas se compilan para los usuarios de confianza.

9. En la pestaña **Marcadores de operaciones con archivos**, de ser necesario, indique los marcadores de operaciones con archivos que desee monitorear:

   a. Seleccione la opción **Detectar las operaciones de archivo en función de los siguientes marcadores**.

   b. En la lista de operaciones con archivos disponibles, seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

   De forma predeterminada, Kaspersky Embedded Systems Security para Windows atiende a todos los marcadores de operaciones con archivos disponibles. La opción **Detectar las operaciones de archivo en función de todos los marcadores reconocibles** está seleccionada.

10. Si desea bloquear todas las operaciones con archivos en el área de supervisión seleccionada, active la casilla **Detectar y bloquear todas las operaciones de archivos en el área seleccionada**.

11. Si desea que la aplicación calcule la suma de control de un archivo que se ha modificado:

    a. Seleccione la opción **Calcular la suma de control del archivo, si es posible. La suma de control se podrá visualizar en el informe de tareas**.

    b. En la lista desplegable **Tipo de suma de control**, seleccione una de las opciones:

    - **Hash SHA256**.
    - **Hash MD5**.

12. De ser necesario, agregue carpetas o unidades que desee excluir de la supervisión de operaciones de archivos:

    a. En la pestaña **Exclusiones**, active la casilla **Excluir las siguientes carpetas del control**.

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

    c. En la ventana que se abre a la derecha, en el campo **Nombre de la carpeta**, ingrese la ruta a la carpeta o unidad que desee excluir del área de supervisión de operaciones de archivos.

    d. Haga clic en el botón **Aceptar**.

    La ruta a la carpeta o unidad especificada se mostrará en la lista.

13. Haga clic en el botón **Aceptar** en la ventana **Regla de supervisión de operaciones de archivos**.

La regla de supervisión de operaciones de archivos configurada se mostrará en la ventana **Monitor de integridad de archivos**, en la pestaña **Configuración de supervisión de operaciones de archivos**.

Exportación e importación de reglas de supervisión de operaciones de archivos

Puede exportar a un archivo XML las reglas de supervisión de operaciones de archivos que haya creado manualmente en las propiedades de la tarea Monitor de integridad de archivos.

Puede importar las reglas de supervisión de operaciones de archivos que haya exportado a un archivo XML a las propiedades de la tarea Monitor de integridad de archivos.

Para exportar o importar reglas de supervisión de operaciones de archivos mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Inspección del sistema**.
5. En la subsección **Monitor de integridad de archivos**, haga clic en el botón **Configuración**.

   Se abre la pestaña **Monitor de integridad de archivos** de la ventana **Configuración de supervisión de operaciones de archivos**.
6. Exporte o importe las reglas de supervisión de operaciones de archivos:

   - Cómo exportar reglas de supervisión de operaciones de archivos.

     Haga clic en el botón **Exportar**.

     La aplicación guardará el archivo FileIntegrityMonitor.xml, que contendrá la configuración de las reglas de supervisión de operaciones de archivos, en la carpeta C:\Usuarios\<Nombre de usuario>\Descargas.

   - Cómo importar reglas para las reglas de supervisión de operaciones de archivos.

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

   Se abre la ventana estándar **Abrir** de Microsoft Windows.

2. Indique la ruta al archivo XML con la configuración de las reglas de supervisión de operaciones de archivos.

3. Haga clic en el botón **Abrir**.

   Las reglas que se importen mediante la combinación de listas de reglas se mostrarán en la pestaña **Configuración de supervisión de operaciones de archivos** de la ventana **Monitor de integridad de archivos**.

   Si en la lista de reglas importadas existe una regla del Monitor de integridad de archivos cuya configuración sea idéntica a la de una regla existente, la regla de la lista importada no será agregada.

7. Haga clic en el botón **Aceptar** para guardar los cambios.

Escáner AMSI

Esta sección contiene información acerca de la tarea del Escáner AMSI y cómo configurarla.

Acerca de la tarea del Escáner AMSI

Cuando se ejecuta la tarea del Escáner AMSI, Kaspersky Embedded Systems Security controla la ejecución de los scripts creados con tecnologías de scripting de Microsoft Windows (Active Scripting) como VBScript o JScript®. La aplicación también puede procesar los scripts de PowerShell™ y los scripts que se ejecutan en las aplicaciones de Microsoft Office en sistemas operativos con la Interfaz de análisis antimalware (AMSI) instalada. Puede permitir o bloquear la ejecución de un script que se considere peligroso o probablemente peligroso. Si Kaspersky Embedded Systems Security identifica un script como potencialmente peligroso, bloquea o permite la ejecución del script de acuerdo con la acción seleccionada. Si se selecciona la acción **Bloquear**, la aplicación permite la ejecución del script solo si se considera que un script es seguro.

A partir del sistema operativo Microsoft Windows 10 y Microsoft Windows Server 2016, Kaspersky Embedded Systems Security para Windows es compatible con la Interfaz de análisis antimalware (AMSI). AMSI permite que las aplicaciones y los servicios se integren con cualquier aplicación antimalware instalada en un dispositivo para que el antimalware intercepte y analice todos los scripts ejecutados.

Puede encontrar más información sobre la funcionalidad AMSI en el sitio web de Microsoft Windows.

Puede configurar las opciones de la tarea del Escáner AMSI.

Configuración predeterminada de la tarea del Escáner AMSI

La tarea del sistema local del Escáner AMSI utiliza la configuración predeterminada que se describe en la tabla a continuación. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea del Escáner AMSI

Configuración	Valor predeterminado	Descripción
Acción que se realizará con los scripts probablemente peligrosos	**Bloquear**	Puede especificar la acción que se realizará al detectar scripts probablemente peligrosos: bloquear o permitir su ejecución.
Analizador heurístico	Se aplica el nivel de seguridad **Medio**.	El analizador heurístico se puede habilitar o deshabilitar. El nivel de análisis se puede configurar.
Zona de confianza	Utilizado	Lista general de exclusiones que se pueden utilizar en tareas seleccionadas.

Configuración de las opciones de la tarea del Escáner AMSI a través del Complemento de administración

Para configurar una tarea del Escáner AMSI, haga lo siguiente:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Protección del servidor en tiempo real** de la ventana **Propiedades: <Nombre de la directiva>**, haga clic en **Configuración** del **Escáner AMSI**.

5. En la sección **Acción que se realizará con los scripts probablemente peligrosos**, en la pestaña **General**, realice una de las siguientes acciones:

   - Para permitir la ejecución de scripts probablemente peligrosos, seleccione **Autorizar**.

   - Para bloquear la ejecución de scripts probablemente peligrosos, seleccione **Bloquear**.

6. En la sección **Analizador heurístico**, realice una de las siguientes acciones:

   - Borre o seleccione la casilla de verificación **Usar el analizador heurístico**.

   - Si es necesario, ajuste el nivel de análisis con el control deslizante.

7. En la sección **Zona de confianza**, seleccione o desactive la casilla **Aplicar zona de confianza**.

8. Haga clic en el botón **Aceptar**.

Se aplica la configuración reciente.

Configuración de las opciones de la tarea del Escáner AMSI a través de la Consola de la aplicación

Para configurar una tarea del Escáner AMSI, haga lo siguiente:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.

2. Seleccione el nodo secundario **Escáner AMSI**.

3. Haga clic en el vínculo **Propiedades** en el panel de resultados del nodo.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.

4. En la sección **Acción que se realizará con los scripts probablemente peligrosos**, realice una de las siguientes acciones:

   - Para permitir la ejecución de scripts probablemente peligrosos, seleccione **Autorizar**.

   - Para bloquear la ejecución de scripts probablemente peligrosos, seleccione **Bloquear**.

5. En la sección **Analizador heurístico**, realice una de las siguientes acciones:

   - Borre o seleccione la casilla de verificación **Usar el analizador heurístico**.

- Si es necesario, ajuste el nivel de análisis con el control deslizante.

6. En la sección **Zona de confianza**, seleccione o desactive la casilla **Aplicar zona de confianza**.
7. Haga clic en el botón **Aceptar**.

Se aplica la configuración reciente.

Configuración de las opciones de la tarea del Escáner AMSI a través del Complemento web

Para configurar una tarea del Escáner AMSI, haga lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Protección del servidor en tiempo real**.
5. Haga clic en **Configuración** en la subsección **Escáner AMSI**.
6. En la sección **Acción que se realizará con los scripts probablemente peligrosos**, en la pestaña **General**, realice una de las siguientes acciones:
   - Para permitir la ejecución de scripts probablemente peligrosos, seleccione **Autorizar**.
   - Para bloquear la ejecución de scripts probablemente peligrosos, seleccione **Bloquear**.
7. En la sección **Analizador heurístico**, realice una de las siguientes acciones:
   - Borre o seleccione la casilla de verificación **Usar el analizador heurístico**.
   - Si es necesario, ajuste el nivel del análisis heurístico.
8. En la sección **Zona de confianza**, seleccione o desactive la casilla **Aplicar zona de confianza**.
9. Haga clic en el botón **Aceptar**.

Se aplica la configuración reciente.

Estadísticas de la tarea del Escáner AMSI

Mientras se ejecuta la tarea del **Escáner AMSI**, puede ver información sobre la cantidad de scripts que procesó Kaspersky Embedded Systems Security desde el momento en que se inició la tarea.

Para ver las estadísticas de la tarea del Escáner AMSI, haga lo siguiente:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.

2. Seleccione el nodo secundario **Escáner AMSI**.

Las estadísticas de la tarea actual se muestran en el panel de resultados del nodo en las secciones **Administración** y **Estadísticas**.

Puede consultar la información sobre objetos procesados por Kaspersky Embedded Systems Security para Windows desde que la tarea se inició (consulte la tabla a continuación).

Estadísticas de la tarea del Escáner AMSI

Campo	Descripción
Scripts bloqueados	Número de scripts que bloqueó Kaspersky Embedded Systems Security.
Scripts peligrosos detectados	Número de scripts peligrosos detectados.
Scripts probablemente peligrosos detectados	Número de scripts probablemente peligrosos detectados.
Scripts procesados	Número total de scripts procesados.

Monitor de acceso a registros

En esta sección, se explica cómo iniciar y configurar la tarea Monitor de acceso a registros.

Acerca de la tarea Monitor de acceso a registros

La tarea Monitor de acceso al registro está diseñada para realizar un seguimiento de las acciones que se realizan con las ramas y claves de registro especificadas en las áreas de supervisión que se definen en la configuración de la tarea. La tarea realiza un seguimiento de las acciones dentro del sistema operativo instalado en el dispositivo o dentro de los contenedores de Windows Server 2016 y versiones posteriores definidos en el área de la supervisión. Puede usar la tarea para detectar los cambios que indican una violación de la seguridad en el dispositivo protegido.

Para iniciar la tarea Monitor de acceso al registro, debe configurar al menos una regla de supervisión.

Acerca de las reglas de monitoreo de acceso al registro

La tarea **Monitor de acceso al registro** funciona sobre la base de reglas de monitoreo de acceso al registro. Puede usar los criterios de activación de la regla para configurar las condiciones que activan la tarea y establecen el nivel de importancia de los eventos detectados y registrados en el registro de tareas.

Cada área de supervisión está asociada a una regla de monitoreo de acceso al registro.

Puede configurar los siguientes criterios de activación de la regla:

- **Acciones**
- **Valores controlados**
- **Usuarios de confianza**

Acciones

Cuando se inicia la tarea Monitor de acceso a registros, Kaspersky Embedded Systems Security para Windows utiliza una lista de acciones para supervisar el registro (ver la tabla a continuación).

Si se detecta una acción especificada como criterio de activación de la regla, la aplicación registra un evento al respecto.

El nivel de importancia de los eventos registrados no depende de las acciones seleccionadas o del número de eventos.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera todas las acciones. Puede configurar la lista de acciones manualmente en la configuración de reglas de la tarea.

Acciones

Acción	Restricciones	Sistema

		operativo
Crear clave	• Para Windows XP y Windows Server 2003, si agrega **Acciones** a la lista de **Crear clave** y luego selecciona el modo **Bloquear operaciones según las reglas**, la creación de claves no se bloquea en los sistemas operativos especificados debido a las restricciones del sistema. La clave se crea con una notificación respectiva enviada al registro de eventos. • Si desea prohibir la creación de una clave específica a través del Editor del registro, cree una regla para una clave de registro principal y asegúrese de agregar **Acciones** a la lista de **Crear subclaves**, y luego seleccione el modo **Bloquear operaciones según las reglas**.	Windows XP y versiones posteriores
Eliminar clave	Si desea eliminar una clave principal, asegúrese de borrar las opciones **Eliminar subclaves** y **Acciones** en la lista de **Eliminar clave** supervisadas para una clave de registro configurada, ya que solo puede eliminar la clave principal con subclaves.	Windows XP y versiones posteriores
Renombrar clave	N/D	Windows XP y versiones posteriores
Cambiar configuración de seguridad de claves	N/D	Windows Vista y versiones posteriores
Eliminar valores	N/D	Windows XP y versiones posteriores
Establecer valores	Si agrega **Acciones** a la lista de **Establecer valores**, define el **Valor o máscara de valor** predeterminado en la regla para una clave y luego selecciona el modo **Bloquear operaciones según las reglas**, la clave no se crea porque una clave nueva solo se puede crear con un valor predeterminado.	Windows XP y versiones posteriores
Crear subclaves	N/D	Windows XP y versiones posteriores
Eliminar subclaves	N/D	Windows XP y versiones posteriores
Renombrar subclaves	N/D	Windows XP y versiones posteriores
Cambiar configuración de seguridad de subclaves	N/D	Windows Vista y versiones posteriores

Valores del registro

Además de la supervisión de las claves de registro, puede bloquear o supervisar los cambios de los valores del registro existentes. Las siguientes opciones están disponibles:

- **Establecer valor**: crea valores del registro nuevos o cambia los valores del registro existentes.
- **Eliminar valor**: elimina los valores del registro existentes.

El cambio de nombre y configuración de seguridad no se aplica a los valores del registro.

Usuarios de confianza

De forma predeterminada, la aplicación trata todas las acciones del usuario como posible violación de la seguridad. La lista de usuarios de confianza está vacía. Puede configurar el nivel de importancia del evento al crear una lista de usuarios de confianza en la configuración de reglas de supervisión del registro de sistemas.

Un *usuario que no es de confianza* es cualquier usuario no indicado en la lista de usuarios de confianza en la configuración de la regla del área de supervisión. Si Kaspersky Embedded Systems Security para Windows detecta una acción que realiza un usuario que no es de confianza, la tarea Monitor de acceso a registros inscribe un Evento crítico en el registro de tareas.

Un *usuario de confianza* es un usuario o grupo de usuarios autorizados para realizar acciones dentro del área de supervisión especificada. Si Kaspersky Embedded Systems Security para Windows detecta una acción que realiza un usuario de confianza, la tarea Monitor de acceso a registros registrará un Evento informativo en el registro de tareas.

Configuración predeterminada de la tarea Monitor de acceso a registros

La configuración predeterminada para la tarea Monitor de acceso al registro se describe en la tabla a continuación. Puede cambiar los valores de la configuración en los siguientes componentes:

- El Complemento de administración
- La Consola de la aplicación
- El Complemento web

Configuración predeterminada de la tarea Monitor de acceso a registros

Configuración	Valor predeterminado	Descripción
Área de supervisión	No definido	Use esta opción para definir las claves y subclaves del registro principal que se supervisará. La configuración es obligatoria. Si no define la configuración, la tarea no se iniciará. Los eventos de supervisión se generan para las claves y subclaves del registro principal en el área de supervisión especificada.
Acciones	Se seleccionan todos los elementos de la lista de acciones	Use esta opción para configurar una lista de acciones pertinentes si selecciona o desmarca las casillas de verificación correspondientes.
Valores del registro	No definido	Use esta opción para agregar, modificar y eliminar los valores del registro que desee supervisar del área de supervisión definida.

Usuarios de confianza	No definido	Puede especificar los usuarios o grupos de usuarios que estarán autorizados a realizar las acciones definidas para las claves del Registro especificadas.
Modo de la tarea.	Solo estadísticas	Puede seleccionar el modo de la tarea para **Bloquear operaciones según las reglas** o puede seleccionar el modo **Solo estadísticas** para recibir las notificaciones.
Programación de inicio de tareas	No definido	Se pueden configurar los ajustes para iniciar la tarea de forma programada.

Administración del Monitor de acceso a registros a través del Complemento de administración

En esta sección, aprenderá a configurar la tarea Monitor de acceso al registro mediante el Complemento de administración.

Configuración de los parámetros de la tarea Monitor de acceso a registros

Para configurar los ajustes de la tarea Monitor de acceso al registro mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Inspección del sistema**, en el bloque **Monitor de acceso al registro**, haga clic en el botón **Configuración**.

   Aparece la ventana **Monitor de acceso al registro**.
5. En la pestaña **Configuración del Monitor de acceso al registro**, en el bloque **Modo de la tarea**, seleccione la opción que precise de las enumeradas:
   - **Bloquear operaciones según las reglas**

     Si selecciona el modo **Bloquear operaciones según las reglas**, Kaspersky Embedded Systems Security para Windows bloquea las **Acciones** definidas para el área de supervisión.

     Por defecto, se aplica el modo **Solo estadísticas**.
   - **Solo estadísticas**.

Si se selecciona el modo **Solo estadísticas** para el área de supervisión, Kaspersky Embedded Systems Security para Windows compila las estadísticas de las acciones de la clave del registro según las reglas configuradas.

Por defecto, se aplica el modo **Solo estadísticas**.

6. Agregue las reglas de monitoreo de acceso al registro que determinarán las acciones de la tarea.
7. En la pestaña **Administración de tareas**, configure la programación de inicio de la tarea.
8. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La información acerca de la fecha y hora de modificación de la configuración se guarda en el registro de auditoría del sistema.

Creación y configuración de una regla de monitoreo de acceso al registro

Las reglas de supervisión de acceso al registro se aplican en el orden en que aparecen en el bloque **Reglas de monitoreo de acceso al registro**.

Para crear y configurar una regla de monitoreo de acceso al registro mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. Realice una de las siguientes opciones:
   - Si va a crear una regla de monitoreo de acceso al registro en una directiva, en la sección **Inspección del sistema**, dentro del bloque **Monitor de acceso al registro**, haga clic en el botón **Configuración**.

     Se abre la pestaña **Configuración del Monitor de acceso al registro** de la ventana **Monitor de acceso al registro**.
   - Si va a crear una regla de monitoreo de acceso al registro para una tarea local, en la ventana **Propiedades: Monitor de acceso al registro**, vaya a la sección **Configuración**.
5. En el bloque **Reglas de monitoreo del acceso al registro**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de monitoreo del acceso al registro**.
6. En el campo **Establecer los criterios de activación de reglas para el área especificada**, ingrese una ruta utilizando una de las **máscaras admitidas**.

Puede usar `?` y `*` como una máscara al ingresar una ruta.

Si ingresa la ruta a una clave de registro raíz, asegúrese de especificar la ruta completa sin una máscara, como `HKEY_USERS`. A continuación, se muestra una lista de claves de registro raíz válidas:

- `HKEY_LOCAL_MACHINE`
- `HKLM`
- `HKEY_CURRENT_USER`
- `HKCU`
- `HKEY_USERS`
- `HKUS`
- `HKU`
- `HKEY_CURRENT_CONFIG`
- `HKEY_CLASSES_ROOT`
- `HKCR`

Evite usar máscaras compatibles para las claves de origen al crear las reglas.
Si especifica solo una clave de origen, como HKEY_CURRENT_USER, o una clave de origen con una máscara para todas las claves secundarias, como HKEY_CURRENT_USER*, se genera un gran número de notificaciones acerca de abordar claves secundarias específicas, lo que resulta en fallas en el rendimiento del sistema. Si especifica una clave de origen, como HKEY_CURRENT_USER, o una clave de origen con una máscara para todas las claves secundarias, como HKEY_CURRENT_USER*, y selecciona el modo **Bloquear operaciones según las reglas**, el sistema no puede leer ni cambiar las claves requeridas para el funcionamiento del sistema operativo y no puede responder.

7. En la pestaña **Agregar**, configure la lista de acciones según corresponda.

8. Especifique los valores del registro que supervisará la regla:

   a. En la pestaña **Valores del registro**, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla del valor de los registros**.

   b. En el campo correspondiente, ingrese una máscara de valor del Registro.

   c. En el bloque **Operaciones controladas**, seleccione qué acciones realizadas en el valor del Registro serán supervisadas por la regla.

   d. Haga clic en el botón **Aceptar** para guardar los cambios.

9. Si es necesario, especifique usuarios de confianza:

   a. En la pestaña **Usuarios de confianza**, en el menú contextual del botón **Agregar**, seleccione el método que desee usar para agregar los usuarios de confianza.

Se abre la ventana **Selección de usuario o grupo de usuarios**.

b. Seleccione un usuario o grupo de usuarios que tenga permiso para realizar las acciones seleccionadas.

c. Haga clic en el botón **Aceptar** para guardar los cambios.

De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera que no son de confianza todos aquellos usuarios que no figuran en la lista de usuarios de confianza y genera eventos críticos para ellos. Las estadísticas se compilan para los usuarios de confianza.

10. En la ventana **Regla del Monitor de acceso al registro**, haga clic en el botón **Aceptar**.

La regla configurada para el Monitor de acceso al registro aparecerá en el bloque **Reglas de monitoreo del acceso al registro** de las ventanas **Monitor de acceso al registro** o **Propiedades: Monitor de acceso al registro**.

Exportación e importación de reglas de monitoreo de acceso al registro

Puede exportar a un archivo XML las reglas de monitoreo de acceso al registro que haya creado manualmente en las propiedades de la tarea Monitor de acceso al registro.

Puede importar las reglas de monitoreo de acceso al registro que haya exportado a un archivo XML a las propiedades de la tarea Monitor de acceso al registro.

Para exportar o importar reglas de monitoreo de acceso al registro mediante el Complemento de administración:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.

   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. Realice una de las siguientes opciones:

   - Si desea importar o exportar las reglas de monitoreo de acceso al registro definidas en una directiva, en la sección **Inspección del sistema**, dentro del bloque **Monitor de acceso al registro**, haga clic en el botón **Configuración**.

     Se abre la pestaña **Configuración del Monitor de acceso al registro** de la ventana **Monitor de acceso al registro**.

   - Si desea importar o exportar las reglas de monitoreo de acceso al registro definidas en una tarea local, en la ventana **Propiedades: Monitor de acceso al registro**, vaya a la sección **Configuración**.

5. Exporte o importe las reglas de monitoreo de acceso al registro:

   - **Cómo exportar reglas de monitoreo de acceso al registro**

1. En el bloque **Reglas de monitoreo del acceso al registro**, haga clic en el botón **Exportar**.

   Se abre la ventana **Guardar como** estándar de Microsoft Windows.

2. Indique la ruta en la que desea guardar el archivo XML con la configuración de las reglas de monitoreo de acceso al registro.

3. Ingrese el nombre del archivo en el campo correspondiente.

4. Haga clic en el botón **Guardar**.

   La aplicación guardará un archivo XML con la configuración de las reglas de monitoreo de acceso al registro en la ruta especificada.

- Cómo importar reglas de monitoreo de acceso al registro

1. En el bloque **Reglas de monitoreo del acceso al registro**, haga clic en el botón **Importar**.

2. En el menú contextual del botón **Importar**, seleccione uno de los valores posibles:

   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes.

     Si el nombre de la rama del Registro de la regla importada coincide con el nombre de la rama del Registro de una regla existente, la regla importada no se agregará aun cuando las reglas no contengan los mismos valores de configuración para esa rama.

   - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.

   - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

   Se abre la ventana estándar **Abrir** de Microsoft Windows.

3. Indique la ruta al archivo XML con la configuración de las reglas de supervisión de acceso al registro.

4. Haga clic en el botón **Abrir**.

   Las reglas importadas se mostrarán en la sección **Reglas de monitoreo del acceso al registro** de las ventanas **Monitor de acceso al registro** o **Propiedades: Monitor de acceso al registro**.

6. Haga clic en el botón **Guardar** para guardar los cambios.

Administración de la tarea Monitor de acceso al registro mediante la Consola de administración

En esta sección, aprenderá a configurar la tarea Monitor de acceso a registros mediante la Consola de la aplicación.

Configuración de los ajustes generales de la tarea Monitor de acceso al registro

Para configurar los ajustes generales de la tarea Monitor de acceso al registro mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de acceso al registro**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Monitor de acceso al registro**.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. En el grupo **Modo de la tarea**, seleccione la opción requerida de la lista:

   - **Bloquear operaciones según las reglas**

     Si selecciona el modo **Bloquear operaciones según las reglas**, Kaspersky Embedded Systems Security para Windows bloquea las **Acciones** definidas para el área de supervisión.

     Por defecto, se aplica el modo **Solo estadísticas**.

   - **Solo estadísticas**.

     Si se selecciona el modo **Solo estadísticas** para el área de supervisión, Kaspersky Embedded Systems Security para Windows compila las estadísticas de las acciones de la clave del registro según las reglas configuradas.

     Por defecto, se aplica el modo **Solo estadísticas**.
5. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas.
6. Haga clic en el botón **Aceptar** para guardar los cambios.

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La información acerca de la fecha y hora de modificación de la configuración se guarda en el registro de auditoría del sistema.

Creación y configuración de una regla de monitoreo de acceso al registro

Las reglas de supervisión de acceso al registro se aplican en el orden en que aparecen en el bloque **Reglas de monitoreo de acceso al registro**.

Para crear y configurar una regla de monitoreo de acceso al registro mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de acceso al registro**.

3. Haga clic en el vínculo **Monitor de acceso al registro** en el panel de resultados del nodo **Reglas del Monitor de acceso al registro**.

   Aparece la ventana **Monitor de acceso al registro**.

4. En el campo **Agregar clave del registro del sistema al monitor**, ingrese la ruta a la clave del registro utilizando una de las máscaras compatibles.

   Evite el uso de máscaras compatibles para las claves raíz al crear las reglas.
   Si especifica solo una clave raíz, como HKEY_CURRENT_USER, o una clave raíz con una máscara para todas las claves secundarias, como HKEY_CURRENT_USER*, se genera una gran cantidad de notificaciones sobre cómo abordar las claves secundarias especificadas, lo que resulta en fallas en el rendimiento del sistema.
   Si especifica una clave raíz, como HKEY_CURRENT_USER, o una clave raíz con una máscara para todas las claves secundarias, como HKEY_CURRENT_USER*, y selecciona el modo **Bloquear operaciones según las reglas**, el sistema no puede leer ni cambiar las claves necesarias para el funcionamiento del sistema operativo y no responde.

5. Haga clic en el botón **Agregar**.

6. En la pestaña **Acciones** correspondiente al área de supervisión seleccionada, configure la lista de acciones según corresponda.

7. Especifique los valores del registro que supervisará la regla:

   a. En la pestaña **Valores controlados**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla del valor de los registros**.

   b. En el campo correspondiente, ingrese el valor del registro o la máscara del valor del registro.

   c. En el bloque **Operaciones controladas**, seleccione qué acciones realizadas en el valor del Registro serán supervisadas por la regla.

   d. Haga clic en el botón **Aceptar** para guardar los cambios.

8. Si es necesario, especifique usuarios de confianza:

   a. En la pestaña **Usuarios de confianza**, haga clic en el botón **Agregar**.

   b. En la ventana **Seleccionar usuarios o grupos**, seleccione los usuarios o grupos de usuarios autorizados a realizar las acciones seleccionadas.

   c. Haga clic en el botón **Aceptar** para guardar los cambios.

   De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera que no son de confianza todos aquellos usuarios que no figuran en la lista de usuarios de confianza y genera eventos críticos para ellos. Las estadísticas se compilan para los usuarios de confianza.

9. En la ventana **Monitor de acceso al registro**, haga clic en el botón **Guardar**.

La regla de supervisión de acceso al registro configurada aparecerá en el bloque **Monitor de acceso al registro** de la ventana **Reglas de monitoreo de acceso al registro**.

Exportación e importación de reglas de monitoreo de acceso al registro

Puede exportar a un archivo XML las reglas de monitoreo de acceso al registro que haya creado manualmente en las propiedades de la tarea Monitor de acceso al registro.

Puede importar las reglas de monitoreo de acceso al registro que haya exportado a un archivo XML a las propiedades de la tarea Monitor de acceso al registro.

Para exportar e importar reglas de monitoreo de acceso al registro mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de acceso al registro**.
3. Haga clic en el vínculo **Monitor de acceso al registro** en el panel de resultados del nodo **Reglas del Monitor de acceso al registro**.

   Aparece la ventana **Monitor de acceso al registro**.
4. Cómo exportar reglas de monitoreo de acceso al registro.

   1. En el bloque **Reglas de monitoreo de acceso al registro**, haga clic en el botón **Exportar a un archivo** para exportar las reglas de monitoreo de acceso al registro.

      Se abre la ventana **Guardar como** estándar de Microsoft Windows.
   2. Indique la ruta en la que desea guardar el archivo XML con la configuración de las reglas de monitoreo de acceso al registro.
   3. Ingrese el nombre del archivo en el campo correspondiente.
   4. Haga clic en el botón **Guardar**.

      La aplicación guardará un archivo XML con la configuración de las reglas de monitoreo de acceso al registro en la ruta especificada.
5. Cómo importar reglas de monitoreo de acceso al registro.

1. En el bloque **Reglas de monitoreo de acceso al registro**, haga clic en el botón **Importar**.
2. En el menú contextual del botón **Importar**, seleccione uno de los valores posibles:
   - **Combinar con reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes.

     Si el nombre de la rama del Registro de la regla importada coincide con el nombre de la rama del Registro de una regla existente, la regla importada no se agregará aun cuando las reglas no contengan los mismos valores de configuración para esa rama.

   - **Agregar a reglas existentes**, si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes**, si desea reemplazar las reglas existentes con las reglas importadas.

   Se abre la ventana estándar **Abrir** de Microsoft Windows.
3. Indique la ruta al archivo XML con la configuración de las reglas de supervisión de acceso al registro.
4. Haga clic en el botón **Abrir**.

   Las reglas importadas se mostrarán en el bloque **Monitor de acceso al registro** de la ventana **Reglas de monitoreo de acceso al registro**.

6. Haga clic en el botón **Guardar** para guardar los cambios.

Administración del Monitor de acceso a registros a través del Complemento web

En esta sección, aprenderá a configurar la tarea Monitor de acceso a registros mediante el Complemento web.

Configuración de los parámetros de la tarea Monitor de acceso a registros

Para configurar la tarea Monitor de acceso a registros a través del Complemento web, realice lo siguiente:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Inspección del sistema**.
5. En la subsección **Monitor de acceso al registro**, haga clic en el botón **Configuración**.

Se abre la pestaña **Configuración del Monitor de acceso al registro** de la ventana **Monitor de acceso al registro**.

6. En el grupo **Modo de la tarea**, seleccione la opción requerida de la lista:

   - **Bloquear operaciones según las reglas**

     Si selecciona el modo **Bloquear operaciones según las reglas**, Kaspersky Embedded Systems Security para Windows bloquea las **Acciones** definidas para el área de supervisión.

     Por defecto, se aplica el modo **Solo estadísticas**.

   - **Solo estadísticas**

     Si se selecciona el modo **Solo estadísticas** para el área de supervisión, Kaspersky Embedded Systems Security para Windows compila las estadísticas de las acciones de la clave del registro según las reglas configuradas.

     Por defecto, se aplica el modo **Solo estadísticas**.

7. Agregue las reglas de monitoreo de acceso al registro que determinarán las acciones de la tarea.

8. En la pestaña **Administración de tareas**, configure la programación de inicio de tareas.

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

Kaspersky Embedded Systems Security para Windows aplicará los nuevos valores de configuración a la tarea en ejecución. La información acerca de la fecha y hora de modificación de la configuración se guarda en el registro de auditoría del sistema.

Creación y configuración de una regla de monitoreo de acceso al registro

Las reglas de supervisión de acceso al registro se aplican en el orden en que aparecen en el bloque **Reglas de monitoreo de acceso al registro**.

Para crear y configurar una regla de monitoreo de acceso al registro mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos → Directivas y perfiles**.

2. Haga clic en el nombre de la directiva que desea configurar.

3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione la sección **Inspección del sistema**.

5. En la subsección **Monitor de acceso al registro**, haga clic en el botón **Configuración**.

   Se abre la pestaña **Configuración del Monitor de acceso al registro** de la ventana **Monitor de acceso al registro**.

6. En el bloque **Reglas del Monitor de acceso al registro**, haga clic en el botón **Agregar**.

Se abre la ventana **Regla del Monitor de acceso al registro**.

7. En el campo **Supervisar acceso al registro para un área**, ingrese una ruta utilizando una de las **máscaras admitidas**.

   Puede usar `?` y `*` como una máscara al ingresar una ruta.

   Si ingresa la ruta a una clave de registro raíz, asegúrese de especificar la ruta completa sin una máscara, como `HKEY_USERS`. A continuación, se muestra una lista de claves de registro raíz válidas:

   - `HKEY_LOCAL_MACHINE`
   - `HKLM`
   - `HKEY_CURRENT_USER`
   - `HKCU`
   - `HKEY_USERS`
   - `HKUS`
   - `HKU`
   - `HKEY_CURRENT_CONFIG`
   - `HKEY_CLASSES_ROOT`
   - `HKCR`

   Evite el uso de máscaras compatibles para las claves raíz al crear las reglas.
   Si especifica solo una clave raíz, como HKEY_CURRENT_USER, o una clave raíz con una máscara para todas las claves secundarias, como HKEY_CURRENT_USER*, se genera una gran cantidad de notificaciones sobre cómo abordar las claves secundarias especificadas, lo que resulta en fallas en el rendimiento del sistema.
   Si especifica una clave raíz, como HKEY_CURRENT_USER, o una clave raíz con una máscara para todas las claves secundarias, como HKEY_CURRENT_USER*, y selecciona el modo **Bloquear operaciones según las reglas**, el sistema no puede leer ni cambiar las claves necesarias para el funcionamiento del sistema operativo y no responde.

8. En la pestaña **Acciones** correspondiente al área de supervisión seleccionada, configure la lista de acciones según corresponda.

9. Especifique los valores del registro que supervisará la regla:

   a. En la pestaña **Valores controlados**, haga clic en el botón **Agregar**.

      Se abre la ventana **Regla del valor de los registros**.

   b. En el campo correspondiente, ingrese una máscara de valor del Registro.

   c. En el bloque **Operaciones controladas**, seleccione qué acciones realizadas con el valor del Registro serán supervisadas por la regla.

d. Haga clic en el botón **Aceptar** para guardar los cambios.

10. Si es necesario, especifique usuarios de confianza:

    a. En la pestaña **Usuarios de confianza**, haga clic en el botón **Agregar**.

    b. Ingrese el **Nombre de usuario** o haga clic en **Establecer el SID el grupo Everyone** para definir los usuarios autorizados que realizarán las acciones seleccionadas.

    c. Haga clic en el botón **Aceptar** para guardar los cambios.

    De forma predeterminada, Kaspersky Embedded Systems Security para Windows considera que no son de confianza todos aquellos usuarios que no figuran en la lista de usuarios de confianza y genera eventos críticos para ellos. Las estadísticas se compilan para los usuarios de confianza.

11. En la ventana **Regla del Monitor de acceso al registro**, haga clic en el botón **Aceptar** para guardar los cambios.

La regla de supervisión de acceso al registro configurada aparecerá en el bloque **Monitor de acceso al registro** de la ventana **Reglas del Monitor de acceso al registro**.

Exportación e importación de reglas de monitoreo de acceso al registro

Puede exportar a un archivo XML las reglas de monitoreo de acceso al registro que haya creado manualmente en las propiedades de la tarea Monitor de acceso al registro.

Puede importar las reglas de monitoreo de acceso al registro que haya exportado a un archivo XML a las propiedades de la tarea Monitor de acceso al registro.

Para exportar o importar reglas de monitoreo de acceso al registro mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Inspección del sistema**.
5. En el bloque **Monitor de acceso al registro**, haga clic en el botón **Configuración**.

   Se abre la pestaña **Configuración del Monitor de acceso al registro** de la ventana **Monitor de acceso al registro**.
6. Exporte o importe las reglas de monitoreo de acceso al registro:

   - Cómo exportar reglas de monitoreo de acceso al registro

     En el bloque **Reglas del Monitor de acceso al registro**, haga clic en el botón **Exportar**.

     La aplicación guardará el archivo RegistryMonitor.xml, que contendrá la configuración de las reglas de monitoreo de acceso al registro, en la carpeta C:\Usuarios\<Nombre de usuario>\Descargas.

- Cómo importar reglas de monitoreo de acceso al registro.

  1. En el bloque **Reglas del Monitor de acceso al registro**, haga clic en el botón **Importar**.
  2. Haga clic en el botón **Importar**.

     Se abre la ventana estándar **Abrir** de Microsoft Windows.
  3. Indique la ruta al archivo XML con la configuración de las reglas de supervisión de acceso al registro.
  4. Haga clic en el botón **Abrir**.

     Las reglas importadas mediante la combinación de las listas de reglas se mostrarán en el bloque **Monitor de acceso al registro** de la ventana **Reglas del Monitor de acceso al registro**.

     Si el nombre de la rama del Registro de la regla importada coincide con el nombre de la rama del Registro de una regla existente, la regla importada no se agregará aun cuando las reglas no contengan los mismos valores de configuración para esa rama.

7. Haga clic en el botón **Guardar** para guardar los cambios.

Inspección de registros

Esta sección contiene la información sobre la tarea Inspección de registros y los parámetros de la tarea.

Acerca de la tarea Inspección de registros

Cuando la tarea Inspección de registros se ejecuta, Kaspersky Embedded Systems Security para Windows supervisa la integridad del entorno protegido según los resultados de una inspección de registros de eventos de Windows. La aplicación notifica al administrador cuando se detecta un comportamiento anormal que puede indicar un intento de ciberataque.

Kaspersky Embedded Systems Security para Windows analiza los registros de eventos de Windows e identifica las violaciones según las reglas especificadas por el usuario o por la configuración del analizador heurístico, que la tarea utiliza para inspeccionar registros.

Reglas predefinidas y análisis heurístico

Puede usar la tarea Inspección de registros para supervisar el estado del sistema protegido aplicando las reglas predefinidas que se basan en la heurística existente. El Analizador heurístico identifica la actividad anormal en el dispositivo protegido, que pueden ser pruebas de intentos de ataque. Las plantillas para identificar el comportamiento anormal se incluyen en las reglas disponibles, en la configuración de reglas predefinidas.

Se incluyen siete reglas en la lista de reglas para la tarea Inspección de registros. Puede habilitar o deshabilitar cualquiera de estas reglas. No puede eliminar las reglas existentes ni crear reglas nuevas.

Puede configurar los criterios de activación para las reglas que supervisan eventos para las siguientes operaciones:

- Detección de la fuerza bruta de la contraseña
- Detección del inicio de sesión de la red

También puede configurar exclusiones en la configuración de la tarea. El Analizador heurístico no se activa cuando un inicio de sesión es realizado por un usuario de confianza o desde una dirección IP de confianza.

Kaspersky Embedded Systems Security para Windows no usa los parámetros heurísticos para inspeccionar registros de Windows si el analizador heurístico no es usado por la tarea. De forma predeterminada, el Analizador heurístico está habilitado.

Cuando se aplican las reglas, la aplicación registra un *Evento crítico* en el registro de tareas de Inspección de registros.

Reglas personalizadas para la tarea de Inspección de registros

Puede usar la configuración de la regla para especificar y cambiar los criterios para desencadenar reglas al detectar los eventos seleccionados en el registro de Windows especificado. De manera predeterminada, la lista de reglas de Inspección de registros tiene cuatro reglas. Puede habilitar y deshabilitar estas reglas, eliminar reglas y modificar la configuración de la regla.

Puede configurar los siguientes criterios de activación de la regla en cada regla:

- Lista de identificadores de registro en Registro de Eventos de Windows.

  La regla se desencadena cuando un registro nuevo se crea en el Registro de Eventos de Windows, si las propiedades del evento incluyen un identificador del evento especificado en la regla. También puede agregar y eliminar identificadores para cada regla especificada.

- Origen del evento.

  Para cada regla, puede especificar un registro dentro del Registro de Eventos de Windows. La aplicación buscará registros con los identificadores del evento especificados solo en este registro. Puede seleccionar uno de los registros estándar (Aplicación, Seguridad o Sistema) o especificar un registro personalizado ingresando el nombre en el campo Selección de origen.

  > La aplicación no verifica que el registro especificado realmente exista en el Registro de Eventos de Windows.

Cuando la regla se desencadena, Kaspersky Embedded Systems Security para Windows registra un Evento crítico en el registro de tareas de Inspección de registros.

De manera predeterminada, la tarea Inspección de registros aplica reglas personalizadas.

> Antes de iniciar la tarea Inspección de registros, asegúrese de que la directiva de auditoría del sistema esté configurada correctamente. Consulte el artículo de Microsoft para obtener detalles.

Configuración predeterminada de la tarea de inspección de registros

De forma predeterminada, la tarea de Inspección de registros tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Configuración predeterminada de la tarea de inspección de registros

Configuración	Valor predeterminado	Descripción
Aplicar reglas personalizadas para la inspección de registros	No aplicado.	Puede habilitar, deshabilitar, agregar o modificar las reglas personalizadas.
Aplicar reglas predefinidas para la inspección de registros	Aplicado.	Puede habilitar o deshabilitar el analizador heurístico que detecta actividad anormal en el dispositivo protegido.
Detección de ataques de fuerza bruta	10 errores de inicio de sesión por 300 segundos.	Puede establecer el número de intentos y período utilizados que el analizador heurístico considerará como desencadenadores.
Inicio de sesión en la red	12:00:00 a. m.	Puede indicar el inicio y el final del intervalo de tiempo durante el cual los intentos de inicio de sesión en Kaspersky Embedded Systems Security para Windows se consideraron como amenazas y como actividad anormal.

Exclusiones	No aplicado.	Puede especificar los usuarios y direcciones IP que no activarán el analizador heurístico.
Programación de inicio de tareas	La primera ejecución no está programada.	Puede configurar las opciones para iniciar la tarea en base a una programación.

Gestión de reglas de inspección de registros a través del Complemento de administración

En esta sección, aprenda cómo agregar y configurar las reglas de Inspección de registros a través del Complemento de administración.

Configuración de reglas de tareas predefinidas

Realice las siguientes acciones para configurar las reglas predefinidas para la tarea Inspección de registros:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.
4. En la sección **Inspección del sistema**, haga clic en el botón **Inspección de registros** en la subsección **Configuración**.

   Se abrirá la ventana **Inspección de registros**.
5. Seleccione la pestaña **Reglas predefinidas**.
6. Seleccione o desactive la casilla **Aplicar reglas predefinidas para la inspección de registros**.

   Para que la tarea se ejecute, debe seleccionarse al menos una regla de inspección de registros.
7. Seleccione las reglas que desea aplicar en la lista de reglas predefinidas:
   - Hay patrones de posibles ataques de fuerza bruta en el sistema.
   - Hay patrones de un posible abuso del registro de eventos de Windows.
   - Se detectaron acciones atípicas en nombre de un nuevo servicio instalado.

- Se detectó un inicio de sesión atípico en el que se usaron credenciales explícitas.
- Hay patrones de un posible ataque PAC (MS14-068) forzado de Kerberos.
- Se detectaron acciones atípicas dirigidas a un grupo integrado y privilegiado de administradores.
- Se detectó una actividad atípica durante un inicio de sesión en la red.

8. Para configurar las reglas seleccionadas, haga clic en el botón **Configuración avanzada**.

   Se abrirá la ventana **Inspección de registros**.

9. En la sección **Detección de ataques de fuerza bruta**, establezca el número de intentos y período utilizados como desencadenadores por el analizador heurístico.

10. En la sección **Detección de inicio de sesión en la red**, establezca el comienzo y el final del intervalo de tiempo. Kaspersky Embedded Systems Security para Windows considerará como actividad anómala los intentos de inicio de sesión que ocurran durante ese intervalo.

11. Seleccione la pestaña **Exclusiones**.

12. Realice las siguientes acciones para agregar a usuarios de confianza:

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

    b. Seleccione a un usuario.

    c. Haga clic en el botón **Aceptar**.

    El usuario seleccionado se añade a la lista de usuarios de confianza.

13. Realice las siguientes acciones para agregar direcciones IP de confianza:

    a. Escriba la dirección IP.

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

14. La dirección IP indicada se añade a la lista de direcciones IP de confianza.

15. En la pestaña **Administración de tareas**, configure la programación de inicio de tareas.

16. Haga clic en el botón **Aceptar** de la ventana **Inspección de registros**.

La configuración de la tarea Inspección de registros se guardó.

Cómo agregar reglas de Inspección de registros a través del Complemento de administración

Realice las siguientes acciones para agregar y configurar una nueva regla de inspección de registros personalizada:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de dispositivos protegidos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>**.
   - Para configurar los ajustes de una tarea o aplicación para un dispositivo protegido específico, seleccione la pestaña **Dispositivos** y vaya a los ajustes de las tareas locales o a los ajustes de la aplicación.

4. En la sección **Inspección del sistema**, haga clic en el botón **Inspección de registros** en la subsección **Configuración**.

   Se abrirá la ventana **Inspección de registros**.

5. En la pestaña **Reglas personalizadas**, seleccione o desmarque la casilla de verificación **Aplicar reglas personalizadas para la inspección de registros**.

   Puede controlar si las reglas predeterminadas se aplican para la Inspección de registros. Seleccione las casillas correspondientes a las reglas desea aplicar a la Inspección de registros.

6. Para agregar una nueva regla personalizada, haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de inspección de registros personalizada**.

7. En la sección **General**, especifique la siguiente información sobre la regla nueva:

   - **Nombre de la regla**
   - **La regla se activa cuando aparecen nuevas entradas en el registro de eventos de Windows si el identificador (ID) especificado se encuentra en los parámetros del evento**

8. En la sección **Criterios de activación**, especifique los Id. de los eventos que activarán la regla:

   a. Ingrese un Id.

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

      El Id. de la regla ingresado se añade a la lista. Puede agregar un número ilimitado de identificadores a cada regla.

9. Haga clic en el botón **Aceptar**.

   La regla de Inspección de registros se añade a la lista de reglas.

Gestión de reglas de Inspección de registros a través de la Consola de la aplicación

En esta sección, aprenda cómo agregar y configurar reglas de Inspección de registros a través de la Consola de la aplicación.

Configuración de reglas de tareas predefinidas

Realice las siguientes acciones para configurar el analizador heurístico para la tarea Inspección de registros:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Inspección de registros**.
3. Haga clic en el vínculo **Inspección de registros** en el panel de resultados del nodo **Propiedades**.
   Aparece la ventana **Configuración de tareas**.
4. Seleccione la pestaña **Reglas predefinidas**.
5. Seleccione o desactive la casilla **Aplicar reglas predefinidas para la inspección de registros**.

   Para que la tarea se ejecute, debe seleccionarse al menos una regla de inspección de registros.

6. Seleccione las reglas que desea aplicar en la lista de reglas predefinidas:
   - Hay patrones de posibles ataques de fuerza bruta en el sistema.
   - Hay patrones de un posible abuso del registro de eventos de Windows.
   - Se detectaron acciones atípicas en nombre de un nuevo servicio instalado.
   - Se detectó un inicio de sesión atípico en el que se usaron credenciales explícitas.
   - Hay patrones de un posible ataque PAC (MS14-068) forzado de Kerberos.
   - Se detectaron acciones atípicas dirigidas a un grupo integrado y privilegiado de administradores.
   - Se detectó una actividad atípica durante un inicio de sesión en la red.
7. Para configurar las reglas seleccionadas, vaya a la pestaña **Extendido**.
8. En la sección **Detección de ataques de fuerza bruta**, establezca el número de intentos y período utilizados como desencadenadores por el analizador heurístico.
9. En la sección **Inicio de sesión en la red**, establezca el comienzo y el final del intervalo de tiempo. Kaspersky Embedded Systems Security para Windows considerará como actividad anómala los intentos de inicio de sesión que ocurran durante ese intervalo.
10. Seleccione la pestaña **Exclusiones**.
11. Realice las siguientes acciones para agregar a usuarios de confianza:
    a. Haga clic en el botón **Examinar**.
    b. Seleccione a un usuario.
    c. Haga clic en el botón **Aceptar**.
       El usuario seleccionado se añade a la lista de usuarios de confianza.
12. Realice las siguientes acciones para agregar direcciones IP de confianza:
    a. Escriba la dirección IP.
    b. Haga clic en el botón **Agregar**.

La dirección IP indicada se añade a la lista de direcciones IP de confianza.

13. Seleccione las pestañas **Programación**Avanzadoy **Avanzado** para configurar la programación de inicio de tareas.

14. Haga clic en el botón **Aceptar** en la ventana **Configuración de tareas**.

    La configuración de la tarea Inspección de registros se guardó.

Cómo agregar reglas de Inspección de registros a través de la Consola de la aplicación

Para agregar y configurar una nueva regla de inspección de registros personalizada:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Inspección de registros**.
3. En el panel de resultados del nodo **Inspección de registros**, haga clic en el vínculo **Reglas de inspección de registros**.
4. Se abre la ventana **Reglas de inspección de registros**.
5. Desactive o seleccione la casilla **Aplicar reglas personalizadas para la inspección de registros. Las reglas configuradas no se aplicarán hasta que se seleccione la casilla de verificación**. La suma de control se muestra en el registro de tareas.

   Puede controlar si las reglas predefinidas se aplican a la tarea Inspección de registros. Seleccione las casillas correspondientes a las reglas desea aplicar a la Inspección de registros.

6. Para crear una nueva regla personalizada:

   a. Introduzca el nombre de la nueva regla.

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

      La regla creada se agrega a la lista de reglas generales.

7. Para configurar cualquier regla, realice lo siguiente:

   a. Seleccione una regla de la lista.

      En el lado derecho de la ventana, la pestaña **Descripción** muestra información general sobre la regla.

      La descripción de la nueva regla está en blanco.

   b. Seleccione la pestaña **Configuración de la regla**.

8. En la sección **General**, especifique la siguiente información sobre la regla nueva:

   - **Nombre de la regla**

- **Nombre del registro**
- **La regla se activa cuando aparecen nuevas entradas en el registro de eventos de Windows si el identificador (ID) especificado se encuentra en los parámetros del evento**

9. En la sección **Identificadores de eventos**, especifique los Id. del evento que desencadenarán la regla:

   a. Ingrese un Id. del evento.

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

   El Id. de la regla ingresado se añade a la lista. Puede agregar un número ilimitado de identificadores a cada regla.

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

Las reglas de inspección de registros configuradas se aplicarán.

Administración de reglas de inspección de registros a través del Complemento web

Para agregar y configurar reglas de Inspección de registros a través del Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Inspección del sistema**.
5. Haga clic en el botón **Configuración** en la subsección **Inspección de registros**.
6. Configure las opciones que se describen en la tabla a continuación.

Configuración de la tarea Inspección de registros

Configuración	Descripción
Aplicar reglas personalizadas para la inspección de registros	Puede habilitar, deshabilitar, agregar o modificar las reglas personalizadas. La configuración está disponible en la tabla con la lista de reglas personalizadas.
Aplicar reglas predefinidas para la inspección de registros	Puede habilitar o deshabilitar el analizador heurístico que detecta actividad anormal en el dispositivo protegido. La configuración está disponible en la tabla con la lista de reglas personalizadas.
Detectar ataques de fuerza bruta si se ingresa una contraseña incorrecta con una frecuencia definida	Puede establecer el número de intentos y período utilizados que el analizador heurístico considerará como desencadenadores.
Detectar inicio de sesión en la red, si se inicia sesión dentro	Puede indicar el inicio y el final del intervalo de tiempo durante el cual los intentos de inicio de sesión en Kaspersky Embedded Systems

de un determinado período	Security para Windows se consideraron como amenazas y como actividad anormal.
Exclusiones de usuarios	Puede especificar los usuarios que no activarán el analizador heurístico.
Direcciones IP excluidas	Puede especificar las direcciones IP que no activarán el analizador heurístico.
Administración de tareas	Puede configurar las opciones para iniciar la tarea en base a una programación.

Análisis a pedido

Esta sección proporciona la información sobre las tareas de Análisis a pedido e instrucciones de la configuración de los ajustes de la tarea Análisis a pedido y ajustes de seguridad en el dispositivo protegido.

Acerca de las tareas de Análisis a pedido

Kaspersky Embedded Systems Security para Windows analiza la zona especificada en busca de virus y otras amenazas de seguridad informática. Kaspersky Embedded Systems Security para Windows analiza archivos de dispositivos protegidos, RAM y objetos de ejecución automática.

Kaspersky Embedded Systems Security para Windows proporciona las siguientes tareas de Análisis a pedido:

- La tarea Análisis al inicio del sistema operativo se realiza cada vez que se inicia Kaspersky Embedded Systems Security para Windows. La aplicación analiza los sectores de arranque y los registros de inicio maestros de los discos duros, las unidades extraíbles, la memoria del sistema y la memoria de los procesos. Cada vez que Kaspersky Embedded Systems Security para Windows ejecuta la tarea, crea una copia de los sectores de inicio no infectados. Si detecta una amenaza en esos sectores la próxima vez que se inicia la tarea, los reemplaza con la copia de seguridad.

  La tarea Análisis al inicio del sistema operativo se crea automáticamente después de la instalación. De manera predeterminada, se aplica el modo Solo notificar. En este caso, después de implementar Kaspersky Embedded Systems Security en los dispositivos, puede habilitar la tarea Análisis al inicio del sistema operativo si no se descubrieron problemas con los servicios del sistema durante el análisis. Si la aplicación detecta servicios críticos del sistema como objetos infectados o probablemente infectados, el modo Solo notificar le da tiempo para averiguar el motivo y resolver el problema. Si Kaspersky Embedded Systems Security para Windows aplica el modo Realizar la acción recomendada, se realizará la acción Desinfectar. Pueden ocurrir problemas graves en el inicio del sistema operativo si se desinfectan o eliminan archivos del sistema operativo como parte de la acción Eliminar si falla la desinfección.

  > Es posible que la tarea de Análisis al inicio del sistema operativo no se realice si un dispositivo protegido se activa después del modo de suspensión o hibernación. La tarea se realiza solo al reiniciar el dispositivo protegido o al inicio después del apagado completo.

- De forma predeterminada, la tarea de Análisis de áreas críticas se realiza cada semana según una programación. Kaspersky Embedded Systems Security para Windows analiza los objetos ubicados en las áreas críticas del sistema operativo: objetos de ejecución automática, sectores de inicio y registros de inicio maestro de discos duros y unidades extraíbles, memoria del sistema y memoria del proceso. La aplicación analiza archivos en las carpetas del sistema, por ejemplo, %windir%\system32. Kaspersky Embedded Systems Security para Windows aplica la configuración de seguridad que corresponde al Nivel recomendado. Puede modificar la configuración de la tarea de Análisis de áreas críticas.

- La tarea Análisis de archivos en cuarentena se ejecuta de manera predeterminada según una programación después de cada actualización de bases de datos. El alcance la tarea de Análisis de archivos en cuarentena no se puede modificar.

- La tarea Control de integridad de la aplicación se realiza a diario. Proporciona la opción de comprobar módulos de Kaspersky Embedded Systems Security para Windows en busca de daños o modificaciones. Se comprueba la carpeta de instalación de la aplicación. Las estadísticas de ejecución de tareas indican el número de módulos comprobados y el número de módulos dañados. Los valores de la configuración de tarea están definidos de forma predeterminada y no se pueden modificar. La configuración de la programación de inicio de tareas se puede modificar.

Además, puede crear tareas de Análisis a pedido personalizadas, por ejemplo, una tarea para analizar las carpetas compartidas en el dispositivo protegido.

Kaspersky Embedded Systems Security para Windows puede ejecutar varias tareas de Análisis a pedido de manera simultánea.

Acerca del área del análisis de la tarea y la configuración de seguridad

En la Consola de la aplicación, el área de análisis de la tarea Análisis a pedido seleccionada se muestra en forma de árbol o en la lista de recursos de archivos del dispositivo protegido que Kaspersky Embedded Systems Security para Windows puede controlar. De forma predeterminada, los recursos de archivos en red del dispositivo protegido se muestran en un modo de vista de lista.

En el Complemento de administración, solo está disponible la vista de la lista.

Para ver recursos de archivos en red en el modo de vista de árbol en la Consola de la aplicación,

abra la lista desplegable en el sector izquierdo superior de la ventana **Configuración del área de análisis** y seleccione **Vista de árbol**.

Los elementos o nodos se muestran en una visualización en forma de lista o en un modo de visualización en forma de árbol de los recursos del archivo del dispositivo protegido de la siguiente manera:

☑ El nodo se incluye en el alcance del análisis.

☐ El nodo se excluye del área del análisis.

☑ Al menos uno de los nodos secundarios de este nodo se excluye del área del análisis, o la configuración de seguridad de los nodos secundarios difiere de la de un nodo principal (solo para el modo de visualización de vista de árbol).

El icono ☑ se muestra si están seleccionados todos los nodos secundarios, pero no el principal. En este caso, los cambios en la composición de los archivos y las carpetas del nodo principal se ignoran automáticamente cuando se está modificando el área del análisis para el subnodo creado.

Si utiliza la Consola de la aplicación, también puede agregar unidades virtuales al alcance del análisis. Los nombres de los nodos virtuales se muestran en letras azules.

Configuración de seguridad

En la tarea de Análisis a pedido seleccionada, la configuración de seguridad predeterminada puede modificarse si se la establece como configuración común para toda el área de protección o de análisis, o como una configuración diferente para los distintos nodos o elementos de la lista o el árbol de recursos de archivos del dispositivo.

La configuración de seguridad para el nodo principal seleccionado se aplica automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

La configuración de un área del análisis o área de protección seleccionada se puede realizar mediante uno de los métodos siguientes:

- Seleccione uno de los tres niveles de seguridad predefinidos (**Máximo rendimiento**, **Recomendado** o **Máxima protección**).
- Cambie manualmente la configuración de seguridad para los nodos o elementos seleccionados en el árbol o lista de los recursos de archivos del dispositivo protegido (el nivel de seguridad cambia a **Personalizado**).

Es posible guardar un conjunto de opciones de configuración de seguridad en una plantilla a fin de aplicarlo más tarde a otros nodos.

Áreas del análisis predefinidas

El árbol o la lista de recursos del archivo del dispositivo protegido para la tarea de Análisis a pedido seleccionada se muestran en la ventana **Configuración del área de análisis**.

El árbol o la lista de recursos de archivos muestran los nodos a los cuales tiene acceso de lectura según las opciones de seguridad configuradas de Microsoft Windows.

Kaspersky Embedded Systems Security para Windows contiene las áreas del análisis predefinidas siguientes:

- **Mi equipo**. Kaspersky Embedded Systems Security para Windows analiza todo el dispositivo protegido.
- **Discos duros locales**. Kaspersky Embedded Systems Security para Windows analiza objetos en los discos duros del dispositivo protegido. Todos los discos duros, discos, carpetas o archivos individuales se pueden incluir en el área del análisis o excluir de él.
- **Unidades extraíbles**. Kaspersky Embedded Systems Security para Windows analiza archivos en dispositivos externos, por ejemplo, unidades extraíbles o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse en el área del análisis o excluirse de ella.
- **Red**. Para agregar los archivos o las carpetas de red al área del análisis, especifique su ruta en formato UNC (convención de nomenclatura universal). La cuenta usada para iniciar la tarea debe tener permisos de acceso para los archivos y las carpetas de red que se agregan. De forma predeterminada, las tareas de Análisis a pedido se ejecutan en la cuenta de sistema.

  Las unidades de red conectadas tampoco se mostrarán en el árbol de recursos de archivos del dispositivo protegido. Para incluir objetos de unidades de red en el área del análisis, especifique la ruta a la carpeta que corresponde a la unidad de red en formato UNC.

- **Memoria del sistema**. Kaspersky Embedded Systems Security para Windows analiza los módulos y archivos ejecutables de los procesos que se ejecutan en el sistema operativo cuando se inicia el análisis.
- **Objetos de inicio**. Kaspersky Embedded Systems Security para Windows analiza objetos referidos por claves de registro y archivos de configuración, por ejemplo WIN.INI o SYSTEM.INI, así como los módulos de la aplicación que se inician automáticamente en el inicio del dispositivo protegido.
- **Carpetas compartidas**. Puede incluir carpetas compartidas del dispositivo protegido en el área del análisis.
- **Unidades virtuales**. Las unidades, archivos y carpetas virtuales conectadas al dispositivo protegido se pueden incluir en el área del análisis, por ejemplo, unidades de clústeres comunes.

Las unidades virtuales creadas mediante un comando SUBST no se muestran en el árbol de recursos de archivo del dispositivo protegido de la Consola de la aplicación. Para analizar objetos en una unidad virtual, incluya la carpeta del dispositivo protegido asociada con la unidad virtual en el área del análisis.

Las áreas de análisis estándar se muestran en el árbol de recursos de archivos de red de forma predeterminada. Se pueden agregar a la lista de recursos de archivos en red cuando se la crea en la configuración de áreas de análisis.

De forma predeterminada, las tareas de Análisis a pedido se ejecutan según las diferentes áreas:

- Tarea de Análisis al inicio del sistema operativo:
  - **Discos duros locales**.
  - **Unidades extraíbles**.
  - **Memoria del sistema**.
- Análisis de áreas críticas:
  - **Discos duros locales** (excluidas las carpetas de Windows)
  - **Unidades extraíbles**.
  - **Memoria del sistema**.
  - **Objetos de inicio**.
- Otras tareas:
  - **Discos duros locales** (excluidas las carpetas de Windows)
  - **Unidades extraíbles**.
  - **Memoria del sistema**.
  - **Objetos de inicio**.
  - **Carpetas compartidas**.

Análisis de archivos almacenados en línea

Acerca de los archivos en la nube

Kaspersky Embedded Systems Security para Windows puede interactuar con archivos en la nube de Microsoft OneDrive. La aplicación admite la nueva función de archivos a pedido de OneDrive.

Kaspersky Embedded Systems Security para Windows no admite otros depósitos en la nube.

OneDrive Files On-Demand ayuda a acceder a todos los archivos OneDrive sin necesidad de descargarlos todos y utilizar espacio de almacenamiento en el dispositivo. Puede descargar archivos en el disco duro cuando lo necesite.

Cuando la función OneDrive Files On-Demand está activada, ve los iconos de estado junto a cada archivo en la columna **Estado** en el Explorador de archivos. Cada archivo tiene uno de los siguientes estados:

Este icono de estado indica que el archivo *solo está disponible en línea*. Los archivos que están solo en línea no se almacenan físicamente en el disco duro. No puede abrir archivos que están solo en línea cuando su dispositivo no está conectado a Internet.

Este icono de estado indica que un archivo *está disponible localmente*. Esto sucede cuando abre un archivo solo en línea y lo descarga a su dispositivo. Puede abrir un archivo disponible localmente en cualquier momento, incluso sin acceso a Internet. Para liberar espacio, puede cambiar el archivo nuevamente a solo en línea.

Este icono de estado indica que un archivo está *almacenado en el disco duro y siempre está disponible*.

Análisis de archivos en la nube

Kaspersky Embedded Systems Security para Windows solo puede analizar archivos en la nube que están almacenados localmente en un dispositivo protegido. Estos archivos de OneDrive deben tener los estados y . Los archivos se omiten durante el análisis, ya que no están ubicados físicamente en el dispositivo protegido.

> Kaspersky Embedded Systems Security para Windows no descarga automáticamente los archivos de la nube durante el análisis, aunque estén incluidos en el área del análisis.

Varias tareas de Kaspersky Embedded Systems Security para Windows procesan los archivos en la nube en distintas situaciones según el tipo de tarea:

- Análisis de archivos en la nube en tiempo real: puede agregar carpetas que contengan archivos en la nube al área de la protección de la tarea Protección de archivos en tiempo real. El archivo se analiza cuando el usuario accede a él. Si el usuario accede al archivo , se descarga para estar disponible localmente y su estado cambia a . Esto permite que la tarea de Protección de archivos en tiempo real procese el archivo.

- Análisis a pedido de archivos en la nube: puede agregar carpetas que contienen archivos en la nube al área de la tarea Análisis a pedido. La tarea analiza archivos con los estados y . Si se encuentra algún archivo en el área, se omitirá durante el análisis, y se registrará un evento informativo en el registro de tareas para indicar que el archivo analizado solo es un marcador de posición de un archivo en la nube y no existe en un disco local.

- Generación y uso de reglas de control de inicio de aplicaciones: puede crear reglas de autorización y de denegación para archivos y con la tarea Generador de reglas de control de inicio de aplicaciones. La tarea Control de inicio de aplicaciones aplica el principio de denegación predeterminada y las reglas creadas para procesar y bloquear archivos en la nube.

  > La tarea Control de inicio de aplicaciones bloquea el inicio de todos los archivos en la nube más allá de su estado. Los archivos no se incluyen en el alcance de generación de reglas que realiza la aplicación, ya que no están presentes físicamente en su disco duro. Como no se puede crear ninguna regla para estos archivos, están sujetos al principio de denegación predeterminada.

Cuando se detecta una amenaza en un archivo de OneDrive en la nube, la aplicación realiza la acción especificada en la configuración de la tarea que lleva a cabo el análisis. Así, se puede realizar una copia de seguridad del archivo, o bien se lo puede eliminar, desinfectar o mover a la cuarentena.

Los cambios en los archivos locales se sincronizan con las copias almacenadas en OneDrive de acuerdo con los principios descritos en la documentación de Microsoft OneDrive.

Acerca de los niveles de seguridad predefinidos

Las opciones de seguridad de **Usar la tecnología iChecker**, **Usar la tecnología iSwift**, **Usar el analizador heurístico** y **Comprobar si el archivo está firmado por Microsoft** no se incluyen en la configuración de los niveles de seguridad predefinidos. Si se modifican las configuraciones de **Usar la tecnología iChecker**, **Usar la tecnología iSwift**, **Usar el analizador heurístico** y **Comprobar si el archivo está firmado por Microsoft**, el nivel de seguridad predefinido que seleccionó no cambiará.

Se puede aplicar uno de los cuatro niveles de seguridad predefinidos a un nodo seleccionado en el árbol de recursos de archivos del dispositivo: **Máximo rendimiento**, **Recomendado**, **Máxima protección** o **Solo notificar**. Cada uno de estos niveles contiene su propia configuración de seguridad predefinida (consulte la tabla a continuación).

Máximo rendimiento

El nivel de seguridad **Máximo rendimiento** se recomienda si su red tiene medidas de seguridad adicionales para los dispositivos protegidos, por ejemplo, firewalls y directivas de seguridad existentes, además de usar Kaspersky Embedded Systems Security para Windows en dispositivos protegidos.

Recomendado

El nivel de seguridad **Recomendado** garantiza la mejor combinación de protección e impacto en el rendimiento de los dispositivos protegidos. Los expertos de Kaspersky recomiendan este nivel porque es adecuado para proteger los dispositivos en la mayoría de las redes corporativas. El nivel de seguridad **Recomendado** está configurado de manera predeterminada.

Máxima protección

Se recomienda el nivel de seguridad **Máxima protección** si la red de la organización ha elevado los requisitos de seguridad del dispositivo.

Solo notificar

Se recomienda el nivel de seguridad **Solo notificar** cuando puedan existir muchos equipos infectados en la red corporativa y bloquearlos pueda tener un impacto significativo en el funcionamiento de la organización.

Niveles de seguridad predefinidos y los valores de configuración de seguridad correspondientes

Opciones	Nivel de seguridad			
	Máximo rendimiento	Recomendado	Máxima protección	Solo notificar
Analizar objetos	Por formato	Todos los objetos	Todos los objetos	Todos los objetos

Analizar solo los archivos nuevos y modificados	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado
Acción que se realizará con los objetos infectados y otros objetos	Desinfectar. Si falla la desinfección, eliminar	Realizar la acción recomendada por los expertos de Kaspersky	Desinfectar. Si falla la desinfección, eliminar	Solo notificar
Acción que se realizará con los objetos probablemente infectados	Cuarentena	Realizar la acción recomendada por los expertos de Kaspersky	Cuarentena	Solo notificar

La denominación "objeto crítico del sistema" hace referencia a aquellos archivos que el sistema operativo y Kaspersky Embedded Systems Security para Windows requieren para funcionar. Estos archivos no se pueden eliminar. Los procesos asociados con dichos objetos no se pueden finalizar.

Excluir archivos	No	No	No	No
No detectar	No	No	No	No
Detener el análisis si demora más de (s)	60 segundos.	No	No	No
Omitir objetos compuestos de más de (MB)	8192 MB	No	No	No
Analizar secuencias alternativas de NTFS	Sí	Sí	Sí	Sí
Analizar sectores de inicio del disco y MBR	Sí	Sí	Sí	Sí
Análisis de objetos compuestos	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Sólo objetos nuevos y modificados	• Archivos* • Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos	• Archivos* • Archivos SFX* • Bases de datos de correo electrónico* • Correo sin formato* • Objetos empaquetados* • Objetos OLE integrados*	• Archivos* • Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos

			* Todos los objetos	

Análisis de unidades extraíbles

Puede configurar el análisis de discos extraíbles conectados al dispositivo protegido mediante un puerto USB.

Kaspersky Embedded Systems Security para Windows analiza un disco extraíble mediante la tarea Análisis a pedido. La aplicación crea automáticamente una nueva tarea de Análisis a pedido cuando la unidad extraíble está conectada y la suprime después de que se completa el análisis. La tarea creada se realiza con el nivel de seguridad predefinido determinado para el análisis de unidades extraíbles. No puede configurar los valores de la tarea temporal de Análisis a pedido.

Si instaló Kaspersky Embedded Systems Security para Windows sin bases de datos antivirus, el análisis de unidades extraíbles no estará disponible.

Los análisis de Kaspersky Embedded Systems Security para Windows conectaron discos extraíbles cuando se registran como dispositivos externos USB en el sistema operativo. La aplicación no analiza una unidad extraíble si la conexión está bloqueada por la tarea Control de dispositivos. La aplicación no analiza dispositivos móviles conectados a MTP.

Kaspersky Embedded Systems Security para Windows permite el acceso a las unidades extraíbles durante el análisis.

Los resultados de análisis de cada unidad extraíble pueden consultarse en el registro de la tarea Análisis a pedido creada cuando se conecta la unidad extraíble.

Puede cambiar las configuraciones del componente Análisis de unidades extraíbles (consulte la tabla a continuación).

Configuración de Análisis de unidades extraíbles

Configuración	Valor predeterminado	Descripción
Analizar discos extraíbles al conectarlos via USB	Desactivada	Puede activar o desactivar el análisis de las unidades extraíbles después de conectarlas al dispositivo protegido por USB.
Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)	8192 MB	Puede reducir el área del componente si configura el volumen máximo de datos del disco analizado. Kaspersky Embedded Systems Security para Windows no analiza una unidad extraíble si el volumen de datos almacenados excede el valor especificado.
Analizar con nivel de seguridad	Máxima protección	Puede configurar tareas creadas de Análisis a pedido a través de uno de los tres niveles de seguridad: • **Máxima protección** • **Recomendado** • **Máximo rendimiento**

		El algoritmo usado cuando se detectaron objetos infectados, posiblemente infectados y otros objetos, así como otras configuraciones de análisis para cada nivel de seguridad, equivalen a los niveles de seguridad predefinidos en las tareas Análisis a pedido.

Acerca de la tarea del Monitor comparativo de integridad de archivos

Durante la tarea Monitor comparativo de integridad de archivos, Kaspersky Embedded Systems Security para Windows no verifica los archivos bloqueados, carpetas, accesos directos a archivos ni archivos en la nube.

La tarea Monitor comparativo de integridad de archivos supervisa la integridad de los archivos en el área de supervisión mediante la comparación del hash del archivo (hash MD5 o SHA256) con una línea base.

En la primera tarea Monitor comparativo de integridad de archivos que se ejecuta, Kaspersky Embedded Systems Security para Windows crea una línea base calculando y almacenando hash para archivos en el área de supervisión de la tarea. Si se modificó el área de supervisión de la tarea del Monitor comparativo de integridad de archivos, Kaspersky Embedded Systems Security para Windows actualiza la línea base en la siguiente tarea del Monitor comparativo de integridad de archivos ejecutada calculando y almacenando hash para los archivos en el área de supervisión de la tarea. Si se eliminó una tarea del Monitor comparativo de integridad de archivos, Kaspersky Embedded Systems Security para Windows elimina la línea base para esta tarea del Monitor de integridad de archivo de línea base.

Puede eliminar una línea base sin eliminar la tarea Monitor comparativo de integridad de archivos mediante la línea de comando.

La tarea Monitor comparativo de integridad de archivos realiza un seguimiento de los siguientes cambios de archivos en el área de supervisión:

- el área de supervisión contiene un archivo que no está presente en la línea base
- el área de supervisión no contiene un archivo presente en la línea base
- el hash de un archivo en el área de supervisión difiere del hash de este archivo en una línea base

La tarea Monitor comparativo de integridad de archivos no rastrea los cambios en los atributos de los archivos y los flujos alternativos.

Si no se puede acceder a un archivo o una carpeta, Kaspersky Embedded Systems Security para Windows no agregará este archivo o carpeta a la línea base durante la creación de la línea base y creará un evento sobre un error al calcular la suma de control del archivo durante la ejecución de la tarea Monitor comparativo de integridad de archivos.

Un archivo o una carpeta pueden ser inaccesibles por las siguientes razones:

- la ruta especificada no existe
- un tipo de archivos especificado por una máscara no está presente en la ruta especificada
- el archivo especificado está bloqueado

- el archivo especificado está vacío

Habilitar el inicio de la tarea Análisis a pedido desde el menú contextual

Puede habilitar el inicio de la tarea Análisis a pedido para uno o varios archivos desde un menú contextual en el Explorador de Microsoft Windows.

Para habilitar el inicio de la tarea Análisis a pedido desde un menú contextual:

1. Cree los siguientes archivos REG:

```
Editor del registro de Windows versión 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Scan with Kaspersky Embedded Systems Security para Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Scan with Kaspersky Embedded Systems Security para Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavshell.exe"="~ RUNASADMIN"
```

> Debe especificar la ubicación real de la carpeta de instalación de Kaspersky Embedded Systems Security.

2. Cree el archivo `scan.cmd` con el siguiente contenido:

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Análisis en curso...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

El archivo `scan.cmd` debe contener la siguiente información:

- La ubicación del archivo `kavshell.exe`.
- La ubicación del archivo temporal que contiene los resultados del análisis.
- Los parámetros del comando `KAVSHELL SCAN`.
- El valor de tiempo de espera para cerrar la ventana de la consola cuando finaliza la tarea.

3. Copie el archivo `scan.cmd` a la carpeta especificada en el archivo REG `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]`.

   La carpeta `C:\Temp` se usa en el ejemplo.

No es necesario reiniciar el sistema operativo.

Configuración de tareas de Análisis a pedido

De manera predeterminada, las tareas de Análisis a pedido tienen la descripción de la configuración en la tabla de arriba. Puede configurar tareas de análisis a pedido locales del sistema y personalizadas.

Configuración de tareas de Análisis a pedido

Configuración	Valor predeterminado	Descripción
Área del análisis	Aplicado en tareas locales del sistema y personalizadas: • **Análisis al inicio del sistema operativo**: el dispositivo protegido completo, excluidas las carpetas compartidas y los objetos de ejecución automática. • **Análisis de áreas críticas**: el dispositivo protegido completo, excluidas las carpetas compartidas y determinados archivos del	Se puede cambiar el área del análisis. El alcance del análisis no se puede configurar para las tareas locales del sistema **Análisis de archivos en cuarentena** y **Control de integridad de la aplicación**. La tarea **Análisis al inicio del sistema operativo** se crea automáticamente después de la instalación. De manera predeterminada, se aplica el modo **Solo notificar**. En este caso, después de implementar Kaspersky Embedded Systems Security en los dispositivos, puede habilitar la tarea **Análisis al inicio del sistema operativo** si no se descubrieron problemas con los servicios del sistema durante el análisis. Si la aplicación detecta servicios críticos del sistema como objetos infectados o probablemente infectados, el modo **Solo notificar** le da tiempo para averiguar el motivo y resolver el problema. Si la aplicación aplica el modo **Realizar la acción recomendada**, se realizará la acción **Desinfectar. Eliminar si falla la desinfección**. Desinfectar o eliminar archivos del sistema puede provocar problemas críticos en el inicio del sistema operativo.

	sistema operativo. • **Análisis a pedido** (tareas personalizadas): el dispositivo protegido completo.	
Configuración de seguridad	La configuración común para toda el área del análisis corresponde al nivel de seguridad **Recomendado**.	Para los nodos seleccionados en la lista o el árbol de recursos de archivos del dispositivo protegido, puede realizar lo siguiente: • Seleccionar un nivel de seguridad predefinido diferente • Cambiar manualmente la configuración de seguridad Puede guardar un grupo de opciones de seguridad para un nodo seleccionado como una plantilla y usarla más tarde en un nodo diferente.
Usar el analizador heurístico	Se utiliza con el nivel de análisis **Medio** para tareas de Análisis de áreas críticas, Análisis al inicio del sistema operativo y tareas personalizadas. Se utiliza con el nivel de análisis **Profundo** para la tarea de Análisis de archivos en cuarentena.	Se puede habilitar o deshabilitar el Analizador heurístico y configurar el nivel de análisis. El nivel de la tarea de Análisis de archivos en cuarentena no se puede configurar. El Analizador heurístico no se usa en las tareas de Control de integridad de la aplicación ni del Monitor comparativo de integridad de archivos.
Aplicar la Zona de confianza	Aplicado (no se aplicó a una tarea de Análisis de archivos en cuarentena)	Lista general de exclusiones que se pueden utilizar en tareas seleccionadas.
Usar KSN para análisis	Aplicado.	Puede mejorar la protección del dispositivo con la infraestructura de servicios en la nube de Kaspersky Security Network.
La configuración para iniciar una tarea con permisos específicos	La tarea se inicia con una cuenta de sistema.	Puede modificar la configuración de inicio de tareas con permisos de cuenta específicos para todas las tareas de Análisis a pedido de sistema o personalizadas, excepto las tareas de Análisis de archivos en cuarentena y Control de integridad de la aplicación.
Ejecutar tarea en segundo plano (prioridad baja)	No aplicado	Puede configurar el nivel de prioridad de las tareas de Análisis a pedido.

Programación de inicio de tareas	Aplicado en tareas locales del sistema: • Análisis al inicio del sistema operativo: **Al inicio de la aplicación** • Análisis de áreas críticas: **Semanal** • Análisis de archivos en cuarentena: **Tras actualizarse las bases de datos** • Control de integridad de la aplicación: **Diaria** No se utiliza en tareas personalizadas recientemente.	Puede configurar las opciones para el inicio programado de tareas.
Registro de ejecución del análisis y actualización del estado de protección del dispositivo	El estado de protección del dispositivo se actualiza cada semana después de la realización del Análisis de áreas críticas.	Puede configurar las opciones para registrar la ejecución del Análisis de áreas críticas de los siguientes modos: • Modificando la configuración de la programación de inicio de tareas de Análisis de áreas críticas. • Modificando el área del análisis de la tarea de Análisis de áreas críticas. • Creando tareas de Análisis a pedido personalizadas.

Gestión de tareas de Análisis a pedido a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración de la tarea para uno o todos los dispositivos protegidos en la red.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir el asistente de la tarea de Análisis a pedido

Para empezar a crear una tarea nueva de Análisis a pedido personalizada:

1. Para crear una tarea local:

   a. Expanda el nodo **Dispositivos administrados** en la Consola de administración de Kaspersky Security Center.

   b. Seleccione el grupo de administración al cual pertenece el dispositivo protegido.

   c. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual para el dispositivo protegido.

   d. Seleccione la opción del menú **Propiedades**.

   e. En la ventana que se abre, haga clic en el botón **Agregar** en la sección **Tareas**.

   Se abre la ventana **Nuevo asistente de tarea**.

2. Para crear una tarea de grupo:

   a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.

   b. Seleccione el grupo de administración para el cual desea crear una tarea.

   c. Abra la pestaña **Tareas**.

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

   Se abre la ventana **Nuevo asistente de tarea**.

3. Para crear una tarea para un grupo personalizado de dispositivos protegidos:

   a. En el nodo **Selecciones de dispositivos** en el árbol de la Consola de administración de Kaspersky Security Center, haga clic en el botón **Ejecutar selección** para realizar una selección de dispositivos.

   b. Abra la pestaña **Resultados de selección *nombre de selección***.

   c. En la lista desplegable **Realizar selección**, seleccione la opción **Crear una tarea para un resultado de selección**.

   Se abre la ventana **Nuevo asistente de tarea**.

4. Seleccione la tarea **Análisis a pedido** en la lista de tareas disponibles para Kaspersky Embedded Systems Security para Windows.

5. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración**.

Ajuste la configuración de la tarea como sea necesario.

Para configurar una tarea de Análisis a pedido existente,

haga doble clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

Se abre la ventana **Propiedades: Análisis a pedido**.

Cómo abrir las propiedades de la tarea de Análisis a pedido

Para abrir las propiedades de la aplicación para la tarea de Análisis a pedido en un solo dispositivo protegido:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración al cual pertenece el dispositivo protegido.
3. Seleccione la pestaña **Dispositivos**.
4. Haga doble clic en el nombre del dispositivo protegido para el cual desea configurar el área de análisis.
   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
5. Seleccione la sección **Tareas**.
6. En la lista de tareas creadas para el dispositivo, seleccione la tarea de Análisis a pedido que creó.
7. Haga clic en el botón **Propiedades**.
   Se abre la ventana **Propiedades: Análisis a pedido**.

Ajuste la configuración de la tarea como sea necesario.

Creación de una tarea de Análisis a pedido

Para empezar a crear una tarea nueva de Análisis a pedido personalizada:

1. Abra la ventana **Configuración** en el Asistente de nueva tarea.
2. Seleccione el **Método de creación de la tarea** requerido.
3. Haga clic en el botón **Siguiente**.
4. Cree un área del análisis en la ventana **Área del análisis**:

   De manera predeterminada, el área del análisis incluye áreas críticas del dispositivo protegido. Las áreas del análisis están marcadas en la tabla con el icono ☑. Las áreas del análisis excluidas están marcadas con el icono ☐ en la tabla.

   Puede cambiar el área del análisis: agregar áreas del análisis predefinidas, discos, carpetas, objetos de red y archivos, y asignar la configuración de seguridad específica para cada área agregada.

   - Para excluir todas las áreas críticas del análisis, abra el menú contextual en cada una de las líneas y seleccione la opción **Eliminar área**.

- Para incluir un área del análisis predeterminada, disco, carpeta, objeto de red o archivo en el área del análisis:

  a. Haga clic con el botón derecho en la tabla **Área del análisis** y seleccione **Agregar área**, o bien haga clic en el botón **Agregar**.

  b. En la ventana **Agregar objetos al área de análisis**, seleccione un área predefinida en la lista **Área predefinida**, especifique el disco, la carpeta, el objeto de red o el archivo del dispositivo protegido o de otro dispositivo de la red, y haga clic en el botón **Aceptar**.

- Para excluir subcarpetas o archivos del análisis, seleccione la carpeta (o el disco) agregado en la ventana **Área del análisis** del asistente:

  a. Abra el menú contextual y seleccione la opción **Configurar**.

  b. Haga clic en el botón **Configuración** en la ventana **Nivel de seguridad**.

  c. En la pestaña **General** de la ventana **Configuración del análisis a pedido**, cancele la selección de las casillas de verificación **Subcarpetas** y **Subarchivos**.

- Para cambiar la configuración de seguridad del área del análisis:

  a. Abra el menú contextual en el análisis cuya configuración desea definir y seleccione **Configurar**.

  b. En la ventana **Configuración del análisis a pedido**, seleccione uno de los niveles de seguridad predefinidos o haga clic en el botón **Configuración** para definir la configuración de seguridad manualmente.

  Las opciones de seguridad se configuran de la misma manera que en la tarea Protección de archivos en tiempo real.

- Para omitir objetos integrados en el área del análisis agregada:

  a. Abra el menú contextual en la tabla **Área del análisis** y seleccione **Agregar exclusión**.

  b. Especifique los objetos que desee excluir: seleccione un área predefinida en la lista **Área predefinida**, especifique el disco del dispositivo protegido, la carpeta, el objeto de red o el archivo en el dispositivo protegido o en otro dispositivo protegido de la red.

  c. Haga clic en el botón **Aceptar**.

5. En la ventana **Opciones**, configure el analizador heurístico y la integración con los demás componentes:

   - Configure el uso del analizador heurístico.
   - Seleccione la casilla de verificación **Aplicar zona de confianza** si quiere excluir objetos agregados en la lista de Zona de confianza del área del análisis de la tarea.
   - Seleccione la casilla de verificación **Usar KSN para análisis** si desea usar los servicios en la nube de Kaspersky Security Network para la tarea.
   - Para asignar la prioridad *Baja* al proceso de trabajo en que se ejecutará la tarea, seleccione la casilla de verificación **Ejecutar tarea en segundo plano** en la ventana **Opciones**.

De manera predeterminada, los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security para Windows reciben la prioridad *Media* (Normal).

- Para utilizar la tarea creada como una tarea del Análisis de áreas críticas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas** en la ventana **Opciones**.

6. Haga clic en el botón **Siguiente**.
7. En la sección **Programación**, configure el inicio programado de la tarea.
8. Haga clic en el botón **Siguiente**.
9. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desea utilizar.
10. Haga clic en el botón **Siguiente**.
11. Especifique el nombre de la tarea.
12. Haga clic en el botón **Siguiente**.

El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos: " * < > & \ : |

Se abre la ventana **Finalizar la creación de la tarea**.

13. Puede ejecutar la tarea opcionalmente después de que el Asistente finalice, seleccionando la casilla **Ejecutar tarea después de que finalice el asistente**.
14. Haga clic en **Finalizar** para terminar de crear la tarea.

Se creará la nueva tarea Análisis a pedido para el dispositivo protegido o el grupo de dispositivos protegidos seleccionados.

Asignar el estado de Análisis de áreas críticas a una tarea de Análisis a pedido

De manera predeterminada, Kaspersky Security Center asigna el estado *Advertencia* al dispositivo protegido si la tarea de Análisis de áreas críticas se ejecuta con menor frecuencia que la especificada por el umbral de generación de eventos *Hace mucho tiempo que no se realiza un análisis de áreas críticas* de Kaspersky Embedded Systems Security para Windows.

Para configurar el análisis de todos los dispositivos protegidos en un único grupo de administración:

1. Crear una tarea de grupo de Análisis a pedido.
2. En la ventana **Opciones** del asistente de tareas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas**. La configuración de tarea especificada (configuración de seguridad y área del análisis) se aplicará a todos los dispositivos protegidos del grupo. Configure la programación de la tarea.

Puede seleccionar la casilla de verificación **Considerar la tarea como análisis de áreas críticas** cuando crea la tarea de Análisis a pedido para un grupo de dispositivos protegidos o en otro momento, desde la ventana **Propiedades: <Nombre de la tarea>**.

3. La utilización de una directiva nueva o existente deshabilita el inicio programado de las tareas locales del sistema Análisis a pedido en los dispositivos protegidos del grupo.

El servidor de administración de Kaspersky Security Center evaluará el estado de seguridad del dispositivo protegido y le enviará una notificación según los resultados de la última ejecución de una tarea con el estado Análisis de áreas críticas y no según los resultados de la tarea local del sistema Análisis de áreas críticas.

Puede asignar el estado de *Análisis de áreas críticas* tanto a tareas en grupo de Análisis a pedido como a tareas para grupos de dispositivos protegidos.

La Consola de la aplicación se puede utilizar para ver si una tarea de Análisis a pedido es una tarea de Análisis de áreas críticas.

En la Consola de la aplicación, la casilla de verificación **Considerar la tarea como análisis de áreas críticas** se muestra en las propiedades de la tarea, pero no se puede modificar.

Ejecución de una tarea de Análisis a pedido en segundo plano

De manera predeterminada, los procesos en que se ejecutan las tareas de Kaspersky Embedded Systems Security para Windows reciben la prioridad *Media (Normal)*.

El proceso que ejecutará una tarea de Análisis a pedido se le puede asignar la prioridad *Baja*. Si se degrada la prioridad del proceso, se aumenta el tiempo requerido para ejecutar la tarea, pero puede tener un efecto beneficioso en el rendimiento de los procesos de otros programas en ejecución.

Varias tareas en segundo plano pueden estar en ejecución en un único proceso de trabajo con prioridad baja. Puede especificar la cantidad máxima de procesos para las tareas de Análisis a pedido en segundo plano.

Para cambiar la prioridad de una tarea de Análisis a pedido existente:

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione o desactive la casilla de verificación **Ejecutar tarea en segundo plano**.
3. Haga clic en el botón **Aceptar**.

La configuración de la tarea se guarda y se aplica inmediatamente a una tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Registro de la ejecución de un Análisis de áreas críticas

De forma predeterminada, el estado de protección del dispositivo se muestra en el panel de resultados del nodo **Kaspersky Embedded Systems Security para Windows** y se actualiza cada semana después de la realización de la tarea Análisis de áreas críticas.

La hora en la que se actualiza el estado de protección del dispositivo está relacionada con la programación de la tarea Análisis a pedido para la cual se ha seleccionado la casilla **Considerar la tarea como análisis de áreas críticas**. De forma predeterminada, la casilla de verificación solo se selecciona para la tarea de Análisis de áreas críticas y no se puede modificar para esta tarea.

Puede seleccionar la tarea Análisis a pedido relacionada al estado de protección del dispositivo solo desde Kaspersky Security Center.

Configuración del área de análisis de la tarea

Si modifica el área del análisis en las tareas Análisis al inicio del sistema operativo y Análisis de áreas críticas, puede restablecer el alcance del análisis predeterminado en estas tareas al restaurar Kaspersky Embedded Systems Security para Windows (**Inicio** > **Programas** > **Kaspersky Embedded Systems Security para Windows** > **Modificar o eliminar Kaspersky Embedded Systems Security para Windows**). En el asistente de configuración, seleccione **Reparar componentes instalados** y haga clic en **Siguiente**. A continuación, seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación**.

Para configurar el área de análisis para una tarea de Análisis a pedido existente:

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione la pestaña **Área del análisis**.
3. Para incluir elementos en el área del análisis:
   a. Abra el menú contextual en una parte vacía de la lista del área de análisis.
   b. Seleccione la opción **Agregar área** en el menú contextual.
   c. En la ventana abierta **Agregar objetos al área de análisis**, seleccione un tipo de objeto que desee agregar:
      - **Área predefinida** para agregar una de las áreas predefinidas en un dispositivo protegido. A continuación, en la lista desplegable, seleccione el área de análisis deseada.
      - **Disco, carpeta o ubicación de red** para incluir una unidad, carpeta, objeto de red particulares en el área del análisis. A continuación, seleccione el área deseada con un clic en el botón **Examinar**.
      - **Archivo** para incluir un archivo particular en el área del análisis. A continuación, seleccione el área deseada con un clic en el botón **Examinar**.

   No puede agregar un objeto al área del análisis si ya se agregó como una exclusión del área del análisis.
4. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos o siga estos pasos:
   a. Abra el menú contextual del área de análisis haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual, seleccione la opción **Agregar exclusión**.
   c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del área del análisis siguiendo el procedimiento utilizado al agregar un objeto al área del análisis.

5. Para modificar el área del análisis o una exclusión agregada, seleccione la opción **Editar área** en el menú contextual para el área del análisis correspondiente.

6. Para ocultar una exclusión o área del análisis agregada anteriormente en la lista de recursos de archivos en red, seleccione la opción **Eliminar área** en el menú contextual para el área del análisis necesaria.

   El área del análisis se excluye del área de la tarea de Análisis a pedido cuando se elimina de la lista de recursos de archivos en red.

7. Haga clic en el botón **Aceptar**.

Se cierra la ventana Configuración de área del análisis. Se guardan las opciones configuradas recientemente.

Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido

Se puede aplicar uno de los siguientes tres niveles de seguridad predefinidos a un nodo seleccionado en la lista de recursos de archivos del dispositivo protegido: **Máximo rendimiento**, **Recomendado** y **Máxima protección**.

Para seleccionar uno de los niveles de seguridad predefinidos:

1. Abra la ventana **Propiedades: Análisis a pedido**.

2. Seleccione la pestaña **Área del análisis**.

3. En la lista del dispositivo protegido, seleccione un elemento incluido en el área del análisis para configurar un nivel de seguridad predefinido.

4. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.

5. En la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se deba aplicar.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.

6. Haga clic en el botón **Aceptar**.

7. Haga clic en el botón **Aceptar** en la ventana **Propiedades: Análisis a pedido**.

   La configuración de la tarea se guarda y se aplica inmediatamente a una tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración manual de las opciones de seguridad

De forma predeterminada, las tareas de Análisis a pedido usan la configuración de seguridad común para toda el área del análisis.

Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área del análisis, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del dispositivo protegido o nodos del árbol.

Para configurar las opciones de seguridad manualmente:

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione la pestaña **Área del análisis**.
3. Seleccione los elementos en la lista del área del análisis para los cuales desea ajustar la configuración de la seguridad.

   Puede aplicar una plantilla de configuración de seguridad predefinida a un nodo o elemento seleccionado en el área de análisis.

4. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.

5. En las siguientes pestañas, configure los valores de seguridad del nodo o elemento seleccionado de acuerdo con sus requisitos:

   - **General**
   - **Acciones**
   - **Rendimiento**
   - **Depósito jerárquico**

6. Haga clic en el botón **Aceptar** de la ventana **Configuración del análisis a pedido**.
7. Haga clic en el botón **Aceptar** de la ventana **Área del análisis**.

Se guarda la nueva configuración del área del análisis.

Configuración de las opciones generales de tareas

Para ajustar la configuración de la tarea de Análisis a pedido general:

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione la pestaña **Área del análisis**.
3. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.

4. Haga clic en el botón **Configuración**.
5. En la pestaña **General**, en el cuadro de grupo **Analizar objetos**, especifique los tipos de objetos que desea incluir en el área del análisis:

- **Objetos para analizar**:
  - **Todos los objetos**
  - **Objetos analizados según su formato**
  - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
  - **Objetos analizados según la lista de extensiones especificada**
- **Subcarpetas**
- **Subarchivos**
- **Analizar sectores de inicio del disco y MBR**
- **Analizar secuencias alternativas de NTFS**

6. En el cuadro de grupo **Rendimiento**, seleccione o desactive la casilla de verificación **Analizar solo los archivos nuevos y modificados**.

   Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

7. En el cuadro de grupo **Análisis de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área del análisis:
   - **Todos** / **Solo nuevos archivos comprimidos**
   - **Todos** / **Solo nuevos archivos SFX**
   - **Todos** / **Solo nuevas bases de datos de correo electrónico**
   - **Todos** / **Solo nuevos objetos empaquetados**
   - **Todos** / **Solo nuevo correo electrónico simple**
   - **Todos** / **Solo nuevos objetos OLE incorporados**
8. Haga clic en el botón **Aceptar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

Para configurar acciones en objetos infectados y otros objetos detectados durante la tarea de Análisis a pedido:

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione la pestaña **Área del análisis**.
3. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.

4. Haga clic en el botón **Configuración**.
5. Seleccione la pestaña **Acciones**.
6. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
   - **Solo notificar**.
   - **Desinfectar**.
   - **Desinfectar; si falla la desinfección, eliminar**.
   - **Eliminar**.
   - **Realizar la acción recomendada**.
7. Seleccione la acción a realizar en los objetos probablemente infectados:
   - **Solo notificar**.
   - **Poner en cuarentena**.
   - **Eliminar**.
   - **Realizar la acción recomendada**.
8. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.
   b. Haga clic en el botón **Configuración**.
   c. En la ventana que se abre, seleccione una acción primaria y una acción secundaria (a realizarse en caso de que falle la acción primaria) para cada tipo de objeto detectado.
   d. Haga clic en el botón **Aceptar**.
9. Seleccione la acción a realizar en objetos compuestos incurables: seleccione o desactive la casilla de verificación **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.
10. Haga clic en el botón **Aceptar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

Para configurar las opciones de rendimiento para la tarea Análisis a pedido:

1. Abra la ventana **Propiedades: Análisis a pedido**.
2. Seleccione la pestaña **Área del análisis**.
3. Haga clic en el botón **Configurar**.

Se abre la ventana **Configuración del análisis a pedido**.

4. Haga clic en el botón **Configuración**.
5. Seleccione la pestaña **Rendimiento**.
6. En el bloque **Exclusiones**:
   - Desactive o seleccione la casilla de verificación **Excluir archivos**.
   - Borre o seleccione la casilla de verificación **No detectar**.
   - Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.
7. En el bloque **Configuración avanzada**:
   - **Detener el análisis si demora más de (s)**
   - **Omitir objetos compuestos de más de (MB)**
   - **Usar la tecnología iSwift**
   - **Usar la tecnología iChecker**
8. Haga clic en el botón **Aceptar**.

Se guardará la nueva configuración de la tarea.

Configuración del Análisis de unidades extraíbles

Para configurar el análisis de unidades extraíbles después de conectar al dispositivo protegido:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.

   En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Adicional**.
5. Haga clic en el botón **Configuración** en la subsección **Análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.
6. En el bloque **Analizar al conectar**, realice las siguientes acciones:
   - Seleccione la casilla de verificación **Analizar discos extraíbles al conectarlos via USB** si desea que Kaspersky Embedded Systems Security para Windows analice automáticamente las unidades extraíbles cuando se conecten.
   - De ser necesario, seleccione **Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)** y especifique el valor máximo en el campo de la derecha.

- En la lista desplegable **Analizar con nivel de seguridad**, seleccione el nivel de seguridad que reúna los parámetros con los que desee ejecutar las tareas de Análisis de unidades extraíbles.

7. Haga clic en el botón **Aceptar**.

La configuración especificada se guarda y se aplica.

Configuración de una tarea Monitor comparativo de integridad de archivos

Para configurar la tarea de grupo del Monitor comparativo de integridad de archivos:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas.
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.

   En la sección **Notificación**, configure las opciones de notificación del evento de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
5. En la sección **Área del análisis**, haga lo siguiente:
   a. Para incluir la carpeta en el área de la tarea del Monitor comparativo de integridad de archivos:
      1. Haga clic en el botón **Agregar**.
         Se abre la ventana **Propiedades del área de análisis**.
      2. Seleccione o desactive la casilla **Analizar esta área**.
      3. Haga clic en el botón **Examinar** para especificar la carpeta que desee incluir en el área de la tarea Monitor comparativo de integridad de archivos.
      4. Seleccione la casilla **Analizar también las subcarpetas**, si desea incluir todas las subcarpetas en el alcance de la tarea Monitor comparativo de integridad de archivos.
   b. Para incluir o excluir la carpeta agregada previamente al área de la tarea Monitor comparativo de integridad de archivos, seleccione o desactive la casilla a la izquierda de la ruta de la carpeta en la tabla **Área del análisis**.
   c. Para eliminar la carpeta previamente agregada al área de la tarea Monitor comparativo de integridad de archivos, seleccione esta carpeta en la tabla **Área del análisis** y haga clic en el botón **Eliminar**.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).

7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para ejecutar la tarea.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

9. Haga clic en el botón **Aceptar** de la ventana **Propiedades: <Nombre de la tarea>**.

   Se guardan las opciones de la tarea de grupo recientemente configuradas.

Gestión de tareas de Análisis a pedido a través de la Consola de la aplicación

En esta sección, aprenderá a navegar por la interfaz de la Consola de la aplicación y a definir la configuración de la tarea en un dispositivo protegido.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la tarea de Análisis a pedido

Para abrir la configuración general de la tarea de Análisis a pedido a través de la Consola de la aplicación:

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. Seleccione el nodo secundario que corresponde a la tarea que desea configurar.
3. En el nodo secundario del panel de resultados, haga clic en el vínculo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

Cómo abrir la configuración del área de la tarea Análisis a pedido

Para abrir la configuración del área del análisis a través de la Consola de la aplicación:

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. Seleccione el nodo secundario correspondiente a una tarea de Análisis a pedido que desea configurar.
3. En el panel de resultados del nodo seleccionado, haga clic en el vínculo **Configurar el área de análisis**.

   Se abre la ventana **Configuración del área de análisis**.

Creación y configuración de una tarea de Análisis a pedido

Las tareas personalizadas para un solo dispositivo protegido pueden generarse en el nodo **Análisis a pedido**. Las tareas personalizadas no pueden crearse en los demás componentes funcionales de Kaspersky Embedded Systems Security para Windows.

Para crear y configurar una tarea nueva de Análisis a pedido:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Análisis a pedido**.
2. Seleccione **Agregar tarea**.

   Se abre la ventana **Agregar tarea**.
3. Defina los siguientes valores de configuración de tarea:

   - **Nombre**: un nombre de tarea que consta de no más de 100 caracteres. Puede contener cualquier símbolo excepto **" * < > & \ : |**.

     No puede guardar una tarea o configurar una tarea nueva en las pestañas **Programación**, **Avanzado** y **Ejecutar como** si el nombre de la tarea no se especifica.

   - **Descripción**: información adicional sobre la tarea, no más de 2000 caracteres. Esta información se mostrará en la ventana de propiedades de la tarea.
   - **Usar el analizador heurístico**.
   - **Ejecutar tarea en segundo plano**.
   - **Aplicar la Zona de confianza**.
   - **Considerar la tarea como análisis de áreas críticas**.
   - **Usar KSN para análisis**.
4. Configure la programación de inicio de tareas en las pestañas **Programación**y **Avanzado**.
5. En la pestaña **Ejecutar como**, ajuste la configuración para que se inicie la tarea con permisos de cuenta específicos.
6. Haga clic en el botón **Aceptar** de la ventana **Agregar tarea**.

   Se crea una nueva tarea de Análisis a pedido personalizada. Se muestra un nodo con el nombre de la tarea nueva en el árbol de la Consola de la aplicación. La operación se registra en el registro de auditoría del sistema.
7. Si es necesario, en el panel de resultados del nodo seleccionado, seleccione **Configurar el área de análisis**.

   Se abre la ventana **Configuración del área de análisis**.
8. En el árbol o lista de recursos del archivo del dispositivo protegido, seleccione los nodos o elementos que desea incluir en el área del análisis.
9. Seleccione uno de los niveles de seguridad predefinidos o configure las opciones de análisis de forma manual.

10. Haga clic en el botón **Guardar** de la ventana **Configuración del área de análisis**.

Las opciones configuradas se aplican en el siguiente inicio de la tarea.

Área del análisis en tareas de Análisis a pedido

Esta sección contiene información sobre la creación y la utilización de un área del análisis en tareas del Análisis a pedido.

Configuración de la visualización para recursos de archivos en red

Para seleccionar la visualización para recursos de archivos en red durante la configuración del área del análisis:

1. Abra la ventana **Configuración del área de análisis**.
2. Abra la lista desplegable en la sección superior izquierda de la ventana y seleccione una de las siguientes opciones:
   - Seleccione la opción **Vista de árbol** para ver los recursos de archivos en red como un árbol.
   - Seleccione la opción **Vista de lista** para ver los recursos de archivos en red como una lista.

   De forma predeterminada, los recursos de archivos en red del dispositivo protegido se muestran en un modo de vista de lista.
3. Haga clic en el botón **Guardar**.

Creación de área del análisis

Si administra Kaspersky Embedded Systems Security para Windows remotamente en el dispositivo protegido mediante la Consola de la aplicación instalada en una estación de trabajo del administrador, debe ser miembro del grupo de administradores del dispositivo protegido para poder ver las carpetas contenidas en él.

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

Si modifica el área del análisis en las tareas Análisis al inicio del sistema operativo y Análisis de áreas críticas, puede restablecer el alcance del análisis predeterminado en estas tareas al restaurar Kaspersky Embedded Systems Security para Windows (**Inicio** > **Programas** > **Kaspersky Embedded Systems Security para Windows** > **Modificar o eliminar Kaspersky Embedded Systems Security para Windows**). En el asistente de configuración, seleccione **Reparar componentes instalados** y haga clic en **Siguiente**. A continuación, seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación**.

El procedimiento para crear el alcance de la tarea de Análisis a pedido depende de la vista seleccionada de los recursos de archivos en red. Puede configurar la visualización de los recursos de archivos en red como un árbol o como una lista (vista predeterminada).

Para crear un área del análisis utilizando el árbol de recursos de archivos en red:

1. Abra la ventana **Configuración del área de análisis**.
2. En la sección izquierda de la ventana, abra el árbol de recursos de archivos en red para ver todos los nodos y nodos secundarios.
3. Haga lo siguiente:
   - Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos.
   - Para incluir nodos individuales al área del análisis, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
     - Si desea incluir todas las unidades de un tipo particular en el área del análisis, seleccione la casilla junto al nombre del tipo de unidad requerida (por ejemplo, para agregar todas las unidades extraíbles del dispositivo protegido, seleccione la casilla **Unidades extraíbles**).
     - Si desea incluir una unidad individual de un tipo particular en el área del análisis, expanda el nodo que contiene las unidades de ese tipo y seleccione la casilla junto al nombre de la unidad requerida. Por ejemplo, para seleccionar la unidad extraíble **F:**, expanda el nodo **Unidades extraíbles** y seleccione la casilla de verificación para la unidad **F:**.
     - Si desea incluir solamente una carpeta o un archivo de la unidad, seleccione la casilla de verificación ubicada al lado del nombre de esa carpeta o de ese archivo.
4. Haga clic en el botón **Guardar**.

Se cerrará la ventana **Configuración del área de análisis**. Se guardan las opciones configuradas recientemente.

Para crear un área del análisis utilizando la lista de recursos de archivos en red:

1. Abra la ventana **Configuración del área de análisis**.
2. Para incluir nodos individuales al área del análisis, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
   a. Abra el menú contextual del área de análisis haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual del botón, seleccione **Agregar área de análisis**.
   c. En la ventana **Agregar área de análisis** abierta, seleccione el tipo de objeto que desee agregar:
      - **Área predefinida**, si desea que el área de análisis incluya una de las áreas predefinidas en el dispositivo protegido. A continuación, en la lista desplegable, seleccione el área de análisis deseada.
      - **Disco, carpeta o ubicación de red** para incluir una unidad, carpeta, objeto de red particulares en el área del análisis. A continuación, seleccione el área deseada con un clic en el botón **Examinar**.
      - **Archivo** para incluir un archivo particular en el área del análisis. A continuación, seleccione el área deseada con un clic en el botón **Examinar**.

   No puede agregar un objeto al área del análisis si ya se agregó como una exclusión del área del análisis.
3. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos o siga estos pasos:

a. Abra el menú contextual del área de análisis haciendo clic en él con el botón derecho del mouse.

b. En el menú contextual, seleccione la opción **Agregar exclusión**.

c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del área del análisis siguiendo el procedimiento utilizado al agregar un objeto al área del análisis.

4. Para modificar el área del análisis o una exclusión agregada, seleccione la opción **Editar área** en el menú contextual para el área del análisis necesario.

5. Para ocultar una exclusión o área del análisis agregada anteriormente en la lista de recursos de archivos en red, seleccione la opción **Eliminar de la lista** en el menú contextual para el área del análisis necesaria.

El área del análisis se excluye del área de la tarea de Análisis a pedido cuando se elimina de la lista de recursos de archivos en red.

6. Haga clic en el botón **Guardar**.

Se cerrará la ventana **Configuración del área de análisis**. Se guardan las opciones configuradas recientemente.

Inclusión de objetos de red en el área del análisis

Se pueden agregar unidades, carpetas o archivos de red en el área del análisis mediante la especificación de su ruta en formato UNC (convención de nomenclatura universal).

Puede analizar carpetas de la red con la cuenta de sistema.

Para agregar una ubicación de la red al área del análisis:

1. Abra la ventana Configuración del área de análisis.

2. Abra la lista desplegable en la parte superior izquierda de la ventana y seleccione **Vista de árbol**.

3. En el menú contextual del nodo **Red**:

   - Seleccione **Agregar carpeta de red** si desea agregar una carpeta de red al área del análisis.
   - Seleccione **Agregar archivo de red** si desea agregar un archivo de red al área del análisis.

4. Introduzca la ruta del archivo o la carpeta de red en formato UNC y presione la tecla **INTRO**.

5. Seleccione la casilla de verificación junto al objeto de red agregado recientemente para incluirlo en el área del análisis.

6. Si es necesario, cambie la configuración de seguridad para el objeto de red agregado.

7. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea especificada.

Creación de un área del análisis virtual

Puede incluir unidades, carpetas y archivos virtuales en el área del análisis a fin de crear un área del análisis virtual.

Se puede ampliar el alcance del análisis si se agregan unidades virtuales, carpetas o archivos individuales solo si el alcance del análisis se presenta como un árbol de recursos de archivos.

Para agregar una unidad virtual al área del análisis:

1. Abra la ventana **Configuración del área de análisis**.
2. Abra la lista desplegable en la parte superior izquierda de la ventana y seleccione **Vista de árbol**.
3. En el árbol de recursos de archivos del dispositivo protegido, abra el menú contextual en el nodo **Unidades virtuales**, haga clic en **Agregar unidad virtual** y seleccione el nombre de la unidad virtual de la lista de nombres disponibles.
4. Seleccione la casilla de verificación junto a la unidad agregada para incluirla en el área del análisis.
5. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea especificada.

Para agregar un archivo o carpeta virtual al área del análisis:

1. Abra la ventana **Configuración del área de análisis**.
2. Abra la lista desplegable en la parte superior izquierda de la ventana y seleccione **Vista de árbol**.
3. En el árbol de recursos de archivos del dispositivo protegido, abra el menú contextual del nodo para agregar una carpeta o un archivo y seleccione una de las opciones siguientes:
   - **Agregar carpeta virtual**, si desea agregar una carpeta virtual al área de análisis.
   - **Agregar archivo virtual**, si desea agregar un archivo virtual al área de análisis.
4. En el campo de entrada, especifique el nombre de la carpeta o el archivo.
5. En la línea con el nombre de la carpeta o el archivo, seleccione la casilla de verificación para incluir esta carpeta o archivo en el área del análisis.
6. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea especificada.

Configuración de las opciones de seguridad

De forma predeterminada, las tareas de Análisis a pedido usan la configuración de seguridad común para toda el área del análisis.

Estos ajustes corresponden al nivel de seguridad predefinido **Recomendado**.

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para toda el área del análisis, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del dispositivo protegido o nodos del árbol.

Al trabajar con el árbol de recursos de archivos en red, las opciones de seguridad que se configuran para el nodo principal seleccionado se aplican automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

Para establecer manualmente la configuración de seguridad:

1. Abra la ventana **Configuración del área de análisis**.

2. En la parte izquierda de la ventana, seleccione el nodo o elemento para los cuales desea ajustar la configuración de la seguridad.

   Puede aplicar una plantilla de configuración de seguridad predefinida a un nodo o elemento seleccionado en el área de análisis.

   En la parte izquierda de la ventana, puede seleccionar la vista de recursos de archivos en red, crear un área de análisis o crear un área de análisis virtual.

3. En la parte derecha de la ventana, realice una de las siguientes acciones:

   - En la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad a aplicar.
   - En las siguientes pestañas, configure los valores de seguridad del nodo o elemento seleccionado de acuerdo con sus requisitos:
     - **General**
     - **Acciones**
     - **Rendimiento**
     - **Depósito jerárquico**

4. Haga clic en el botón **Guardar** de la ventana **Configuración del área de análisis**.

Se guarda la nueva configuración del área del análisis.

Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido

Se puede aplicar uno de los siguientes tres niveles de seguridad predefinidos a un nodo seleccionado en el árbol o la lista de recursos de archivos del dispositivo protegido: **Máximo rendimiento**, **Recomendado** y **Máxima protección**.

Para seleccionar uno de los niveles de seguridad predefinidos:

1. Abra la ventana **Configuración del área de análisis**.

2. En la lista o árbol de recursos de archivos en red del dispositivo protegido, seleccione un nodo o elemento para establecer el nivel de seguridad predefinido.

3. Asegúrese que el nodo o elemento seleccionado se incluya en el área del análisis.

4. En la parte derecha de la ventana, en la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se aplicará.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.

5. Haga clic en el botón **Guardar**.

   La configuración de la tarea se guarda y se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración de las opciones generales de tareas

Para configurar las opciones de seguridad generales de la tarea de Análisis a pedido:

1. Abra la ventana **Configuración del área de análisis**.

2. Abra la pestaña **General**.

3. En el cuadro de grupo **Analizar objetos**, especifique los tipos de objetos que desea incluir en el área del análisis:

   - **Objetos para analizar**:
     - **Todos los objetos**
     - **Objetos analizados según su formato**
     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
     - **Objetos analizados según la lista de extensiones especificada**
   - **Analizar sectores de inicio del disco y MBR**
   - **Analizar secuencias alternativas de NTFS**

4. En el cuadro de grupo **Rendimiento**, seleccione o desactive la casilla de verificación **Analizar solo los archivos nuevos y modificados**.

   Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En el cuadro de grupo **Análisis de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área del análisis:

   - **Todos** / **Solo nuevos archivos comprimidos**
   - **Todos** / **Solo nuevos archivos SFX**
   - **Todos** / **Solo nuevas bases de datos de correo electrónico**

- **Todos** / **Solo nuevos objetos empaquetados**
- **Todos** / **Solo nuevo correo electrónico simple**
- **Todos** / **Solo nuevos objetos OLE incorporados**

6. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Análisis a pedido:

1. Abra la ventana **Configuración del área de análisis**.
2. Seleccione la pestaña **Acciones**.
3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
   - **Solo notificar**.
   - **Desinfectar**.
   - **Desinfectar; si falla la desinfección, eliminar**Si falla la desinfección, eliminar
   - **Eliminar**.
   - **Realizar la acción recomendada**.
4. Seleccione la acción a realizar en los objetos probablemente infectados:
   - **Solo notificar**.
   - **Poner en cuarentena**.
   - **Eliminar**.
   - **Realizar la acción recomendada**.
5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.
   b. Haga clic en el botón **Configuración**.
   c. En la ventana que se abre, seleccione una acción primaria y una acción secundaria (a realizarse en caso de que falle la acción primaria) para cada tipo de objeto detectado.
   d. Haga clic en el botón **Aceptar**.
6. Seleccione la acción a realizar en objetos compuestos incurables: seleccione o desactive la casilla de verificación **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.

7. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

Para configurar las opciones de rendimiento para la tarea Análisis a pedido:

1. Abra la ventana **Configuración del área de análisis**.
2. Seleccione la pestaña **Rendimiento**.
3. En el bloque **Exclusiones**:
   - Desactive o seleccione la casilla de verificación **Excluir archivos**.
   - Borre o seleccione la casilla de verificación **No detectar**.
   - Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.
4. En el bloque **Configuración avanzada**:
   - **Detener el análisis si demora más de (s)**
   - **Omitir objetos compuestos de más de (MB)**
   - **Usar la tecnología iSwift**
   - **Usar la tecnología iChecker**
5. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración del depósito jerárquico

Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Análisis a pedido:

1. Abra la ventana **Configuración del área de análisis**.
2. Seleccione la pestaña **Depósito jerárquico**.
3. Seleccione la acción que desea realizar en los archivos:
   - **No analizar**
   - **Analizar solo la parte residente del archivo**
   - **Analizar todo el archivo**
     Si selecciona esta acción, puede determinar las siguientes opciones:

- Marque o desmarque la casilla de verificación **Solo si se accedió al archivo en el período especificado (días)** e indique el número de días.
- Marque o desmarque la casilla de verificación **No copiar el archivo al disco duro local (de ser posible)**.

4. Haga clic en el botón **Guardar**.

Se guardará la nueva configuración de la tarea.

Análisis de unidades extraíbles

Para configurar el análisis de unidades extraíbles después de conectar al dispositivo protegido en la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo de **Kaspersky Embedded Systems Security para Windows** y seleccione la opción **Configurar análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.

2. En el bloque **Analizar al conectar**, realice las siguientes acciones:
   - Seleccione la casilla de verificación **Analizar discos extraíbles al conectarlos via USB** si desea que Kaspersky Embedded Systems Security para Windows analice automáticamente las unidades extraíbles cuando se conecten.
   - De ser necesario, seleccione **Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, seleccione el nivel de seguridad que reúna los parámetros con los que desee ejecutar las tareas de Análisis de unidades extraíbles.
3. Haga clic en el botón **Aceptar**.

La configuración especificada se guarda y se aplica.

Estadísticas de la tarea de Análisis a pedido

Mientras se ejecuta la tarea de Análisis a pedido, puede visualizar información sobre la cantidad de objetos procesados por Kaspersky Embedded Systems Security para Windows desde que se inició.

Esta información permanecerá disponible aún si se pausa la tarea. Puede ver las estadísticas de la tarea en el registro de tareas.

Para ver las estadísticas de una tarea de Análisis a pedido:

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. Seleccione la tarea de Análisis a pedido cuyas estadísticas desea ver.

   Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de resultados del nodo seleccionado.

En la tabla a continuación, se puede ver la información sobre los objetos procesados por Kaspersky Embedded Systems Security para Windows desde que se inició.

Campo	Descripción
Detectado	Número de objetos detectados por Kaspersky Embedded Systems Security para Windows. Por ejemplo, si Kaspersky Embedded Systems Security para Windows detecta un objeto malicioso en cinco archivos, el valor de este campo aumenta en uno.
Objetos infectados y otros objetos detectados	Número de objetos que Kaspersky Embedded Systems Security para Windows encontró y clasificó como infectados o número de archivos encontrados de software legítimo que no se excluyeron del alcance del análisis y se clasificaron como software legítimo que los intrusos pueden utilizar para dañar el dispositivo o sus datos personales.
Objetos probablemente infectados detectados	Cantidad de objetos probablemente infectados encontrados por Kaspersky Embedded Systems Security para Windows.
Objetos no desinfectados	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows no desinfectó debido a los siguientes motivos: • El tipo de objeto detectado no se puede desinfectar. • Se produjo un error durante la desinfección.
Objetos que no se pasaron a Cuarentena	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows intentó poner en cuarentena sin éxito, por ejemplo, debido a espacio insuficiente en el disco.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security para Windows intentó eliminar sin éxito debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos no analizados	Cantidad de objetos en el área de la protección que Kaspersky Embedded Systems Security para Windows no pudo analizar debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos sin copia de seguridad	Cantidad de objetos cuyas copias Kaspersky Embedded Systems Security para Windows intentó guardar sin éxito en Copia de seguridad; por ejemplo, debido a espacio insuficiente en el disco.
Errores de procesamiento	Cantidad de objetos en los que se produjo un error durante su procesamiento.
Objetos desinfectados	Número de objetos desinfectados por Kaspersky Embedded Systems Security para Windows.
Pasados a Cuarentena	Número de objetos pasados a Cuarentena por Kaspersky Embedded Systems Security para Windows.
Pasados a Copia de seguridad	Cantidad de objetos cuyas copias Kaspersky Embedded Systems Security para Windows guardó en Copia de seguridad.
Objetos eliminados	Número de objetos eliminados por Kaspersky Embedded Systems Security para Windows.
Objetos protegidos con contraseña	Cantidad de objetos (por ejemplo, archivos) que Kaspersky Embedded Systems Security para Windows omitió porque estaban protegidos por contraseña.
Objetos dañados	Cantidad de objetos omitidos por Kaspersky Embedded Systems Security para Windows porque el formato estaba dañado.
Objetos procesados	Cantidad total de objetos que procesó Kaspersky Embedded Systems Security para Windows.

También puede ver las estadísticas de la tarea Análisis a pedido en el registro de tareas seleccionado si hace clic en el vínculo **Abrir el registro de tareas** en la sección **Administración** del panel de resultados.

Le recomendamos procesar manualmente los eventos incluidos en la pestaña **Eventos** en el registro de tareas al finalizar la tarea.

Creación y configuración de una tarea del Monitor comparativo de integridad de archivos

Para crear o configurar una nueva tarea del Monitor comparativo de integridad de archivos:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Inspección del sistema**.
2. Seleccione **Crear tarea del Monitor comparativo de integridad de archivos**.

   Se abre la ventana **Agregar tarea**.
3. En la lista desplegable **Algoritmo de cálculo del hash**, seleccione una de las opciones:
   - **MD5**
   - **SHA256**
4. En la tabla **Áreas de análisis**, realice las siguientes acciones:
   a. Para agregar un archivo o carpeta en el área de la tarea del Monitor comparativo de integridad de archivos:
      1. Haga clic en el botón **Agregar**.

         Se abre la ventana **Propiedades del área de análisis**.
      2. Seleccione o desactive la casilla **Analizar esta área**.
      3. Haga clic en el botón **Examinar** para especificar el archivo o la carpeta que desee incluir en el área de la tarea Monitor comparativo de integridad de archivos.
      4. Seleccione la casilla **Analizar también las subcarpetas**, si desea incluir todas las subcarpetas en el alcance de la tarea Monitor comparativo de integridad de archivos.
      5. Haga clic en el botón **Aceptar**.
   b. Para cambiar un archivo o una carpeta agregados previamente al área de la tarea del Monitor comparativo de integridad de archivos:
      1. Haga clic en el botón **Cambiar**.

         Se abre la ventana **Propiedades del área de análisis**.
      2. Seleccione o desactive la casilla **Analizar esta área**.
      3. Haga clic en el botón **Examinar** para especificar el archivo o la carpeta que desee incluir en el área de la tarea Monitor comparativo de integridad de archivos.

4. Seleccione o desactive la casilla **Analizar también las subcarpetas**, si desea incluir o excluir todas las subcarpetas del alcance de la tarea Monitor comparativo de integridad de archivos.

5. Haga clic en el botón **Aceptar**.

c. Para eliminar un archivo o una carpeta que haya agregado al área de la tarea Monitor comparativo de integridad de archivos, seleccione el archivo o la carpeta en cuestión en la tabla **Áreas de análisis** y haga clic en el botón **Eliminar**.

5. Configure la programación de inicio de tareas en las pestañas **Programación**y **Avanzado**.

6. En la pestaña **Ejecutar como**, ajuste la configuración para que se inicie la tarea con permisos de cuenta específicos.

7. Haga clic en el botón **Aceptar** de la ventana **Agregar tarea**.

   Se crea una nueva tarea personalizada del Monitor comparativo de integridad de archivos. Se muestra un nodo con el nombre de la tarea nueva en el árbol de la Consola de la aplicación. La operación se registra en el registro de auditoría del sistema.

Para abrir la configuración de la tarea del Monitor comparativo de integridad de archivos:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.

2. Seleccione el nodo secundario que corresponde a la tarea que desea configurar.

3. En el nodo secundario del panel de resultados, haga clic en el vínculo **Propiedades**.

   Aparece la ventana **Configuración de tareas**.

Administración de tareas de Análisis a pedido a través del Complemento web

En esta sección, aprenderá a navegar la interfaz del Complemento web para los dispositivos protegidos de la red.

Cómo abrir el asistente de la tarea de Análisis a pedido

Para empezar a crear una tarea local nueva de Análisis a pedido:

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

2. Haga clic en la pestaña **Grupos** para seleccionar el grupo de administración al que pertenece el dispositivo protegido.

3. Haga clic en el nombre del dispositivo protegido.

4. En la ventana **<Nombre del dispositivo>** que se abre, seleccione la pestaña **Tareas**.

5. Haga clic en el botón **Agregar**.

   Se abre la ventana **Nuevo asistente de tarea**.

6. En la lista desplegable **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security para Windows**.

7. En la lista desplegable **Tipo de tarea**, seleccione la tarea **Análisis a pedido**.
8. Haga clic en el botón **Siguiente**.

Ajuste la configuración de la tarea como sea necesario.

Para empezar a crear una tarea nueva de Análisis a pedido de grupo:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en la pestaña **Grupos** para seleccionar el grupo de administración para el cual desea crear una tarea.
3. Haga clic en el botón **Agregar**.
   Se abre la ventana **Nuevo asistente de tarea**.
4. En la lista desplegable **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security para Windows**.
5. En la lista desplegable **Tipo de tarea**, seleccione la tarea **Análisis a pedido**.
6. Haga clic en el botón **Siguiente**.

Ajuste la configuración de la tarea como sea necesario.

Para empezar a crear una tarea nueva de Análisis a pedido para un grupo personalizado:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Selecciones de dispositivos**.
2. Elija la selección para la cual desea crear una tarea.
3. Haga clic en el botón **Iniciar**.
4. En la ventana **Resultados de la selección**, seleccione los dispositivos para los que desea crear una tarea.
5. Haga clic en el botón **Nueva tarea**.
6. En la lista desplegable **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security para Windows**.
7. En la lista desplegable **Tipo de tarea**, seleccione la tarea **Análisis a pedido**.
8. Haga clic en el botón **Siguiente**.

Ajuste la configuración de la tarea como sea necesario.

Para configurar una tarea de Análisis a pedido existente:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Tareas**.
2. Haga clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

Se abre la ventana **<Nombre de la tarea>**.

Cómo abrir las propiedades de la tarea de Análisis a pedido

Para abrir las propiedades de la aplicación para la tarea de Análisis a pedido en un solo dispositivo protegido:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en la pestaña **Grupos** para seleccionar el grupo de administración al que pertenece el dispositivo protegido.
3. Haga clic en el nombre del dispositivo protegido.
4. En la ventana **<Nombre del dispositivo>** que se abre, seleccione la pestaña **Tareas**.
5. En la lista de tareas creadas para el dispositivo, seleccione la tarea de Análisis a pedido que creó.
6. Abra la pestaña **Configuración de la aplicación**.

Configuración del área de análisis de la tarea

Para configurar el área de análisis para una tarea de Análisis a pedido existente:

1. Abra las propiedades de la tarea Análisis a pedido.
2. Seleccione la sección **Área del análisis**.
3. Realice una de las siguientes opciones:
   - Haga clic en el botón **Agregar** para agregar una nueva regla.
   - Seleccione una regla existente y haga clic en el botón **Editar**.

   Se abre la ventana **Editar área**.
4. Cambie el botón de alternancia a **Activa** y seleccione un tipo de objeto.
5. En la sección **Protección de objetos**, configure las siguientes opciones:
   - **Modo de protección de objetos**:
     - **Todos los objetos**
     - **Objetos analizados según su formato**
     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**
     - **Objetos analizados según la lista de extensiones especificada**
   - **Subcarpetas**
   - **Subarchivos**
   - **Analizar sectores de inicio del disco y MBR**
   - **Analizar secuencias alternativas de NTFS**

- Proteger solo los archivos nuevos y modificados

6. En la sección **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área de análisis:
   - **Archivos comprimidos**
   - **Archivos SFX**
   - **Objetos empaquetados**
   - **Bases de datos de correo electrónico**
   - **Correo electrónico simple**
   - **Objetos OLE incorporados**
7. En la sección **Acción que se realizará con los objetos infectados y otros objetos**, seleccione la acción que se realizará con los objetos infectados y otros objetos detectados:
   - **Solo notificar**.
   - **Desinfectar**.
   - **Desinfectar; si falla la desinfección, eliminar**Si falla la desinfección, eliminar
   - **Eliminar**.
   - **Recomendado**.
8. En la sección **Acción que se realizará con los objetos probablemente infectados**, seleccione la acción que se realizará sobre estos objetos:
   - **Solo notificar**.
   - **Poner en cuarentena**.
   - **Eliminar**.
   - **Recomendado**.
9. En la sección **Acción que se realizará con los objetos probablemente infectados**, seleccione o desactive la casilla de verificación **Si se detecta un objeto integrado, eliminar todo el archivo compuesto que la aplicación no pueda modificar**.
10. En la sección **Exclusiones**, configure las siguientes opciones:
    - Desactive o seleccione la casilla de verificación **Excluir archivos**.
    - Borre o seleccione la casilla de verificación **No detectar**.
11. En la sección **Configuración avanzada**, configure los siguientes parámetros:
    - **Detener el análisis si demora más de (s)**
    - **No analizar objetos compuestos de más de (MB)**

- **Usar la tecnología iSwift**
- **Usar la tecnología iChecker**

12. En la sección **Acción para los archivos sin conexión**, seleccione la acción a realizar en los archivos:

    - **No analizar**
    - **Analizar solo la parte residente del archivo**
    - **Analizar todo el archivo**

      Si selecciona esta acción, puede determinar las siguientes opciones:

      - Marque o desmarque la casilla de verificación **Solo si se accedió al archivo en el período especificado (días)** e indique el número de días.
      - Marque o desmarque la casilla de verificación **No copiar el archivo al disco duro local (de ser posible)**.

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

Configuración de los parámetros de la tarea

Para configurar los parámetros de una tarea Análisis a pedido existente, realice lo siguiente:

1. Abra las propiedades de la tarea Análisis a pedido.
2. Seleccione la sección **Opciones**.
3. Borre o seleccione la casilla de verificación **Usar el analizador heurístico**.
4. Si es necesario, seleccione el nivel de análisis desde la lista desplegable **Nivel del análisis heurístico**.
5. En la sección **Integración con otros componentes**, configure las siguientes opciones:

    - Seleccione la casilla de verificación **Aplicar zona de confianza** si quiere excluir objetos agregados en la lista de Zona de confianza del área del análisis de la tarea.
    - Seleccione la casilla de verificación **Usar KSN para análisis** si desea usar los servicios en la nube de Kaspersky Security Network para la tarea.
    - Para asignar la prioridad *Baja* al proceso de trabajo en el que se ejecutará la tarea, seleccione la casilla de verificación **Ejecutar tarea en segundo plano**.

      De manera predeterminada, los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security para Windows reciben la prioridad *Media* (Normal).

    - Para utilizar la tarea creada como una tarea Análisis de áreas críticas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas**.

Zona de confianza

Esta sección brinda información sobre la Zona de confianza en Kaspersky Embedded Systems Security para Windows, así como instrucciones sobre cómo agregar objetos a la Zona de confianza al ejecutar tareas.

Acerca de la Zona de confianza

La Zona de confianza es una lista de exclusiones o excepciones al área de protección o de análisis que puede generar y aplicar a las tareas de Análisis a pedido y Protección de archivos en tiempo real, a nuevas tareas de Análisis a pedido personalizadas y a todas las tareas de Análisis a pedido del sistema, excepto por la tarea de Análisis de archivos en cuarentena.

La Zona de confianza se aplica a las tareas de Análisis a pedido y de Protección de archivos en tiempo real de forma predeterminada.

La lista de reglas para generar la Zona de confianza se puede exportar a un archivo de configuración XML para luego importarla a Kaspersky Embedded Systems Security para Windows que se ejecuta en otro dispositivo protegido.

Procesos de confianza

Se aplica a las tareas de Protección de archivos en tiempo real.

Algunas aplicaciones del dispositivo protegido pueden estar inestables si los archivos a los que acceden son interceptados por Kaspersky Embedded Systems Security para Windows. Dichas aplicaciones incluyen, por ejemplo, aplicaciones de controladores de dominio del sistema.

Para evitar la interrupción de la operación de dichas aplicaciones, se puede deshabilitar la protección de los archivos a los que acceden los procesos que se están ejecutando de dichas aplicaciones (se crea así una lista de procesos de confianza dentro de la Zona de confianza).

Microsoft Corporation recomienda excluir algunos archivos del sistema operativo Microsoft Windows y archivos de aplicación de Microsoft de la Protección de archivos en tiempo real como programas que no se pueden infectar. Los nombres de algunos de dichos archivos figuran en el sitio web de Microsoft (código de artículo: KB822158).

Se puede habilitar o deshabilitar el uso de procesos de confianza en la Zona de confianza.

> Si se modifica un archivo ejecutable, por ejemplo, a través de una actualización, Kaspersky Embedded Systems Security para Windows lo excluirá de la lista de procesos de confianza.

La aplicación no utiliza la ruta del archivo en un dispositivo protegido para confiar en el proceso. La ruta al archivo en el dispositivo protegido solo se usa para buscar el archivo, calcular una suma de control y proveer al usuario la información sobre la fuente del archivo ejecutable.

Operaciones de copia de seguridad

Se aplica a las tareas de Protección del equipo en tiempo real.

Cuando se hacen copias de seguridad de los datos almacenados en discos en dispositivos externos, puede deshabilitar la protección de objetos a los que se puede acceder durante las operaciones de copia de seguridad. Kaspersky Embedded Systems Security para Windows analizará los objetos que la aplicación de copia de seguridad abre para la lectura con el atributo FILE_FLAG_BACKUP_SEMANTICS.

Exclusiones

- Se aplica a las tareas de Protección de archivos en tiempo real.
- Todos los objetos detectables en las áreas especificadas del dispositivo protegido.
- Objetos detectables especificados por nombre o máscara del nombre dentro de toda la protección o el área del análisis.

Gestión de la Zona de confianza mediante el Complemento de administración

En esta sección, aprenda cómo navegar a través de la interfaz del Complemento de administración y configurar la Zona de confianza para uno o todos los dispositivos protegidos de la red.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de directivas de la Zona de confianza

Para abrir la Zona de confianza a través de la directiva de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Adicional**.
6. Haga clic en el botón **Configuración** en la subsección **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.

Configure la Zona de confianza según sea necesario.

Si un dispositivo protegido es administrado por una directiva activa de Kaspersky Security Center y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede editar a través de la Consola de la aplicación.

Cómo abrir la ventana de propiedades Zona de confianza

Para configurar la Zona de confianza en la ventana de propiedades de la Aplicación:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del dispositivo protegido.
   - Abra el menú contextual del nombre del dispositivo protegido y seleccione el elemento **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security 3.3 para Windows**.
6. Haga clic en el botón **Propiedades**.

   Se abre la ventana **Configuración de la aplicación Kaspersky Embedded Systems Security 3.3 para Windows**.
7. Seleccione la sección **Adicional**.
8. Haga clic en el botón **Configuración** en la subsección **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.

Configure la Zona de confianza según sea necesario.

Configuración las opciones de la Zona de confianza mediante el Complemento de administración

Para configurar los parámetros de Zona de confianza:

1. En la pestaña **Exclusiones**, especifique qué objetos deberá omitir Kaspersky Embedded Systems Security para Windows cuando se ejecute la tarea.
2. En la pestaña **Procesos de confianza**, especifique qué procesos deberá omitir Kaspersky Embedded Systems Security para Windows cuando se ejecute la tarea.
3. Aplique la máscara de "no es un virus".

Cómo agregar exclusiones

Para agregar una exclusión a la Zona de confianza en la directiva de Kaspersky Security Center:

1. Abra la ventana **Zona de confianza**.
2. En la pestaña **Exclusiones**, especifique los objetos que debe omitir Kaspersky Embedded Systems Security para Windows durante el análisis y la protección:
   - Para crear exclusiones recomendadas, haga clic en el botón Agregar exclusiones recomendadas.
   - Para importar exclusiones preconfiguradas, haga clic en el botón **Importar** y, en la ventana que se abre, seleccione el archivo de configuración en formato XML almacenado en su dispositivo.

     Las exclusiones del archivo XML se agregan a la lista de exclusiones.
   - Para especificar manualmente las condiciones en las cuales un objeto se considerará de confianza, haga clic en el botón **Agregar** y avance a los siguientes pasos.

     Se abre la ventana **Parámetros de la regla de exclusión**.
3. Si hizo clic en el botón **Agregar**, en la sección **El objeto no se analizará si se cumplen las siguientes condiciones**, especifique los objetos que desee excluir del área del análisis o protección y los objetos que desee excluir de los objetos detectables:
   - Si desea excluir un objeto del alcance del análisis o protección:
     a. Seleccione la casilla de verificación **Objeto excluido del análisis**.
     b. Haga clic en el botón **Editar**.

        Se abre la ventana **Objeto que excluir del análisis**.
     c. Especifique el objeto que desea excluir del alcance del análisis.

        > Al especificar los objetos, puede usar máscaras de nombres (mediante los caracteres ? y *) y todo tipo de variables de entorno. Kaspersky Embedded Systems Security para Windows realiza la resolución de las variables del entorno (reemplazar las variables por sus valores) al iniciar una tarea o al aplicar una nueva configuración a una tarea en ejecución (no aplicable a las tareas de Análisis a pedido). Kaspersky Embedded Systems Security para Windows resuelve las variables del entorno en la cuenta utilizada para iniciar la tarea. Para obtener más información sobre las variables del entorno, consulte Microsoft Knowledge Base.

     d. Haga clic en el botón **Aceptar**.
     e. Seleccione la casilla de verificación **Aplicar a subcarpetas**, si desea excluir todos los archivos y carpetas secundarias del objeto especificado del área de la protección o del análisis.
   - Si desea especificar el nombre de un objeto detectable:
     a. Seleccione la casilla de verificación **Objetos excluidos de la detección**.
     b. Haga clic en el botón **Editar**.

        La ventana **Objetos que excluir de la detección** se abre.

c. Especifique el nombre o la máscara del nombre del objeto detectable según la clasificación de la Enciclopedia de Virus.

d. Haga clic en el botón **Agregar**.

e. Haga clic en el botón **Aceptar**.

4. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que se deba aplicar la exclusión.

5. Haga clic en el botón **Aceptar**.

La exclusión se muestra en la lista en la pestaña **Exclusiones** de la ventana **Zona de confianza**.

Agregar procesos de confianza con el Complemento de administración

Para agregar uno o más procesos a la lista de procesos de confianza mediante el Complemento de administración:

1. Abra la ventana **Zona de confianza**.

2. Seleccione la pestaña **Procesos de confianza**.

3. Seleccione la casilla de verificación No analizar las operaciones de copia de seguridad de archivos para omitir el análisis de las operaciones de lectura de archivos.

4. Seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados** para omitir el análisis de las operaciones de archivos para los procesos de confianza.

5. Para agregar procesos a la lista de procesos de confianza, realice una de las siguientes acciones:

   - Para importar procesos de confianza preconfigurados, haga clic en el botón **Importar** y, en la ventana que se abre, seleccione el archivo de configuración en formato XML almacenado en su dispositivo.

     Los procesos del archivo XML se agregan a la lista de procesos de confianza.

   - Para especificar manualmente los procesos, haga clic en el botón **Agregar** y continúe con los siguientes pasos.

6. Si hizo clic en el botón **Agregar**, en el menú contextual del botón, seleccione una de las opciones:

   - **Varios procesos**.

     En la ventana **Agregar procesos de confianza** que se abre, configure lo siguiente:

     a. **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza**.

     b. **Usar hash de archivo de proceso para que se considere de confianza**.

     c. Haga clic en el botón **Examinar** para agregar datos basados en procesos ejecutables.

     d. Seleccione un archivo ejecutable en la ventana que se abre.

     > Solo puede agregar un archivo ejecutable a la vez. Repita los pasos c y d para agregar otros archivos ejecutables.

e. Haga clic en el botón **Procesos** para agregar datos basados en procesos en ejecución.

f. Seleccione los procesos en la ventana que se abre. Para seleccionar varios procesos, mantenga presionado el botón **CTRL** al realizar la selección.

g. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que desee aplicar exclusiones.

h. Haga clic en el botón **Aceptar**.

La cuenta desde la que se ejecuta la tarea de Protección de archivos en tiempo real debe contar con los derechos de administrador en el dispositivo con Kaspersky Embedded Systems Security para Windows instalado con el fin de autorizar la visualización de la lista de procesos activos. Se pueden ordenar los procesos en la lista de procesos activos por nombre de archivo, identificador del proceso (PID) o ruta de acceso al archivo ejecutable del proceso en el dispositivo protegido. Tenga en cuenta que para seleccionar los procesos en ejecución debe hacer clic en el botón **Procesos** usando solo la Consola de la aplicación en un dispositivo protegido o en la configuración de host especificada mediante Kaspersky Security Center.

- **Un proceso según el nombre de archivo y la ruta**.

  En la ventana **Agregar un proceso** que se abre, realice lo siguiente:

  a. Escriba una ruta de acceso a un archivo ejecutable (incluido el nombre de archivo).

  Al especificar los objetos, puede usar máscaras de nombres (mediante los caracteres `?` y `*`) y todo tipo de variables de entorno. Kaspersky Embedded Systems Security para Windows realiza la resolución de las variables del entorno (reemplazar las variables por sus valores) al iniciar una tarea o al aplicar una nueva configuración a una tarea en ejecución (no aplicable a las tareas de Análisis a pedido). Kaspersky Embedded Systems Security para Windows resuelve las variables del entorno en la cuenta utilizada para iniciar la tarea. Para obtener más información sobre las variables del entorno, consulte Microsoft Knowledge Base.

  b. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que desee aplicar exclusiones.

  c. Haga clic en el botón **Aceptar**.

- **Un proceso según las propiedades de los objetos**.

  En la ventana **Adición de proceso de confianza** que se abre, configure lo siguiente:

  a. Haga clic en el botón **Examinar** para seleccionar un proceso.

  b. Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza.

  c. Usar hash del archivo para determinar si el proceso es de confianza.

  d. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que desee aplicar exclusiones.

  e. Haga clic en el botón **Aceptar**.

Para agregar el proceso seleccionado a la lista de procesos de confianza, debe seleccionarse al menos un criterio de confianza.

Si define un proceso como de confianza para la tarea Control de inicio de aplicaciones y crea un paquete de distribución de confianza a partir del archivo ejecutable de ese proceso en la configuración de la tarea, la configuración de la Zona de confianza tendrá prioridad. Kaspersky Embedded Systems Security para Windows considerará que el proceso es de confianza, pero impedirá que se ejecute el archivo ejecutable del proceso.

7. En la ventana **Zona de confianza**, haga clic en el botón **Aceptar**.

El proceso o archivo seleccionado se agregará a la lista de procesos de confianza en la ventana **Zona de confianza**.

Aplicación de la máscara “no es un virus”

La máscara "no es un virus" permite omitir el análisis de archivos de software y recursos web legítimos que pueden considerarse dañinos. La máscara afecta las siguientes tareas:

- Protección de archivos en tiempo real.
- Análisis a pedido.

Si no se agrega la máscara a la lista de exclusiones, Kaspersky Embedded Systems Security para Windows aplicará las acciones especificadas en la configuración de la tarea para el software que caen en esta categoría.

Para aplicar la máscara "no es un virus":

1. Abra la ventana **Zona de confianza**.
2. En la pestaña **Exclusiones**, en la columna **Objetos que detectar**, desplácese en la lista y seleccione la línea con no es un virus:*, si la casilla de verificación no está seleccionada.
3. Haga clic en el botón **Aceptar**.

Se aplica la nueva configuración.

Administración de la Zona de confianza a través de la Consola de la aplicación

En esta sección, aprenda cómo navegar a través de la interfaz de la Consola de la aplicación y configurar la Zona de confianza en un dispositivo protegido.

Cómo aplicar la Zona de confianza a tareas en la Consola de la aplicación

De forma predeterminada, la Zona de confianza se aplica a la tarea de Protección de archivos en tiempo real, las tareas definidas por el usuario de Análisis a pedido creadas recientemente y todas las tareas de Análisis a pedido del sistema, excepto la tarea de Análisis de archivos en cuarentena.

Después de que la Zona de confianza se habilita o deshabilita, las exclusiones especificadas se aplican o dejan de aplicarse inmediatamente a las tareas que se están ejecutando.

Para habilitar o deshabilitar la utilización de la Zona de confianza en las tareas de Kaspersky Embedded Systems Security para Windows:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nombre de la tarea para la cual desea configurar el uso de la Zona de confianza.
2. Seleccione **Propiedades**.

   Aparece la ventana **Configuración de tareas**.
3. En la ventana que se abre, seleccione la pestaña **General** y realice una de las siguientes acciones:
   - Para aplicar la Zona de confianza en la tarea, active la casilla de verificación **Aplicar la Zona de confianza**.
   - Para deshabilitar la Zona de confianza en la tarea, desactive la casilla de verificación **Aplicar la Zona de confianza**.
4. Si desea ajustar la configuración de la Zona de confianza, haga clic en el vínculo del nombre de la casilla de verificación **Aplicar la Zona de confianza**.

   Se abre la ventana **Zona de confianza**.

   En la ventana **Zona de confianza** configure las exclusiones y los procesos de confianza y haga clic en **Aceptar**.
5. Haga clic en el botón **Aceptar** de la ventana **Configuración de tareas** para guardar los cambios.

Configuración de los parámetros de la Zona de confianza en la Consola de la aplicación

Para configurar los parámetros de Zona de confianza:

1. Especifique los objetos para omitir por Kaspersky Embedded Systems Security para Windows durante la ejecución de la tarea en la pestaña **Exclusiones**.
2. Especifique los procesos para omitir por Kaspersky Embedded Systems Security para Windows durante la ejecución de la tarea en la pestaña **Procesos de confianza**.
3. Aplique la Zona de confianza para las tareas de la aplicación.
4. Aplique la máscara de "no es un virus".

Cómo agregar una exclusión a la Zona de confianza

Para agregar manualmente una exclusión a la Zona de confianza a través de la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.

2. Seleccione la opción **Configurar los parámetros de Zona de confianza** del menú.

   Se abre la ventana **Zona de confianza**.

3. Seleccione la pestaña **Exclusiones**.

4. Especifique los objetos que Kaspersky Embedded Systems Security para Windows debe omitir durante el análisis y la protección:

   - Para importar exclusiones preconfiguradas, haga clic en el botón **Importar** y, en la ventana que se abre, seleccione el archivo de configuración en formato XML almacenado en su dispositivo.

     Las exclusiones del archivo XML se agregan a la lista de exclusiones.

   - Para especificar manualmente las condiciones en las cuales un objeto se considerará de confianza, haga clic en el botón **Agregar** y avance a los siguientes pasos.

     Se abre la ventana **Parámetros de la regla de exclusión**.

5. Si hizo clic en el botón **Agregar**, en la sección **El objeto no se analizará si se cumplen las siguientes condiciones**, especifique los objetos que desee excluir del área del análisis o protección y los objetos que desee excluir de los objetos detectables:

   - Si desea excluir un objeto del alcance del análisis o protección:

     a. Seleccione la casilla de verificación **Objeto excluido del análisis**.

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

        Se abre la ventana **Objeto que excluir del análisis**.

     c. Especifique el objeto que desea excluir del alcance del análisis.

        > Al especificar los objetos, puede usar máscaras de nombres (mediante los caracteres ? y *) y todo tipo de variables de entorno. Kaspersky Embedded Systems Security para Windows realiza la resolución de las variables del entorno (reemplazar las variables por sus valores) al iniciar una tarea o al aplicar una nueva configuración a una tarea en ejecución (no aplicable a las tareas de Análisis a pedido). Kaspersky Embedded Systems Security para Windows resuelve las variables del entorno en la cuenta utilizada para iniciar la tarea. Para obtener más información sobre las variables del entorno, consulte Microsoft Knowledge Base.

     d. Haga clic en el botón **Aceptar**.

     e. Seleccione la casilla de verificación **Aplicar a subcarpetas**, si desea excluir todos los archivos y carpetas secundarias del objeto especificado del área de la protección o del análisis.

   - Si desea especificar el nombre de un objeto detectable:

     a. Seleccione la casilla de verificación **Objetos excluidos de la detección**.

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

        La ventana **Objetos que excluir de la detección** se abre.

     c. Especifique el nombre o la máscara del nombre del objeto detectable según la clasificación de la Enciclopedia de Virus.

d. Haga clic en el botón **Agregar**.

e. Haga clic en el botón **Aceptar**.

6. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que se deba aplicar la exclusión.

7. Haga clic en el botón **Aceptar**.

La exclusión se muestra en la lista en la pestaña **Exclusiones** de la ventana **Zona de confianza**.

Agregar procesos de confianza con la Consola de la aplicación

Es posible agregar un proceso a la lista de procesos de confianza mediante uno de los siguientes métodos:

- Seleccionar el proceso de la lista de procesos actualmente en ejecución en el dispositivo protegido.
- Seleccionar el archivo ejecutable de un proceso sin tener en cuenta si el proceso está actualmente en ejecución.

> Si se modificó el archivo ejecutable de un proceso, Kaspersky Embedded Systems Security para Windows excluye este proceso de la lista de procesos de confianza.

Para agregar uno o más procesos a la lista de procesos de confianza mediante la Consola de la aplicación:

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.

2. Seleccione la opción **Configurar los parámetros de Zona de confianza** del menú.

   Se abre la ventana **Zona de confianza**.

3. Seleccione la pestaña **Procesos de confianza**.

4. Seleccione la casilla de verificación **No analizar las operaciones de copia de seguridad de archivos** para omitir el análisis de las operaciones de lectura de archivos.

5. Seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados** para omitir el análisis de las operaciones de archivos para los procesos de confianza.

6. Para agregar procesos a la lista de procesos de confianza, realice una de las siguientes acciones:

   - Para importar procesos de confianza preconfigurados, haga clic en el botón **Importar** y, en la ventana que se abre, seleccione el archivo de configuración en formato XML almacenado en su dispositivo.

     Los procesos del archivo XML se agregan a la lista de procesos de confianza.

   - Para especificar manualmente los procesos, haga clic en el botón **Agregar** y continúe con los siguientes pasos.

7. Si hizo clic en el botón **Agregar**, en el menú contextual del botón, seleccione una de las opciones:

   - **Varios procesos**.

     En la ventana **Agregar procesos de confianza** que se abre, configure lo siguiente:

a. Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza.

b. Usar hash de archivo de proceso para que se considere de confianza.

c. Haga clic en el botón **Examinar** para agregar datos basados en procesos ejecutables.

d. Seleccione un archivo ejecutable en la ventana que se abre.

> Solo puede agregar un archivo ejecutable a la vez. Repita los pasos c y d para agregar otros archivos ejecutables.

e. Haga clic en el botón **Procesos** para agregar datos basados en procesos en ejecución.

f. Seleccione los procesos en la ventana que se abre. Para seleccionar varios procesos, mantenga presionado el botón **CTRL** al realizar la selección.

g. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que desee aplicar exclusiones.

h. Haga clic en el botón **Aceptar**.

> La cuenta desde la que se ejecuta la tarea de Protección de archivos en tiempo real debe contar con los derechos de administrador en el dispositivo con Kaspersky Embedded Systems Security para Windows instalado con el fin de autorizar la visualización de la lista de procesos activos. Se pueden ordenar los procesos en la lista de procesos activos por nombre de archivo, identificador del proceso (PID) o ruta de acceso al archivo ejecutable del proceso en el dispositivo protegido. Tenga en cuenta que para seleccionar los procesos en ejecución debe hacer clic en el botón **Procesos** usando solo la Consola de la aplicación en un dispositivo protegido o en la configuración de host especificada mediante Kaspersky Security Center.

- **Un proceso según el nombre de archivo y la ruta**.

  En la ventana **Agregar un proceso** que se abre, realice lo siguiente:

  a. Escriba una ruta de acceso a un archivo ejecutable (incluido el nombre de archivo).

  > Al especificar los objetos, puede usar máscaras de nombres (mediante los caracteres `?` y `*`) y todo tipo de variables de entorno. Kaspersky Embedded Systems Security para Windows realiza la resolución de las variables del entorno (reemplazar las variables por sus valores) al iniciar una tarea o al aplicar una nueva configuración a una tarea en ejecución (no aplicable a las tareas de Análisis a pedido). Kaspersky Embedded Systems Security para Windows resuelve las variables del entorno en la cuenta utilizada para iniciar la tarea. Para obtener más información sobre las variables del entorno, consulte Microsoft Knowledge Base.

  b. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que desee aplicar exclusiones.

  c. Haga clic en el botón **Aceptar**.

- **Un proceso según las propiedades de los objetos**.

  En la ventana **Adición de proceso de confianza** que se abre, configure lo siguiente:

a. Haga clic en el botón **Examinar** para seleccionar un proceso.

b. **Usar la ruta de acceso completa del proceso en el disco para determinar si el proceso es de confianza**.

c. **Usar hash del archivo para determinar si el proceso es de confianza**.

d. En el bloque **Área de aplicación de exclusión**, seleccione las casillas adyacentes a los nombres de las tareas a las que desee aplicar exclusiones.

e. Haga clic en el botón **Aceptar**.

Para agregar el proceso seleccionado a la lista de procesos de confianza, debe seleccionarse al menos un criterio de confianza.

Si define un proceso como de confianza para la tarea Control de inicio de aplicaciones y crea un paquete de distribución de confianza a partir del archivo ejecutable de ese proceso en la configuración de la tarea, la configuración de la Zona de confianza tendrá prioridad. Kaspersky Embedded Systems Security para Windows considerará que el proceso es de confianza, pero impedirá que se ejecute el archivo ejecutable del proceso.

8. En la ventana **Zona de confianza**, haga clic en el botón **Aceptar**.

El proceso o archivo seleccionado se agregará a la lista de procesos de confianza en la ventana **Zona de confianza**.

Aplicación de la máscara “no es un virus”

La máscara "no es un virus" permite omitir el análisis de archivos de software y recursos web legítimos que pueden considerarse dañinos. La máscara afecta las siguientes tareas:

- Protección de archivos en tiempo real.
- Análisis a pedido.

Si no se agrega la máscara a la lista de exclusiones, Kaspersky Embedded Systems Security para Windows aplicará las acciones especificadas en la configuración de la tarea para el software o los recursos web que caen en esta categoría.

Para aplicar la máscara "no es un virus":

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security para Windows**.
2. Seleccione la opción **Configurar los parámetros de Zona de confianza** del menú.

   Se abre la ventana **Zona de confianza**.
3. Seleccione la pestaña **Exclusiones**.
4. Desplácese por la lista para encontrar el valor *no es un virus:**.

5. Seleccione la casilla de verificación correspondiente si está desactivada.
6. Haga clic en el botón **Aceptar**.

Se aplica la nueva configuración.

Administración de la Zona de confianza mediante el Complemento web

Para administrar la Zona de confianza mediante el Complemento web:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Adicional**.
5. Haga clic en el botón **Configuración** en la subsección **Zona de confianza**.
6. Configure la Zona de confianza según sea necesario.

Prevención de exploits

Esta sección contiene instrucciones sobre cómo configurar las opciones de protección de la memoria del proceso.

Acerca de la prevención de exploits

Kaspersky Embedded Systems Security para Windows proporciona la capacidad de proteger la memoria del proceso de exploits. Esta función se implementa en el componente Prevención de exploits. Puede cambiar el estado de actividad del componente y configurar las opciones de protección de memoria del proceso.

El componente protege la memoria de un proceso contra los exploits a través de un Agente de protección externo ("Agente de protección") insertado en el proceso protegido.

Un Agente de protección de proceso es un módulo de Kaspersky Embedded Systems Security para Windows cargado dinámicamente que se introduce en procesos protegidos para supervisar su integridad y reducir el riesgo de ataques de exploit.

La operación del Agente dentro del proceso protegido requiere iniciar y detener el proceso: la carga inicial del Agente en un proceso agregado a la lista de procesos protegidos solo es posible si el proceso se reinicia. Además, después de que un proceso se elimina de la lista de procesos protegidos, el Agente solo se puede descargar después de que el proceso se reinicie.

El Agente se debe detener para descargarlo de los procesos protegidos: si el componente Prevención de exploits no está instalado, la aplicación congela el entorno y fuerza la descarga del Agente de los procesos protegidos. Si durante la desinstalación del componente se inserta el Agente en alguno de los procesos protegidos, usted debe finalizar el proceso afectado. Es posible que se deba reiniciar el dispositivo protegido (por ejemplo, si el proceso del sistema está protegido).

Si se detectan pruebas de un ataque de exploit en un proceso protegido, Kaspersky Embedded Systems Security para Windows realiza una de las siguientes acciones:

- Finaliza el proceso si se lleva a cabo un intento de ataque de exploit.
- Informa que el proceso se ha puesto en peligro.

Puede detener la protección del proceso con uno de los siguientes métodos:

- Desinstalación del componente.
- Eliminación del proceso de la lista de procesos protegidos y reinicio del proceso.

Servicio de Kaspersky Security Exploit Prevention

Se requiere el servicio de Kaspersky Security Exploit Prevention en el dispositivo protegido para que el componente Prevención de exploits sea más efectivo. Este servicio y el componente Prevención de exploits son parte de la instalación recomendada. Durante la instalación del servicio en el dispositivo protegido, se crea y se inicia el proceso kavfswh. Esto comunica la información sobre los procesos protegidos del componente al Agente de protección.

Después de que el servicio de Kaspersky Security Exploit Prevention se detiene, Kaspersky Embedded Systems Security para Windows continúa protegiendo los procesos agregados a la lista de procesos protegidos, y también se carga en procesos agregados recientemente y se aplican todas las técnicas de prevención de exploits disponibles para proteger la memoria del proceso.

Si su dispositivo ejecuta el sistema operativo Windows 10 o posterior, la aplicación no continuará protegiendo los procesos y la memoria del proceso una vez que se haya detenido el servicio de Kaspersky Security Exploit Prevention.

Si el servicio de Kaspersky Security Exploit Prevention se detiene, la aplicación no recibirá información sobre eventos que ocurren con procesos protegidos (incluida información sobre ataques de exploits y cancelación de procesos). Además, el Agente no podrá recibir la información sobre la configuración de protección nueva y la adición de procesos nuevos a la lista de procesos protegidos.

Modo de Prevención de exploits

Puede seleccionar uno de los modos siguientes para configurar acciones tomadas para reducir los riesgos de que las vulnerabilidades sufran ataques de exploits en procesos protegidos:

- **Finalizar en caso de exploit**: aplique este modo para cancelar un proceso cuando se lleva a cabo un intento de exploit.

  Cuando se detecta un intento de realizar un ataque de exploit en una vulnerabilidad de un proceso del sistema operativo crítico protegido, Kaspersky Embedded Systems Security para Windows no cancela el proceso, independientemente del modo indicado en la configuración del componente Prevención de exploits.

- **Solo notificar**: aplique este modo para recibir la información sobre casos de exploits en procesos protegidos mediante eventos en el registro de seguridad.

  Si selecciona este modo, Kaspersky Embedded Systems Security para Windows crea eventos para registrar todos los intentos de realizar un ataque de exploit en vulnerabilidades. Seleccionado por defecto.

Gestión de Prevención de exploits a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración del componente para uno o todos los dispositivos protegidos en la red.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración de la directiva para Prevención de exploits

Para abrir la configuración de Prevención de exploits a través de la directiva de Kaspersky Security Center:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas**.
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Protección del equipo en tiempo real**.
6. Haga clic en **Configuración** en la subsección **Prevención de exploits**.

   Se abre la ventana **Prevención de exploits**.

Configure Prevención de exploits como sea necesario.

Cómo abrir la ventana de propiedades Prevención de exploits

Para abrir la ventana de propiedades de Prevención de exploits:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del dispositivo protegido>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del dispositivo protegido.
   - Abra el menú contextual del nombre del dispositivo protegido y seleccione el elemento **Propiedades**.

   Se abre la ventana **Propiedades: <Nombre del dispositivo protegido>**.
5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security 3.3 para Windows**.
6. Haga clic en el botón **Propiedades**.

   Se abre la ventana **Configuración de la aplicación Kaspersky Embedded Systems Security 3.3 para Windows**.
7. Seleccione la sección **Protección del equipo en tiempo real**.
8. Haga clic en **Configuración** en la subsección **Prevención de exploits**.

   Se abre la ventana **Prevención de exploits**.

Configure Prevención de exploits como sea necesario.

Configuración de protección de memoria del proceso

Para configurar los ajustes de Prevención de exploits para los procesos agregados a la lista de procesos protegidos, realice las siguientes acciones:

1. Abra la ventana **Prevención de exploits**.
2. En el bloque **Modo de prevención de exploits**, configure las siguientes opciones:
   - **Prevenir exploit de procesos vulnerables**.
     - **Finalizar en caso de exploit**.
     - **Solo notificar**.
3. En el bloque **Acciones de prevención**, configure las siguientes opciones:
   - **Notificar sobre los procesos abusados a través de Terminal Service**.
   - **Prevenir exploit de procesos vulnerables, incluso si el servicio de Kaspersky Security está deshabilitado**.
4. Haga clic en el botón **Aceptar** de la ventana **Prevención de exploits**.

Kaspersky Embedded Systems Security para Windows guarda y aplica las opciones de protección de memoria del proceso configuradas.

Cómo agregar un proceso al área de la protección

El componente Prevención de exploits protege varios procesos de forma predeterminada. Para excluir los procesos del área de protección, desactive las casillas correspondientes en la lista.

Para agregar un proceso a la lista de procesos protegidos:

1. Abra la ventana **Prevención de exploits**.
2. En la pestaña **Procesos protegidos**, haga clic en el botón **Examinar**.
   Se abre una ventana del Explorador de Microsoft Windows.
3. Seleccione el proceso que desea agregar a la lista.
4. Haga clic en el botón **Abrir**.
   Se muestra el nombre de proceso en la línea.
5. Haga clic en el botón **Agregar**.
   El proceso se añadirá a la lista de procesos protegidos.
6. Seleccione el proceso agregado.
7. Haga clic en el botón **Configurar técnicas de prevención de exploits**.
   Se abre la ventana **Técnicas de prevención de exploits**.

8. Seleccione una de las opciones para aplicar técnicas de reducción de impacto:

   - **Aplicar todas las técnicas de prevención de exploits disponibles**.

     Si se selecciona esta opción, la lista no se puede modificar. De forma predeterminada, todas las técnicas disponibles se aplican a un proceso.

   - **Aplicar las técnicas de prevención de exploits seleccionadas**

     Si esta opción se selecciona, puede modificar la lista de técnicas de reducción de impacto aplicadas:

     a. Seleccione las casillas al lado de las técnicas que desea aplicar para proteger el proceso seleccionado.

     b. Seleccione o desactive la casilla de verificación **Aplicar técnica de Reducción de la superficie de ataque**.

9. Configure las opciones de la Técnica de reducción de la superficie de ataque:

   - Ingrese los nombres de los módulos cuyo inicio se bloqueará desde el proceso protegido en el campo **Denegar módulos**.

   - En el campo **No denegar módulos si se cargan en la zona de Internet**, seleccione las casillas de verificación al lado de las opciones para las cuales desea permitir que se inicien los módulos:

     - **Internet**
     - **Intranet local**
     - **URL de confianza**
     - **URL restringida**
     - **Equipo**

     Esta configuración solo se aplica a Internet Explorer®.

10. Haga clic en el botón **Aceptar**.

    El proceso se añade al área de protección de la tarea.

Gestión de Prevención de exploits a través de la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y establecer la configuración del componente en un dispositivo protegido.

Navegación

Obtenga información sobre cómo dirigirse a la configuración de la tarea requerida a través de la interfaz que elija.

Cómo abrir la configuración general de Prevención de exploits

*Para abrir la ventana **Ajustes de prevención de exploits**:*

1. Expanda el nodo **Protección de archivos en tiempo real** en el árbol de la Consola de la aplicación.
2. Seleccione el nodo **Prevención de exploits**.
3. En la sección **Configuración de protección de los procesos**, haga clic en el vínculo **Propiedades**.
   Se abre la ventana **Ajustes de prevención de exploits**.

Ajuste la configuración general para Prevención de exploits como sea necesario.

Cómo abrir la configuración de protección de procesos de Prevención de exploits

*Para abrir la ventana **Configuración de protección de los procesos**, realice lo siguiente:*

1. Expanda el nodo **Protección de archivos en tiempo real** en el árbol de la Consola de la aplicación.
2. Seleccione el nodo **Prevención de exploits**.
3. En la sección **Configuración de protección de los procesos**, haga clic en el vínculo **Parámetros de protección de los procesos**.
   Se abre la ventana **Configuración de protección de los procesos**.
4. Ajuste la configuración de protección de procesos para Prevención de exploits como sea necesario.

Configuración de protección de memoria del proceso

Para agregar un proceso a la lista de procesos protegidos:

1. Abra la ventana **Ajustes de prevención de exploits**.
2. En el bloque **Modo de prevención de exploits**, configure las siguientes opciones:
   - **Prevenir exploit de procesos vulnerables**.
     - **Finalizar en caso de exploit**.
     - **Solo notificar**.
3. En el bloque **Acciones de prevención**, configure las siguientes opciones:
   - **Notificar sobre los procesos abusados a través de Terminal Service**.
   - **Prevenir exploit de procesos vulnerables, incluso si el servicio de Kaspersky Security está deshabilitado**.

4. Haga clic en el botón **Aceptar** de la ventana **Ajustes de prevención de exploits**.

Kaspersky Embedded Systems Security para Windows guarda y aplica las opciones de protección de memoria del proceso configuradas.

Cómo agregar un proceso al área de la protección

El componente Prevención de exploits protege varios procesos de forma predeterminada. Puede desmarcar los procesos que no desea proteger en la lista de procesos protegidos.

Para agregar un proceso a la lista de procesos protegidos:

1. Abra la ventana **Configuración de protección de los procesos**.
2. Para agregar un proceso para protegerlo de abuso y reducir el impacto potencial de exploits, realice las siguientes acciones:
   a. Haga clic en el botón **Examinar**.
      Se abre la ventana estándar **Abrir** de Microsoft Windows.
   b. En la ventana que se abre, seleccione el proceso que quiere añadir a la lista.
   c. Haga clic en el botón **Abrir**.
   d. Haga clic en el botón **Agregar**.
      El proceso se añadirá a la lista de procesos protegidos.
3. Seleccione un proceso de la lista.
4. La configuración actual se muestra en la pestaña **Configuración de protección de los procesos**:
   - **Nombre del proceso**.
   - **En ejecución**.
   - **Se aplicaron técnicas de prevención de exploits**.
   - **Configuración de la Reducción de la superficie de ataque**.
5. Para modificar las técnicas de prevención de exploits que se aplican al proceso, seleccione la pestaña **Denegar carga de módulos**.
6. Seleccione una de las opciones para aplicar técnicas de reducción de impacto:
   - **Aplicar todas las técnicas de prevención de exploits disponibles**.
     Si se selecciona esta opción, la lista no se puede modificar. De forma predeterminada, todas las técnicas disponibles se aplican a un proceso.
   - **Aplicar las técnicas de prevención de exploits disponibles de la lista para el proceso**.
     Si esta opción se selecciona, puede modificar la lista de técnicas de reducción de impacto aplicadas:
     a. Seleccione las casillas al lado de las técnicas que desea aplicar para proteger el proceso seleccionado.

7. Configure las opciones de la Técnica de reducción de la superficie de ataque:

   - En el campo **Denegar módulos**, ingrese los nombres de los módulos que no se podrán iniciar desde el proceso protegido.
   - En la sección **No denegar módulos si se cargan en la zona de Internet**, seleccione las casillas de verificación al lado de las opciones para las cuales desee permitir que se inicien los módulos:
     - **Internet**
     - **Intranet local**
     - **URL de confianza**
     - **Sitios restringidos**
     - **Equipo**

   Esta configuración solo se aplica a Internet Explorer®.

8. Haga clic en el botón **Guardar**.

El proceso se añade al área de protección de la tarea.

Administración de Prevención de exploits a través del Complemento web

En esta sección, aprenda a navegar la interfaz del Complemento web y establecer la configuración del componente en un dispositivo protegido.

Configuración de protección de memoria del proceso

Para configurar los ajustes de Prevención de exploits para los procesos agregados a la lista de procesos protegidos, realice las siguientes acciones:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Protección del equipo en tiempo real**.
5. Haga clic en **Configuración** en la subsección **Prevención de exploits**.
6. Abra la pestaña **Ajustes de prevención de exploits**.
7. En el bloque **Modo de prevención de exploits**, configure las siguientes opciones:
   - Prevenir exploit de procesos vulnerables.

- Finalizar en caso de exploit.
- Solo notificar.

8. En el bloque **Acciones de prevención**, configure las siguientes opciones:
   - Notificar sobre los procesos abusados a través de Terminal Service.
   - Prevenir exploit de procesos vulnerables, incluso si el servicio de Kaspersky Security está deshabilitado.
9. Haga clic en el botón **Aceptar** de la ventana **Prevención de exploits**.

Kaspersky Embedded Systems Security para Windows guarda y aplica las opciones de protección de memoria del proceso configuradas.

Cómo agregar un proceso al área de la protección

Para configurar los ajustes de Prevención de exploits para los procesos agregados a la lista de procesos protegidos, realice las siguientes acciones:

1. En la ventana principal de Kaspersky Security Center Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva que desea configurar.
3. En la ventana **<Nombre de la directiva>** que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Protección del equipo en tiempo real**.
5. Haga clic en **Configuración** en la subsección **Prevención de exploits**.
6. Abra la pestaña **Procesos protegidos**.
7. Haga clic en el botón **Agregar**.
8. Se abre la ventana **Técnicas de prevención de exploits**.
9. Especifique el nombre del proceso.
10. Seleccione una de las opciones para aplicar técnicas de reducción de impacto:
    - **Aplicar todas las técnicas de prevención de exploits disponibles**.

      Si se selecciona esta opción, la lista no se puede modificar. De forma predeterminada, todas las técnicas disponibles se aplican a un proceso.
    - **Aplicar las técnicas de prevención de exploits seleccionadas**

      Si esta opción se selecciona, puede modificar la lista de técnicas de reducción de impacto aplicadas:

      a. Seleccione las casillas al lado de las técnicas que desea aplicar para proteger el proceso seleccionado.

      b. Seleccione o desactive la casilla de verificación **Aplicar técnica de Reducción de la superficie de ataque**.

11. Configure las opciones de la Técnica de reducción de la superficie de ataque:

    - Ingrese los nombres de los módulos cuyo inicio se bloqueará desde el proceso protegido en el campo **Denegar módulos**.
    - En el campo **No denegar módulos si se cargan en la zona de Internet**, seleccione las casillas de verificación al lado de las opciones para las cuales desea permitir que se inicien los módulos:
        - **Internet**
        - **Intranet local**
        - **URL de confianza**
        - **URL restringida**
        - **Equipo**

    Esta configuración solo se aplica a Internet Explorer®.

12. Haga clic en el botón **Aceptar**.

El proceso se añade al área de protección de la tarea.

Técnicas de prevención de exploits

Técnicas de prevención de exploits

Técnica de prevención de exploits	Descripción
Prevención de ejecución de datos (DEP)	La prevención de ejecución de datos bloquea la ejecución del código arbitrario en áreas protegidas de la memoria.
Randomización del diseño del espacio de direcciones (ASLR)	Cambia el diseño de estructuras de datos en el espacio de direcciones del proceso.
Protección de sobrescritura del controlador de excepciones estructuradas (SEHOP)	Reemplazo de registros de excepciones o reemplazo del controlador de excepciones.
Ubicación de página nula	Prevención de desvío el indicador nulo
Verificación de llamada de la red de LoadLibrary (anti-ROP)	Protección contra DLL de carga desde rutas de la red.
Pilas ejecutables (anti ROP)	Bloqueo de ejecución no autorizada de áreas de las pilas.
Verificación anti RET (anti ROP)	Compruebe que la instrucción de LLAMADA se invoque de manera segura.
Anti traslado de pilas (anti ROP)	La Protección contra el traslado de indicadores de pilas de ESP a una dirección ejecutable.
Monitor de acceso a la función exportar tabla de direcciones simple (Monitor de acceso a EAT y Monitor de acceso a EAT mediante el registro de depuraciones)	Protección de acceso de lectura a la función exportar tabla de direcciones para kernel32.dll, kernelbase.dll y ntdll.dll.
Asignación de Heap Spray (Heapspray)	Protección contra asignación de memoria para ejecutar

	código malicioso.
Simulación del flujo de ejecución (programación orientada a la antidevolución)	Detección de cadenas potencialmente peligrosas de instrucciones (posible gadget ROP) en el componente API de Windows.
Monitor de llamada de IntervalProfiler (Protección del controlador funcional auxiliar [AFDP])	Protección contra elevación de privilegios a través de una vulnerabilidad en el controlador AFD (ejecución de código arbitrario en anillo 0 a través de una llamada de QueryIntervalProfile).
Reducción de la superficie de ataque (ASR)	Bloqueo del inicio de complementos automáticos vulnerables mediante el proceso protegido.
Hollowing antiproceso (Hollowing)	Protección contra creación y ejecución de copias maliciosas de procesos de confianza.
Anti AtomBombing (APC)	Exploit de la tabla de atom global mediante llamadas de procedimiento asíncronas (APC).
Anti CreateRemoteThread (RThreadLocal)	Otro proceso ha creado un subproceso en el proceso protegido.
Anti CreateRemoteThread (RThreadRemote)	El proceso protegido ha creado un subproceso en otro proceso.

Integración con sistemas de terceros

Esta sección describe la integración de Kaspersky Embedded Systems Security para Windows con funciones y tecnologías de terceros.

Contadores de rendimiento para el supervisor del sistema

Esta sección contiene información sobre contadores de rendimiento para el supervisor del sistema de Microsoft Windows que Kaspersky Embedded Systems Security para Windows registra durante la instalación.

Acerca de los contadores de rendimiento de Kaspersky Embedded Systems Security para Windows

"Contadores de rendimiento" es un componente de Kaspersky Embedded Systems Security para Windows que puede usar para supervisar el rendimiento de la aplicación durante la ejecución de las tareas de protección del equipo en tiempo real. Puede identificar cuellos de botella cuando se ejecuta con otras aplicaciones y escasez de recursos. Puede diagnosticar cuando se interrumpe Kaspersky Embedded Systems Security para Windows e identificar una configuración no deseada.

Puede ver los contadores de rendimiento de Kaspersky Embedded Systems Security para Windows si abre la consola **Rendimiento** en la sección **Administración** del Panel de control de Windows.

Las siguientes secciones enumeran definiciones de contadores, intervalos recomendados para obtener lecturas, valores de umbral y ajustes recomendados de Kaspersky Embedded Systems Security para Windows si los valores del contador superan los umbrales.

Cantidad total de solicitudes denegadas

Cantidad total de solicitudes denegadas

Nombre	Cantidad total de solicitudes denegadas
Definición	Cantidad total de solicitudes de procesamiento de objetos realizadas por el controlador de interceptación de archivos y rechazadas por los procesos de la aplicación, obtenida desde el último inicio de Kaspersky Embedded Systems Security para Windows. La aplicación omite objetos para los cuales las solicitudes de procesamiento son denegadas por procesos de Kaspersky Embedded Systems Security para Windows.
Objetivo	Este contador puede ayudarlo a detectar: • Reducción de la Protección del equipo en tiempo real debido a la sobrecarga de los procesos de Kaspersky Embedded Systems Security para Windows. • Interrupción de la Protección del equipo en tiempo real debido a fallas de los distribuidores para la interceptación de archivos.
Valor umbral/ normal	0/1
Intervalo de	1 hora.

lectura recomendado	
Recomendaciones para la configuración si el valor supera el umbral	La cantidad de solicitudes del proceso denegadas corresponde a la cantidad de objetos omitidos. Las siguientes situaciones son posibles según el comportamiento del contador: • El contador muestra varias solicitudes denegadas durante un período extendido: todos los procesos de Kaspersky Embedded Systems Security para Windows se cargan totalmente para que Kaspersky Embedded Systems Security para Windows no pueda analizar objetos. Para evitar que se omitan objetos, aumente el número de procesos de la aplicación para las tareas de Protección del equipo en tiempo real. A tal fin, puede usar ajustes de Kaspersky Embedded Systems Security para Windows como **Número de procesos para la protección en tiempo real**. • La cantidad de solicitudes denegadas supera de manera considerable el umbral crítico y aumenta rápidamente: el distribuidor para la interceptación de archivos dejó de funcionar. Kaspersky Embedded Systems Security para Windows no analiza los objetos cuando obtiene acceso a ellos. Reinicie Kaspersky Embedded Systems Security para Windows.

Cantidad total de solicitudes omitidas

Cantidad total de solicitudes omitidas

Nombre	Cantidad total de solicitudes omitidas
Definición	La cantidad total de solicitudes de procesamiento de objetos realizadas por el controlador de interceptación de archivos que recibió Kaspersky Embedded Systems Security para Windows y no generaron eventos que indiquen la finalización del procesamiento. Esta cantidad se cuenta desde el momento en que la aplicación se inició por última vez. Si una solicitud de procesamiento de objetos es aceptada por uno de los procesos de trabajo, pero no envía un evento que indique la finalización del procesamiento, el controlador transferirá la solicitud a otro proceso y el valor del contador **Cantidad total de solicitudes omitidas** aumentará a 1. Si el controlador revisó todos los procesos de trabajo y ningún de ellos aceptó la solicitud de procesamiento (por estar ocupados) ni envió ningún evento que indique la finalización del procesamiento, Kaspersky Embedded Systems Security para Windows omitirá el objeto y el valor del contador **Cantidad total de solicitudes omitidas** aumentará a 1.
Objetivo	Este contador le permite detectar bajas en el rendimiento debido a fallas de los distribuidores para la interceptación de archivos.
Valor umbral/ normal	0/1
Intervalo de lectura recomendado	1 hora.
Recomendaciones para la configuración si el valor supera el umbral	Si el contador es distinto de cero, significa que uno o más flujos del distribuidor para la interceptación de archivos está interrumpido y no funciona. El valor del contador corresponde a la cantidad de flujos actualmente inactivos. Si la velocidad del análisis no es satisfactoria, reinicie Kaspersky Embedded Systems Security para Windows a fin de restaurar los flujos fuera de línea.

Cantidad de solicitudes sin procesar por falta de recursos del sistema

Cantidad de solicitudes sin procesar por falta de recursos del sistema

Nombre	Cantidad de solicitudes sin procesar debido a una falta de recursos.
Definición	Cantidad total de solicitudes del controlador de interceptación de archivos que no se procesaron por falta de recursos del sistema (por ejemplo, de memoria RAM), calculada desde el último inicio de Kaspersky Embedded Systems Security para Windows. Kaspersky Embedded Systems Security para Windows omite las solicitudes de procesamiento de objetos que no están procesadas por el controlador de interceptación de archivos.
Objetivo	Este contador se puede usar para detectar y eliminar una posible menor calidad de la Protección del equipo en tiempo real que se produce debido a una baja de recursos del sistema.
Valor umbral/ normal	0/1
Intervalo de lectura recomendado	1 hora.
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador no es cero, los procesos en ejecución de Kaspersky Embedded Systems Security para Windows necesitarán más RAM para procesar solicitudes. Es posible que los procesos activos de otras aplicaciones estén usando toda la memoria RAM disponible.

Cantidad de solicitudes enviadas para su proceso

Cantidad de solicitudes enviadas para su proceso

Nombre	Cantidad de solicitudes enviadas para su proceso.
Definición	La cantidad de objetos que esperan ser procesados por los procesos de trabajo.
Objetivo	Este contador se puede usar para supervisar la carga de los procesos de trabajo de Kaspersky Embedded Systems Security para Windows y el nivel general de la actividad de los archivos en el dispositivo protegido.
Valor umbral/ normal	El contador puede variar según el nivel de la actividad de los archivos en el dispositivo protegido.
Intervalo de lectura recomendado	1 minuto.
Recomendaciones para la configuración si el valor supera el umbral	N/D

Cantidad promedio de flujos del distribuidor para la interceptación de archivos

Cantidad promedio de flujos del distribuidor para la interceptación de archivos

Nombre	Cantidad promedio de flujos del distribuidor para la interceptación de archivos.
Definición	La cantidad de flujos del distribuidor para la interceptación de archivos en un proceso y el promedio de todos los procesos actualmente involucrados en las tareas de Protección del equipo en tiempo real.
Objetivo	Este contador se puede usar para detectar y eliminar una posible reducción de la Protección del equipo en tiempo real debido a una carga completa en los procesos de Kaspersky Embedded Systems Security para Windows.
Valor umbral/ normal	Varía / 40
Intervalo de lectura recomendado	1 minuto.
Recomendaciones para la configuración si el valor supera el umbral	Se pueden crear hasta 60 flujos del distribuidor para la interceptación de archivos en cada proceso de trabajo. Si el contador se acerca a 60, existe el riesgo de que ninguno de los procesos de trabajo pueda procesar la solicitud siguiente en la cola del controlador de interceptación de archivos y Kaspersky Embedded Systems Security para Windows omita el objeto. Aumente la cantidad de procesos de Kaspersky Embedded Systems Security para Windows para las tareas de Protección del equipo en tiempo real. A tal fin, puede usar ajustes de Kaspersky Embedded Systems Security para Windows como **Número de procesos para la protección en tiempo real**.

Cantidad máxima de flujos del distribuidor para la interceptación de archivos

Cantidad máxima de flujos del distribuidor para la interceptación de archivos

Nombre	Cantidad máxima de flujos del distribuidor para la interceptación de archivos.
Definición	La cantidad de flujos del distribuidor para la interceptación de archivos en un proceso y la cantidad máxima de todos los procesos actualmente involucrados en las tareas de Protección del equipo en tiempo real.
Objetivo	Este contador le permite detectar y eliminar bajas de rendimiento debido a una distribución de cargas dispar en los procesos en ejecución.
Valor umbral/ normal	Varía / 40
Intervalo de lectura recomendado	1 minuto.
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador supera de manera considerable y continua el contador **Cantidad promedio de flujos de distribuidor para la interceptación de archivos**, Kaspersky Embedded Systems Security para Windows está distribuyendo la carga para los procesos en ejecución de manera dispar. Reinicie Kaspersky Embedded Systems Security para Windows.

Cantidad de elementos en la cola de objetos infectados

Cantidad de elementos en la cola de objetos infectados

Nombre	Cantidad de elementos en la cola de objetos infectados.
Definición	Cantidad de objetos infectados que actualmente esperan ser procesados (desinfectados o eliminados).
Objetivo	Este contador puede ayudarlo a detectar: • Interrupción de la Protección del equipo en tiempo real debido a fallas potenciales de los distribuidores para la interceptación de archivos. • Sobrecarga de procesos debido a una distribución dispar del tiempo del procesador entre diferentes procesos de trabajo y Kaspersky Embedded Systems Security para Windows. • Ataques de virus.
Valor umbral/ normal	Este valor puede ser distinto de cero mientras Kaspersky Embedded Systems Security para Windows procesa objetos infectados o probablemente infectados, pero regresará a cero cuando el procesamiento haya finalizado./El valor se mantiene distinto de cero durante un período prolongado.
Intervalo de lectura recomendado	1 minuto.
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador no regresa a cero durante un periodo prolongado: • Kaspersky Embedded Systems Security para Windows no está procesando objetos (es posible que se haya interrumpido el distribuidor para la interceptación de archivos); Reinicie Kaspersky Embedded Systems Security para Windows. • Puede que no haya suficiente tiempo del procesador para procesar los objetos. Asegúrese de que Kaspersky Embedded Systems Security para Windows reciba tiempo adicional del procesador (por ejemplo, reduzca la carga de otras aplicaciones en el dispositivo protegido). • Se produjo un brote de virus. Una gran cantidad de objetos infectados o probablemente infectados en la tarea de Protección de archivos en tiempo real es también un signo de un brote de virus. Puede consultar la información sobre el número de objetos detectados en las estadísticas de la tarea o los registros de tareas.

Cantidad de objetos procesados por segundo

Cantidad de objetos procesados por segundo

Nombre	Cantidad de objetos procesados por segundo.
Definición	Cantidad de objetos procesados dividida por la cantidad de tiempo empleado para procesar esos objetos (calculada durante intervalos de tiempo idénticos).
Objetivo	Este contador refleja la velocidad de procesamiento de objetos. Se puede usar para detectar y eliminar niveles bajos de rendimiento del dispositivo protegido que se producen debido a que el procesador asigna tiempo insuficiente a los procesos de Kaspersky Embedded Systems Security para Windows o debido a errores en la operación de Kaspersky Embedded Systems Security para Windows.
Valor umbral/	Varía / n.°

normal	
Intervalo de lectura recomendado	1 minuto.
Recomendaciones para la configuración si el valor supera el umbral	Los valores de este contador dependen de los valores establecidos en la configuración de Kaspersky Embedded Systems Security para Windows y de la carga de procesos de otras aplicaciones en el dispositivo protegido. Observe el valor promedio de contador durante un periodo prolongado. El valor promedio del contador puede reducirse en las siguientes situaciones: • Los procesos de Kaspersky Embedded Systems Security para Windows no disponen del tiempo del procesador necesario para procesar los objetos. Asegúrese de que Kaspersky Embedded Systems Security para Windows reciba tiempo adicional del procesador (por ejemplo, reduzca la carga de otras aplicaciones en el dispositivo protegido). • Kaspersky Embedded Systems Security para Windows experimentó un error (varios flujos están inactivos). Reinicie Kaspersky Embedded Systems Security para Windows.

Contadores y capturas SNMP de Kaspersky Embedded Systems Security para Windows

Esta sección contiene información sobre contadores y capturas de Kaspersky Embedded Systems Security para Windows.

Acerca de contadores y capturas SNMP de Kaspersky Embedded Systems Security para Windows

Si se incluyeron Contadores y capturas SNMP en el conjunto de componentes Antivirus para instalar, puede ver contadores y capturas de Kaspersky Embedded Systems Security para Windows a través del Protocolo simple de administración de redes (SNMP).

Para ver los contadores y las capturas de Kaspersky Embedded Systems Security para Windows desde la estación de trabajo del administrador, inicie el servicio SNMP en el dispositivo protegido e inicie los servicios de capturas SNMP en la estación de trabajo del administrador.

Contadores SNMP de Kaspersky Embedded Systems Security para Windows

Esta sección contiene tablas con una descripción de la configuración para los contadores SNMP de Kaspersky Embedded Systems Security para Windows.

Contadores de rendimiento

Contadores de rendimiento

Contador	Definición
currentRequestsAmount	Cantidad de solicitudes enviadas para su proceso
currentInfectedQueueLength	Cantidad de elementos en la cola de objetos infectados
currentObjectProcessingRate	Cantidad de objetos procesados por segundo
currentWorkProcessesNumber	Cantidad actual de procesos de trabajo utilizados por Kaspersky Embedded Systems Security para Windows

Contadores de cuarentena

Contadores de cuarentena

Contador	Definición
totalObjects	Cantidad de objetos que se encuentran actualmente en cuarentena
totalSuspiciousObjects	Cantidad de objetos probablemente infectados que se encuentran actualmente en cuarentena
currentStorageSize	Cantidad total de datos en cuarentena (MB)

Contador de Copia de seguridad

Contador de Copia de seguridad

Contador	Definición
currentBackupStorageSize	Cantidad total de datos en copia de seguridad (MB)

Contadores generales

Contadores generales

Contador	Definición
lastCriticalAreasScanAge	El periodo desde el último análisis completo de las áreas críticas del dispositivo protegido (tiempo transcurrido en segundos desde que se completó la última tarea de Análisis de áreas críticas).
licenseExpirationDate	Fecha de caducidad de la licencia. Si se ha agregado una clave activa y una clave adicional, se muestra la fecha de caducidad de la licencia asociada con la clave adicional.
currentApplicationUptime	Cantidad de tiempo que Kaspersky Embedded Systems Security para Windows ha estado en ejecución desde su último inicio, en centésimos de segundos.

Contador de actualización

Contador de actualización

Contador	Definición

avBasesAge	"Antigüedad" de las bases de datos (tiempo transcurrido en centésimos de segundos desde la fecha de creación de las últimas actualizaciones instaladas de las bases de datos).

Contadores de protección de archivos en tiempo real

Contadores de protección de archivos en tiempo real

Contador	Definición
totalObjectsProcessed	Cantidad total de objetos analizados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalInfectedObjectsFound	Cantidad total de Objetos infectados y otros objetos detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalSuspiciousObjectsFound	Cantidad total de Objetos probablemente infectados detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalVirusesFound	Cantidad total de objetos detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalObjectsQuarantined	Cantidad total de objetos infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security para Windows colocó en cuarentena; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotQuarantined	Cantidad total de objetos infectados o probablemente infectados que Kaspersky Embedded Systems Security para Windows intentó poner en cuarentena, pero no pudo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsDisinfected	Cantidad total de objetos infectados que Kaspersky Embedded Systems Security para Windows desinfectó; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotDisinfected	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security para Windows intentó desinfectar, pero no pudo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsDeleted	Cantidad total de objetos infectados, objetos probablemente infectados y otros objetos que Kaspersky Embedded Systems Security para Windows eliminó; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotDeleted	Cantidad total de objetos probablemente infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security para Windows intentó eliminar, pero no pudo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsBackedUp	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security para Windows colocó en Copia de seguridad; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotBackedUp	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security para Windows intentó colocar en Copia de seguridad, pero no pudo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez

Capturas SNMP de Kaspersky Embedded Systems Security para Windows y sus opciones

A continuación, se resumen las opciones de capturas SNMP en Kaspersky Embedded Systems Security para Windows:

- eventThreatDetected: se ha detectado un objeto.

  La captura tiene las siguientes opciones:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: se superó el tamaño máximo de Copia de seguridad. La cantidad total de los datos en Copia de seguridad supera el valor especificado por el **Tamaño máx. de Copia de seguridad (MB)**. Kaspersky Embedded Systems Security para Windows continúa realizando copias de seguridad de objetos infectados.

  La captura tiene las siguientes opciones:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: umbral de espacio disponible para la copia de seguridad alcanzado. La cantidad de espacio libre en Copia de seguridad es menor o igual que el valor especificado por **Valor umbral de espacio disponible (MB)**. Kaspersky Embedded Systems Security para Windows continúa realizando copias de seguridad de objetos infectados.

  La captura tiene las siguientes opciones:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: se superó el tamaño máximo de la cuarentena. El tamaño total de los datos en Cuarentena ha superado el valor especificado por el **Tamaño máximo de cuarentena (MB)**. Kaspersky

Embedded Systems Security para Windows continúa poniendo en cuarentena objetos probablemente infectados.

La captura tiene las siguientes opciones:

- eventDateAndTime
- eventSeverity
- eventSource

- eventThresholdQuarantineStorageSizeExceeds: umbral de espacio disponible para Cuarentena alcanzado. La cantidad de espacio libre en Cuarentena asignado por el **Valor umbral de espacio disponible (MB)** es igual o menor que el valor especificado. Kaspersky Embedded Systems Security para Windows continúa realizando copias de seguridad de objetos infectados.

  La captura tiene las siguientes opciones:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: error de la cuarentena.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped: error al guardar una copia de objeto en Copia de seguridad.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError: error interno de la cuarentena.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError: error de copia de seguridad.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: la base de datos antivirus está desactualizada. La cantidad de días desde la última vez que se ejecutó la tarea Actualización de bases de datos (tarea local o tarea de grupo, o tarea para conjuntos de dispositivos protegidos).

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días

- eventAVBasesTotallyOutdated: la base de datos antivirus es obsoleta. La cantidad de días desde la última vez que se ejecutó la tarea Actualización de bases de datos (tarea local o tarea de grupo, o tarea para conjuntos de dispositivos protegidos).

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días

- eventApplicationStarted: Kaspersky Embedded Systems Security para Windows se está ejecutando.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime

- eventSource

- eventApplicationShutdown: Kaspersky Embedded Systems Security para Windows está detenido.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: las áreas críticas no se han analizado durante un periodo prolongado. Número de días desde la última vez que se completó la tarea Análisis de áreas críticas.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días

- eventLicenseHasExpired: la licencia ha caducado

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: la licencia caduca pronto. Calculado como la cantidad de días hasta la fecha de caducidad de la licencia.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días

- eventTaskInternalError: la tarea finalizó con un error.

  La captura tiene las siguientes opciones:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode

- knowledgeBaseId
- taskName

- eventUpdateError: error al ejecutar la tarea de actualización.
  La captura tiene las siguientes opciones:
  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Descripciones de opciones y posibles valores de las capturas SNMP de Kaspersky Embedded Systems Security para Windows

Las descripciones de las opciones de capturas y sus posibles valores se incluyen a continuación:

- eventDateAndTime: fecha y hora del evento.
- eventSeverity: nivel de importancia.
  La opción puede tener los siguientes valores:
  - critical (1): crítico
  - warning (2): advertencia
  - info (3): informativo
- userName: nombre de usuario (por ejemplo, el nombre de un usuario que intentó acceder a un archivo infectado).
- computerName: nombre del dispositivo protegido (por ejemplo, el nombre de un dispositivo protegido desde el que un usuario intentó acceder a un archivo infectado).
- eventSource: componente funcional que generó el evento.
  La opción puede tener los siguientes valores:
  - unknown (0): componente funcional no conocido
  - quarantine (1): cuarentena
  - backup (2): Copia de seguridad
  - reporting (3): registros de tareas
  - updates (4): actualización
  - realTimeProtection (5): protección de archivos en tiempo real

- onDemandScanning (6): análisis a pedido
- product (7): evento relacionado con el funcionamiento de Kaspersky Embedded Systems Security para Windows en su totalidad en lugar de estar relacionado con operaciones de componentes individuales
- systemAudit (8): registro de auditoría del sistema

- eventReason: activador del evento, lo que desencadenó el evento.

  La opción puede tener los siguientes valores:

  - reasonUnknown (0): se desconoce el motivo.
  - reasonInvalidSettings (1): solo para eventos de Copia de seguridad y Cuarentena. Se muestra si las carpetas de Cuarentena o Copia de seguridad no están disponibles; esta situación puede presentarse cuando faltan los permisos de acceso necesarios o cuando, en los ajustes de Cuarentena, se ha configurado una ruta de acceso no válida a la carpeta (por ejemplo, una ruta de red). En este caso, Kaspersky Embedded Systems Security para Windows utilizará la carpeta de Copia de seguridad o de Cuarentena predeterminada.

- objectName: un nombre de objeto (por ejemplo, el nombre del archivo donde se detectó el virus).
- threatName: el nombre del objeto según la clasificación de la Enciclopedia de Virus. Este nombre se incluye en el nombre completo en los resultados de detección de objetos de Kaspersky Embedded Systems Security para Windows. Puede ver el nombre completo de un objeto detectado en el registro de tareas.
- detectType: tipo de objeto detectado.

  La opción puede tener los siguientes valores:

  - undefined (0): sin definir
  - virware: virus habituales y gusanos de red
  - trojware: troyanos
  - malware: otros programas maliciosos
  - adware: software de publicidad
  - pornware: software pornográfico
  - riskware: aplicaciones legítimas que utilizan los intrusos para dañar el dispositivo o los datos personales del usuario

- detectCertainty: nivel de certeza de detección de amenaza.

  La opción puede tener los siguientes valores:

  - Sospecha (probablemente infectado): Kaspersky Embedded Systems Security para Windows ha detectado una coincidencia parcial entre una sección del código del objeto y una sección conocida del código malicioso.
  - Seguro (infectado): Kaspersky Embedded Systems Security para Windows ha detectado una coincidencia completa entre una sección del código en el objeto y una sección conocida del código malicioso.

- days: cantidad de días (por ejemplo, la cantidad de días hasta la fecha de caducidad de la licencia).
- errorCode: un código de error.

- knowledgeBaseId: dirección de un artículo de la base de conocimientos (por ejemplo, dirección del artículo que explica un error en particular).
- taskName: un nombre de la tarea.
- updaterErrorEventReason: el motivo del error de actualización.

  La opción puede tener los siguientes valores:

  - reasonUnknown(0): se desconoce el motivo.
  - reasonAccessDenied: acceso denegado.
  - reasonUrlsExhausted: se agotó la lista de orígenes de actualizaciones.
  - reasonInvalidConfig: archivo de configuración no válido.
  - reasonInvalidSignature: firma no válida.
  - reasonCantCreateFolder: no se puede crear la carpeta.
  - reasonFileOperError: error de archivo.
  - reasonDataCorrupted: el objeto está dañado.
  - reasonConnectionReset: conexión restablecida.
  - reasonTimeOut: tiempo de espera agotado para la conexión.
  - reasonProxyAuthError: error de autenticación de proxy.
  - reasonServerAuthError: error de autenticación del servidor.
  - reasonHostNotFound: no se encontró el dispositivo.
  - reasonServerBusy: servidor no disponible.
  - reasonConnectionError: error de conexión.
  - reasonModuleNotFound: no se encontró el objeto.
  - reasonBlstCheckFailed(16): error al revisar la lista de claves rechazada. Es posible que se estuvieran publicando actualizaciones de las bases de datos durante la actualización; repita la actualización dentro de unos minutos.
- storageObjectNotAddedEventReason: el motivo por el que el objeto no se colocó en Copia de seguridad o Cuarentena.

  La opción puede tener los siguientes valores:

  - reasonUnknown (0): se desconoce el motivo.
  - reasonStorageInternalError: error de la base de datos; se debe restaurar Kaspersky Embedded Systems Security para Windows.
  - reasonStorageReadOnly: la base de datos es de solo lectura; se debe restaurar Kaspersky Embedded Systems Security para Windows.

- reasonStorageIOError: error de entrada/salida: a) Kaspersky Embedded Systems Security para Windows tiene daños y debe hacerse una restauración; b) hay daños en la unidad que contiene los archivos de Kaspersky Embedded Systems Security para Windows.
- reasonStorageCorrupted: el almacenamiento está dañado; se debe restaurar Kaspersky Embedded Systems Security para Windows.
- reasonStorageFull: la base de datos está llena; se requiere espacio libre en disco.
- reasonStorageOpenError: no se pudo abrir el archivo de la base de datos; se debe restaurar Kaspersky Embedded Systems Security para Windows.
- reasonStorageOSFeatureError: algunas funciones del sistema operativo no se corresponden con los requisitos de Kaspersky Embedded Systems Security para Windows.
- reasonObjectNotFound: el objeto que se coloca en Cuarentena no existe en el disco.
- reasonObjectAccessError: permisos insuficientes para usar la API de Copia de seguridad. La cuenta que se utiliza para realizar la operación no tiene permisos del operador de Copia de seguridad.
- reasonDiskOutOfSpace: espacio en disco insuficiente.

Integración con WMI

Kaspersky Embedded Systems Security para Windows admite la integración con Windows Management Instrumentation (WMI): puede usar sistemas cliente que utilicen WMI para recibir datos a través del estándar Web-Based Enterprise Management (WBEM) para recibir información sobre el estado de Kaspersky Embedded Systems Security para Windows y sus componentes.

Cuando Kaspersky Embedded Systems Security para Windows se instala, registra un módulo propietario en el sistema para crear un espacio de nombre de Kaspersky Embedded Systems Security para Windows en el dispositivo protegido. Un espacio de nombre de Kaspersky Embedded Systems Security para Windows le permite trabajar con clases e instancias de Kaspersky Embedded Systems Security para Windows y sus propiedades.

Los valores de algunas propiedades de instancias dependen de los tipos de tareas.

Una *tarea no periódica* es una tarea de aplicación que no posee límite de tiempo y puede estar en constante ejecución o detenida. Dichas tareas no tienen progreso de ejecución. Los resultados de la tarea se registran de manera continua mientras la tarea se está ejecutando como evento individual (por ejemplo, la detección de un objeto infectado por cualquiera de las tareas de Protección del equipo en tiempo real). Este tipo de tareas se administra mediante las directivas de Kaspersky Security Center.

Una *tarea periódica* es una tarea de aplicación que posee límite de tiempo y posee un progreso de ejecución que se muestra como porcentaje. Los resultados de este tipo de tarea se generan cuando la tarea finaliza y se representan como un único elemento o cambio en el estado de la aplicación (por ejemplo, "Se completó la actualización de las bases de datos de la aplicación", "Se generaron los archivos de configuración para las tareas de generación de reglas"). Varias tareas periódicas del mismo tipo pueden ejecutarse simultáneamente en un único dispositivo protegido (por ejemplo, tres tareas de Análisis a pedido con diferentes áreas del análisis). Las tareas periódicas se pueden administrar mediante Kaspersky Security Center como tareas de grupo.

Si usa herramientas para generar consultas de espacios de nombre WMI y recibir datos dinámicos de espacios de nombre WMI en una red corporativa, podrá recibir información sobre el estado de la aplicación actual (consulte la tabla a continuación).

Información sobre el estado de la aplicación

Propiedad de la instancia	Descripción	Valores
ProductName	Nombre de la aplicación instalada.	Nombre completo de aplicación sin número de versión.
ProductVersion	Versión completa de la aplicación instalada.	Número completo de la versión de la aplicación, incluido el número de compilación.
InstalledPatches	Conjunto de nombres de muestra para los parches instalados.	La lista de parches críticos instalados para la aplicación.
IsLicenseInstalled	Estado de activación de la aplicación.	El estado de la clave utilizada para activar la aplicación. Valores posibles: • Falso: no se ha agregado ninguna clave de licencia la aplicación. • Verdadero: Se han agregado una clave de licencia a la aplicación.
LicenseDaysLeft	Muestra cuántos días restan antes de que caduque la licencia actual.	Número de días restantes antes del vencimiento de la licencia actual. Valores no positivos posibles: • 0 - La licencia ha caducado. • -1 - No se pudo obtener información sobre la clave actual, o la clave especificada no puede usarse para activar la aplicación (por ejemplo, se bloquea según una lista de claves rechazadas).
AVBasesDatetime	Marca de fecha y hora para la versión actual de la base de datos antivirus.	Fecha y hora de la creación de las bases de datos antivirus actualmente en uso. Si la aplicación instalada no usa bases de datos antivirus, el campo tiene el valor "No instalada".
IsExploitPreventionEnabled	Estado del componente Prevención de exploits.	Estado del componente Prevención de exploits. Valores posibles: • True - El componente Prevención de exploits está habilitado y ofrece protección. • False - El componente Prevención de exploits no ofrece protección. Por ejemplo: desactivado, no instalado, se ha infringido el contrato de licencia.
ProtectionTasksRunning	Grupo de tareas de protección que se están ejecutando actualmente.	Enumera las tareas de protección, control y supervisión que se están ejecutando actualmente. Este campo debería explicar todas las tareas no periódicas en ejecución. Si no se está ejecutando ninguna tarea no periódica, el campo tiene el valor "None".

IsAppControlRunning	Estado de la tarea Control de inicio de aplicaciones.	Estado de la tarea Control de inicio de aplicaciones. • True - La tarea Control de inicio de aplicaciones se está ejecutando actualmente. • False - La tarea Control de inicio de aplicaciones no se está ejecutando actualmente o el componente Control de inicio de aplicaciones no está instalado.
AppControlMode	Modo de la tarea Control de inicio de aplicaciones.	Describe el estado actual del componente Control de inicio de aplicaciones que explicita el modo seleccionado para la tarea correspondiente. Valores posibles: • Activo - El modo **Activo** está seleccionado en la configuración de la tarea. • Solo estadísticas - El modo **Solo estadísticas** está seleccionado en la configuración de la tarea. • No instalado - El componente Control de inicio de aplicaciones no está instalado.
AppControlRulesNumber	Número total de reglas de Control de inicio de aplicaciones.	El número de reglas especificadas actualmente en la configuración de la tarea Control de inicio de aplicaciones.
AppControlLastBlocking	La marca de fecha y hora del último inicio de aplicaciones bloqueado por la tarea Control de inicio de aplicaciones en cualquier modo.	La fecha y la hora en que el componente Control de inicio de aplicaciones bloqueó por última vez el inicio de una aplicación. Este campo incluye todas las aplicaciones bloqueadas, sin tener en cuenta el modo de la tarea. Si no hubo ningún caso de ejecuciones bloqueadas al momento de procesarse la consulta WMI, el campo tiene el valor "None".
PeriodicTasksRunning	Grupo de tareas periódicas que se están ejecutando actualmente.	Lista de tareas Análisis a pedido, Actualización y de inventario que se están ejecutando actualmente. Este campo debe incluir todas las tareas periódicas en ejecución. Si no hay ningúna tarea periódica en ejecución, el campo tiene el valor "None".
ConnectionState	Estado de la conexión entre el componente Proveedor de WMI y el servicio de Kaspersky Security (KAVFS).	Información sobre el estado de la conexión entre el componente Proveedor de WMI y el servicio de Kaspersky Security. Valores posibles: • Éxito - Se estableció correctamente la conexión: el cliente de WMI puede recibir el estado de la aplicación.

		• Error. Código de error: <código> - La conexión no se pudo establecer debido a un error con el código especificado.

Estos datos representan propiedades de instancias KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security para Windows, donde:

- KasperskySecurity_ProductInfo es el nombre de la clase Kaspersky Embedded Systems Security para Windows
- .ProductName=Kaspersky Embedded Systems Security para Windows son las propiedades de la clave de Kaspersky Embedded Systems Security para Windows

La instancia se crea en el espacio de nombre ROOT\Kaspersky\Security.

Cómo utilizar Kaspersky Embedded Systems Security para Windows desde la línea de comandos

Esta sección describe cómo utilizar Kaspersky Embedded Systems Security para Windows desde la línea de comandos.

Comandos

Puede ejecutar comandos básicos de administración de Kaspersky Embedded Systems Security para Windows desde la línea de comandos del dispositivo protegido mediante el componente de la utilidad de línea de comandos, que se incluye en el grupo de componentes de la aplicación de Kaspersky Embedded Systems Security para Windows.

Puede utilizar comandos para administrar solo aquellas funciones a las que tiene acceso según los permisos asignados a su Kaspersky Embedded Systems Security para Windows.

Ciertos comandos de Kaspersky Embedded Systems Security para Windows se ejecutan en los modos siguientes:

- Modo síncrono: el control regresa a la Consola solo después de que el comando se ha completado.
- Modo asíncrono: el control regresa a la Consola inmediatamente después de que el comando se inicia.

Para interrumpir un comando que se ejecuta en modo síncrono,

presione el acceso directo del teclado **Ctrl+C**.

Siga estas reglas al introducir comandos de Kaspersky Embedded Systems Security para Windows:

- Introduzca modificadores y comandos utilizando mayúsculas y minúsculas.
- Separe los modificadores con un espacio.
- Si la ruta de acceso de un archivo/carpeta especificado como valor incluye un espacio, ponga la ruta entre comillas, por ejemplo: `"C:\TEST\test cpp.exe"`.
- Si es necesario, puede usar comodines en el nombre de archivo o la ruta, por ejemplo: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.Doc"`, `"C:\Temp\Temp*.doc"`.

Se puede usar la línea de comandos para realizar todas las operaciones requeridas para la administración de Kaspersky Embedded Systems Security para Windows (consulte la tabla a continuación).

Comandos de Kaspersky Embedded Systems Security para Windows

Comando	Descripción
KAVSHELL APPCONTROL	Actualizar la lista de reglas según la regla de importación seleccionada.
KAVSHELL APPCONTROL /CONFIG	Establecer el modo de operación de la tarea Control de inicio de aplicaciones
KAVSHELL APPCONTROL /GENERATE	Iniciar la tarea de Generador de reglas de Control de inicio de aplicaciones.

KAVSHELL VACUUM	Desfragmentar los archivos de registro de Kaspersky Embedded Systems Security para Windows.
KAVSHELL PASSWORD	Administrar la configuración de protección con contraseña.
KAVSHELL HELP	Mostrar la ayuda de comandos de Kaspersky Embedded Systems Security para Windows.
KAVSHELL START	Iniciar el servicio de Kaspersky Security.
KAVSHELL STOP	Detener el servicio de Kaspersky Security.
KAVSHELL SCAN	Crear e iniciar una tarea de Análisis a pedido temporal con la configuración de seguridad y el área del análisis especificada por las opciones de comando.
KAVSHELL SCANCRITICAL	Iniciar la tarea local del sistema Análisis de áreas críticas.
KAVSHELL TASK	Inicia, pausa, reanuda o detiene la tarea especificada de forma asincrónica. Devuelve el estado en que se encuentra la tarea o las estadísticas de la tarea.
KAVSHELL RTP	Iniciar o detener todas las tareas de Protección del equipo en tiempo real.
KAVSHELL UPDATE	Iniciar la tarea Actualización de bases de datos con los ajustes especificados por las opciones de línea de comandos.
KAVSHELL ROLLBACK	Revertir las bases de datos a la versión anterior.
KAVSHELL LICENSE	Agregar o eliminar las claves. Visualizar la información sobre las claves agregadas.
KAVSHELL TRACE	Habilitar o deshabilitar el seguimiento. Administrar la configuración del seguimiento.
KAVSHELL DUMP	Habilitar o deshabilitar la creación de archivos de volcado cuando los procesos de Kaspersky Embedded Systems Security para Windows terminen de forma anormal.
KAVSHELL IMPORT	Importar los valores de configuración, funciones y tareas generales de Kaspersky Embedded Systems Security para Windows de un archivo de configuración.
KAVSHELL EXPORT	Exportar todos los valores de configuración de Kaspersky Embedded Systems Security para Windows y las tareas existentes a un archivo de configuración.
KAVSHELL DEVCONTROL	Agregar a la lista de reglas de control de dispositivos generadas según el método seleccionado.

Obtener ayuda para los comandos de Kaspersky Embedded Systems Security para Windows. KAVSHELL HELP

Para ver la lista de todos los comandos de Kaspersky Embedded Systems Security para Windows, ejecute uno de los comandos siguientes:

```
/KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Para ver una descripción de un comando y su sintaxis, ejecute uno de los siguientes comandos:

```
KAVSHELL HELP <comando>
```

```
KAVSHELL <comando> /?
```

Ejemplos de KAVSHELL HELP

Para ver información detallada sobre el comando KAVSHELL SCAN, ejecute el siguiente comando:

```
KAVSHELL HELP SCAN
```

Iniciar y detener el servicio de Kaspersky Security: KAVSHELL START, KAVSHELL STOP

Para ejecutar el servicio de Kaspersky Security, ejecute el siguiente comando:

```
KAVSHELL START
```

De manera predeterminada, cuando se inicia el servicio de Kaspersky Security, se inician Protección de archivos en tiempo real y Análisis al inicio del sistema operativo, así como las demás tareas cuyo inicio esté programado **Al inicio de la aplicación**.

Para detener el servicio de Kaspersky Security, ejecute el comando siguiente:

```
KAVSHELL STOP
```

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Analizar un área específica: KAVSHELL SCAN

Para iniciar una tarea de análisis de áreas específicas del dispositivo protegido, utilice `KAVSHELL SCAN`. Las opciones de la línea de comandos especifican el área del análisis y la configuración de seguridad del nodo seleccionado.

Una tarea de Análisis a pedido que inicia con el comando `KAVSHELL SCAN` es una tarea temporal. Se muestra en Consola de la aplicación solo al ejecutarse (no se puede ver su configuración de la tarea en la Consola de la aplicación). Sin embargo, se crea un registro de tareas y se visualiza en el **Registros de tareas** en la Consola de la aplicación.

Al especificar las rutas de acceso en las tareas de análisis de áreas específicas, se pueden utilizar las variables del entorno. Si utiliza una variable del entorno del usuario, ejecute el comando `KAVSHELL SCAN` como el usuario correspondiente.

El comando KAVSHELL SCAN se ejecuta en modo síncrono.

Para iniciar una tarea Análisis a pedido desde la línea de comandos, use el comando KAVSHELL TASK.

Sintaxis del comando KAVSHELL SCAN

```
KAVSHELL SCAN <área del análisis>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< ruta de acceso al archivo
con la lista de áreas del análisis >] [/F<A|C|E>] [/NEWONLY] [/AI:
<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>]
[/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"máscaras">] [/ES:<tamaño>] [/ET:<cantidad de
segundos>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<días>] [NORECALL]>] [/NOICHECKER]
[/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<ruta de acceso al archivo de registro de
tareas>] [/ANSI] [/ALIAS:<alias de la tarea>]
```

El comando KAVSHELL SCAN tiene parámetros y opciones obligatorias y opcionales (consulte la tabla a continuación).

Ejemplo del comando KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM
/EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log

KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Parámetros y opciones de la línea de comandos KAVSHELL SCAN

Parámetro y opción	Descripción
Área del análisis. La configuración es obligatoria.	
<archivos>	Especifica el área del análisis: lista de archivos, carpetas, rutas de red y áreas predefinidas. Especifique las rutas de acceso de red en formato convención de nomenclatura universal (UNC).
<carpetas>	El siguiente ejemplo contiene la carpeta Folder4, pero no la ruta de acceso a la misma. Esto significa que la carpeta se encuentra en la carpeta desde la que se ejecuta el comando KAVSHELL. KAVSHELL SCAN Folder4
<ruta de red>	Si el nombre del objeto a analizar tiene espacios, se debe colocar entre comillas. Si se especifica una carpeta, Kaspersky Embedded Systems Security para Windows también analizará todas sus subcarpetas. Los símbolos * o ? se pueden utilizar para analizar un grupo de archivos.
/MEMORY	Analizar objetos en RAM
/SHARED	Analizar carpetas compartidas en el dispositivo protegido
/STARTUP	Analizar objetos de ejecución automática
/REMDRIVES	Analizar unidades extraíbles
/FIXDRIVES	Analizar unidades de disco duro

/MYCOMP	Analizar todas las áreas del dispositivo protegido
/L:<ruta del archivo con una lista de áreas del análisis>	Ruta completa del archivo con una lista de áreas del análisis. Utilice saltos de línea para separar las áreas del análisis en el archivo. Puede especificar áreas del análisis predefinidas como se muestra en el siguiente ejemplo del contenido de un archivo con una lista de áreas del análisis: C:\ D:\Docs*.doc E:\Mis documentos /STARTUP /SHARED
Analizar objetos (tipos de archivos). Si no especifica esta opción, Kaspersky Embedded Systems Security para Windows analizará los objetos por formato.	
/FA	Analizar todos los objetos
/FC	Analizar los objetos por formato (manera predeterminada). Kaspersky Embedded Systems Security para Windows analiza solo objetos cuyos formatos se incluyen en la lista de formatos de objetos infectables.
/FE	Analizar los objetos por extensión Kaspersky Embedded Systems Security para Windows analiza solo objetos con extensiones que figuran en la lista de extensiones de objetos infectables.
/NEWONLY	Analizar solo los archivos nuevos y modificados. Si no especifica esta opción, Kaspersky Embedded Systems Security para Windows analizará todos los objetos.
Acción que se realizará con los objetos infectados y otros objetos. Si no se especificaron valores para este modificador, Kaspersky Embedded Systems Security para Windows ejecutará la acción **Omitir**.	
DISINFECT	Desinfectar, omitir si la desinfección es imposible Las opciones DISINFECT y DELETE se conservan en la versión actual de Kaspersky Embedded Systems Security para Windows a fin de asegurar compatibilidad con versiones anteriores. Estas opciones pueden utilizarse en lugar de las opciones /AI y /AS. En ese caso, Kaspersky Embedded Systems Security para Windows no procesará objetos probablemente infectados.
DISINFDEL	Desinfectar, eliminar si la desinfección es imposible
DELETE	Eliminar Las opciones DISINFECT y DELETE se conservan en la versión actual de Kaspersky Embedded Systems Security para Windows a fin de asegurar compatibilidad con versiones anteriores. Estas opciones pueden utilizarse en lugar de las opciones /AI y /AS. En ese caso, Kaspersky Embedded Systems Security para Windows no procesará objetos probablemente infectados.
REPORT	Enviar un informe (manera predeterminada)
AUTO	Realizar la acción recomendada
Acción que se realizará con los objetos probablemente infectados. Si no se especificó esta opción, Kaspersky Embedded Systems Security para Windows ejecutará la acción **Omitir**.	
QUARANTINE	Cuarentena
DELETE	Eliminar
REPORT	Enviar un informe (manera predeterminada)
AUTO	Realizar la acción recomendada

Exclusiones	
/E:ABMSPO	Excluir los siguientes tipos de objetos compuestos: A: archivos (se analizan solo los archivos SFX) B: bases de datos de correo electrónico M: correo electrónico sin formato S: archivos y archivos SFX P: objetos empaquetados O: objetos OLE integrados
/EM: <"máscaras">	Excluir archivos por máscara Puede especificar varias máscaras, por ejemplo: `EM:"*.txt; *.png; C\Videos\*.avi"`.
/ET:<cantidad de segundos>	Detener el procesamiento de un objeto si demora más tiempo que la cantidad de segundos especificada por <cantidad de segundos>. De manera predeterminada, no hay ninguna restricción de tiempo.
/ES:<tamaño>	No analizar objetos compuestos que superen el tamaño (en MB) especificado por el valor <tamaño>. De forma predeterminada, Kaspersky Embedded Systems Security para Windows analiza objetos de todos los tamaños.
/TZOFF	Deshabilitar exclusiones de zonas de confianza
Configuración avanzada (Opciones)	
/NOICHECKER	Deshabilitar la utilización de iChecker (habilitada de forma predeterminada).
/NOISWIFT	Deshabilitar la utilización de iSwift (habilitada de forma predeterminada).
/ANALYZERLEVEL: <nivel del análisis heurístico>	Habilitar el Analizador heurístico, configurar el nivel de análisis. Los siguientes niveles de análisis heurístico están disponibles: 1: ligero 2: medio 3: profundo Si se omite esta opción, Kaspersky Embedded Systems Security para Windows no utilizará el Analizador heurístico.
/ALIAS:<alias de la tarea>	Asigna un nombre temporal a una tarea de Análisis a pedido, lo que le permite hacer referencia a la tarea mientras se ejecuta, por ejemplo, para ver las estadísticas con el comando TASK. El alias de tarea debe ser único entre los alias de tarea de todos los componentes de Kaspersky Embedded Systems Security para Windows. Si no se especificó esta opción, se asigna un nombre temporal como scan_<pid_de_kavshell>, por ejemplo, scan_1234. En la Consola de la aplicación, se asigna a la tarea el nombre "Analizar objetos <fecha y hora>", por ejemplo, Analizar objetos 16/08/2007 5:13:14 p. m.
Configuración del registro de tareas (configuración del informe)	
/W:<ruta del archivo de registro de tareas>	Si se especifica este parámetro, Kaspersky Embedded Systems Security para Windows guardará el archivo de registro de tareas usando el nombre definido por el valor del parámetro. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos que ocurrieron durante la tarea.

	El registro se utiliza para registrar eventos definidos por la configuración del registro de tareas y del registro de eventos de Kaspersky Embedded Systems Security para Windows en Visor de eventos. Puede especificar tanto la ruta relativa como la ruta absoluta del archivo de registro. Si se especifica solo un nombre de un archivo sin una ruta, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo Registros de tareas de la Consola de la aplicación. Si Kaspersky Embedded Systems Security para Windows no puede crear el archivo de registro, se mostrará un mensaje de error, pero aun así ejecutará el comando.
/ANSI	Esta opción utiliza la codificación ANSI para registrar eventos en el registro de tareas. La opción ANSI no se aplicará si el parámetro W no está especificado. Si no se especifica la opción ANSI, se utilizará UNICODE para generar el registro de tareas.

Iniciar la tarea Análisis de áreas críticas: KAVSHELL SCANCRITICAL

Use el comando `KAVSHELL SCANCRITICAL` para iniciar la tarea Análisis de áreas críticas con la configuración definida en la Consola de la aplicación.

Sintaxis del comando KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<ruta del archivo del registro de tareas>]
```

Ejemplos del comando KAVSHELL SCANCRITICAL

Para ejecutar la tarea Análisis de áreas críticas y guardar un registro de tareas scancritical.log en la carpeta actual, ejecute el siguiente comando:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Puede utilizar el parámetro /W para configurar la ubicación del registro de tareas (consulte la tabla a continuación).

Sintaxis del parámetro `/W` para el comando `KAVSHELL SCANCRITICAL`

Parámetro y opción	Descripción
/W:<ruta del archivo de registro de tareas>	Si se especifica este parámetro, Kaspersky Embedded Systems Security para Windows guardará el archivo de registro de tareas usando el nombre definido por el valor del parámetro. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos que ocurrieron durante la tarea. El registro se utiliza para registrar eventos definidos por la configuración del registro de tareas y del registro de eventos de Kaspersky Embedded Systems Security para Windows en Visor de eventos.

	Puede especificar tanto la ruta relativa como la ruta absoluta del archivo de registro. Si se especifica solo un nombre de un archivo sin una ruta, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo **Registros de tareas** de la Consola de la aplicación. Si Kaspersky Embedded Systems Security para Windows no puede crear el archivo de registro, se mostrará un mensaje de error, pero aun así ejecutará el comando.

Administración de tareas de manera asíncrona: KAVSHELL TASK

Puede utilizar el comando `KAVSHELL TASK` para administrar la tarea especificada: ejecutar, pausar, reanudar y detener la tarea y ver el estado y estadísticas de la tarea actual. El comando se ejecuta en modo asíncrono.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL TASK

```
KAVSHELL TASK [<alias de nombre de tarea> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Ejemplo del comando KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

El comando `KAVSHELL TASK` puede ejecutarse sin parámetros ni opciones o con uno o más parámetros y opciones (consulte la tabla a continuación).

Parámetros y opciones de la línea de comandos KAVSHELL TASK

Parámetro y opción	Descripción
Sin parámetros	Regresar la lista de todas las tareas existentes de Kaspersky Embedded Systems Security para Windows. La lista incluye los siguientes campos: alias de la tarea, categoría de la tarea (sistema o personalizado) y estado actual de la tarea.
<alias de tarea>	En lugar del nombre de la tarea, en el comando SCAN TASK use el alias de la tarea, un nombre adicional abreviado que Kaspersky Embedded Systems Security para Windows

	asigna a las tareas. Para ver los alias de tarea de Kaspersky Embedded Systems Security para Windows, introduzca el comando KAVSHELL TASK sin ningún parámetro.
/START	Iniciar la tarea especificada en modo asíncrono.
/STOP	Detener la tarea especificada.
/PAUSE	Poner en pausa la tarea especificada.
/RESUME	Reanudar la tarea especificada en modo asíncrono.
/STATE	Muestra el estado de la tarea actual (por ejemplo, *En ejecución*, *Completada*, *En pausa*, *Detenida*, *Error*, *Iniciando*, *Reanudando*)
/STATISTICS	Recuperar las estadísticas de la tarea: información acerca de la cantidad de objetos procesados desde el inicio de la tarea

Tenga en cuenta que no todas las tareas de Kaspersky Embedded Systems Security para Windows son totalmente compatibles con las claves /PAUSE, /RESUME y /STATE.

Códigos de devolución para el comando KAVSHELL TASK.

Eliminación del atributo PPL: KAVSHELL CONFIG

El comando `KAVSHELL CONFIG` le permite eliminar el atributo PPL (Protected Process Light) para el servicio de Kaspersky Security por medio del controlador ELAM instalado durante la instalación de la aplicación.

Sintaxis del comando KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

Parámetros y opciones de la línea de comandos KAVSHELL CONFIG

Parámetro y opción	Descripción
/PPL:OFF	Eliminar el atributo PPL para el servicio de Kaspersky Security.

Iniciar y detener las tareas de Protección del equipo en tiempo real. KAVSHELL RTP

Puede utilizar el comando `KAVSHELL RTP` para iniciar o detener todas las tareas de Protección del equipo en tiempo real.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Ejemplo del comando KAVSHELL RTP

Para iniciar todas las tareas de Protección del equipo en tiempo real, ejecute el siguiente comando:

```
KAVSHELL RTP /START
```

El comando `KAVSHELL RTP` debe incluir una de dos opciones (consulte la tabla a continuación).

Opciones de línea de comandos KAVSHELL RTP

Parámetro y opción	Descripción
/START	Iniciar todas las tareas de Protección del equipo en tiempo real: Protección de archivos en tiempo real y uso de KSN.
/STOP	Detener todas las tareas de Protección del equipo en tiempo real.

Administración de la tarea Control de inicio de aplicaciones: KAVSHELL APPCONTROL /CONFIG

Puede usar el comando `KAVSHELL APPCONTROL /CONFIG` para configurar el modo en el cual la tarea Control de inicio de aplicaciones se ejecuta y supervisa la carga de módulos DLL.

Sintaxis del comando KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<ruta completa al archivo XML>
```

Ejemplos del comando KKAVSHELL APPCONTROL /CONFIG

*Para ejecutar la tarea Control de inicio de aplicaciones en el modo **Activo** sin supervisar la carga de DLL y guardar la configuración de la tarea después de la finalización, ejecute el siguiente comando:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Puede ajustar la configuración de la tarea de Control de inicio de aplicaciones usando los parámetros de la línea de comandos (ver la tabla a continuación).

Parámetros y opciones de la línea de comandos `KAVSHELL APPCONTROL /CONFIG`

Parámetro y opción	Descripción
`/mode:<applyrules|statistics>`	Modo de la tarea Control de inicio de aplicaciones. Puede seleccionar uno de los siguientes modos: • active: aplicar reglas de Control de inicio de aplicaciones; • statistics: solo genera estadísticas.
`/dll:<no|yes>`	Habilitar o deshabilitar la supervisión de la carga de DLL.

`/savetofile: <ruta de acceso completa al archivo XML>`	Exportar las reglas especificadas en el archivo indicado en formato XML.
`/savetofile: <nombre completo del archivo XML>`	Guardar la lista de reglas en el archivo.
`/savetofile: <nombre completo del archivo XML> /sdc`	Guardar la lista de reglas de Control de distribución de software en el archivo.
`/clearsdc`	Eliminar todas las reglas de control de distribución de software de la lista.

Generador de reglas de Control de inicio de aplicaciones: KAVSHELL APPCONTROL /GENERATE

Puede utilizar el comando `KAVSHELL APPCONTROL /GENERATE` para generar listas de reglas de Control de inicio de aplicaciones.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <ruta de acceso a la carpeta> | /source:<ruta de acceso a archivos con lista de carpetas> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<usuario o grupo de usuarios>] [/export:<ruta de acceso a archivo XML>] [/import:<a|r|m>] [/prefix:<prefijo para nombres de reglas>] [/unique]
```

Ejemplos del comando KAVSHELL APPCONTROL /GENERATE

Para generar reglas para archivos desde carpetas especificadas, ejecute el siguiente comando:

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

Para generar reglas para archivos ejecutables con cualquier extensión en la carpeta especificada y, después de la finalización de la tarea, guardar las reglas generadas en el archivo XML del archivo especificado, ejecute el siguiente comando:

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

Puede utilizar parámetros y opciones de la línea de comandos para establecer las opciones de la generación automática de reglas para la tarea Control de inicio de aplicaciones (consulte la tabla a continuación).

Parámetros y opciones de la línea de comandos `KAVSHELL APPCONTROL /GENERATE`

Parámetro y opción	Descripción
Área de aplicación de las reglas de autorización	

<ruta de acceso a la carpeta>	Especificar la ruta de acceso de la carpeta con archivos ejecutables para los que se generarán automáticamente las reglas de autorización.
/source: <ruta de acceso al archivo con la lista de carpetas>	Especificar la ruta de acceso a un archivo TXT con una lista de carpetas con archivos ejecutables para las que se generarán automáticamente las reglas de autorización.
/masks: <edms>	Especificar las extensiones de archivos ejecutables para las que se generarán automáticamente las reglas de autorización. Puede incluir archivos con las siguientes extensiones en el área de las reglas: • e: archivos EXE • d: archivos DLL • m: archivos MSI • s: scripts
/runapp	Al generar reglas de autorización, tenga en cuenta las aplicaciones que se están ejecutando actualmente en el dispositivo protegido.
Acciones al generar automáticamente reglas de autorización	
/rules: <ch|cp|h>	Especificar acciones a realizar mientras se generan las reglas para la tarea Control de inicio de aplicaciones: • ch: usar el certificado digital. De no haber un certificado, usar el hash SHA256. • cp: usar el certificado digital. De no haber un certificado, usar la ruta al archivo ejecutable. • h: usar el hash SHA256.
/strong	Use el asunto y la huella del certificado digital al generar automáticamente las reglas de autorización para la tarea Control de inicio de aplicaciones. El comando se ejecuta si se especifica un valor para la opción /rules: <ch|cp>.
/user: <usuario o grupo de usuarios>	Especificar el usuario o grupo de usuarios para los cuales se aplicarán las reglas. La aplicación supervisará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.
Acciones después de la finalización de la tarea Generador de reglas de Control de inicio de aplicaciones	
/export: <ruta de acceso completa al archivo XML>	Guardar las reglas generadas en un archivo XML.
/unique	Añadir información sobre el dispositivo protegido con aplicaciones instaladas que son la base para generar las reglas de autorización de Control de inicio de aplicaciones.
/prefix: <prefijo para nombres de regla>	Especificar un prefijo para los nombres de las reglas de autorización de Control de inicio de aplicaciones.
/import: <a|r|m>	Importar las reglas generadas en la lista especificada de reglas de Control de inicio de aplicaciones según la regla de importación seleccionada: • a: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican)

	• r: **Reemplazar reglas existentes** (las reglas con ajustes idénticos no se agregan; se agrega una regla si al menos un ajuste de la regla es único) • m: **Combinar con reglas existentes** (las reglas con ajustes idénticos no se agregan; se agrega una regla si al menos un ajuste de la regla es único)

Agregar reglas a la lista de reglas de Control de inicio de aplicaciones. KAVSHELL APPCONTROL

Puede utilizar el comando `KAVSHELL APPCONTROL` para agregar reglas de un archivo XML a la lista de reglas de la tarea Control de inicio de aplicaciones basándose en la regla de importación seleccionada, así como para eliminar todas las reglas que existan en la lista.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <ruta de acceso al archivo XML> | /replace <ruta de acceso al archivo XML> | /merge <ruta de acceso al archivo XML> | /clear
```

Ejemplo del comando KAVSHELL APPCONTROL

Para agregar reglas de un archivo XML a reglas existentes de Control de inicio de aplicaciones según la regla de importación Agregar a reglas existentes, ejecute el siguiente comando:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Puede utilizar opciones en la línea de comandos para seleccionar el principio con el que se agregarán las nuevas reglas del archivo XML especificado a la lista de reglas de Control de inicio de aplicaciones definida (consulte la tabla a continuación).

Parámetros y opciones de la línea de comandos `KAVSHELL APPCONTROL`

Parámetro y opción	Descripción
/append <ruta de acceso al archivo XML>	Actualizar la lista de reglas de Control de inicio de aplicaciones según el archivo XML especificado. Regla de importación: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican).
/replace <ruta de acceso al archivo XML>	Actualizar la lista de reglas de Control de inicio de aplicaciones según el archivo XML especificado. Regla de importación: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un ajuste de la regla es único).
/merge <ruta de	Actualizar la lista de reglas de Control de inicio de aplicaciones según el archivo XML especificado. Regla de importación: **Combinar con reglas existentes** (las nuevas reglas no

acceso al archivo XML>	duplican reglas existentes).
/clear	Vacía la lista de reglas de Control de inicio de aplicaciones.

Agregar reglas a la lista de reglas de Control de dispositivos. KAVSHELL DEVCONTROL

Puede utilizar el comando `KAVSHELL DEVCONTROL` para agregar reglas de un archivo XML a la lista de reglas de la tarea Control de dispositivos según la regla de importación seleccionada y eliminar todas las reglas existentes de la lista.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <ruta de acceso al archivo XML> | /replace <ruta de acceso al archivo XML> | /merge <ruta de acceso al archivo XML> | /clear
```

Ejemplo del comando KAVSHELL DEVCONTROL

Para agregar las reglas de un archivo XML a las reglas de control de dispositivos existentes usando la regla de importación "Agregar a reglas existentes", ejecute el siguiente comando:

```
KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml
```

Puede utilizar opciones en la línea de comandos para seleccionar la regla de importación que se usará para agregar las nuevas reglas del archivo XML especificado a la lista de reglas de Control de dispositivos definida (consulte la tabla a continuación).

Parámetros y opciones de la línea de comandos `KAVSHELL DEVCONTROL`

Clave	Descripción
/append <ruta de acceso al archivo XML>	Actualizar la lista de reglas de Control de dispositivos según el archivo XML especificado. Regla de importación: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican).
/replace <ruta de acceso al archivo XML>	Actualizar la lista de reglas de Control de dispositivos según el archivo XML especificado. Regla de importación: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un ajuste de la regla es único).
/merge <ruta de acceso al	Actualizar la lista de reglas de Control de dispositivos según el archivo XML especificado. Regla de importación: **Combinar con reglas existentes** (las nuevas reglas no duplican reglas existentes).

archivo XML>	
/clear	Vacía la lista de reglas de Control de dispositivos.

Inicio de la tarea Actualización de bases de datos: KAVSHELL UPDATE

El comando `KAVSHELL UPDATE` se puede utilizar para iniciar la tarea Actualización de bases de datos de Kaspersky Embedded Systems Security para Windows en modo sincrónico.

Una tarea de Actualización de bases de datos iniciada con el comando `KAVSHELL UPDATE` es una tarea temporal. Solo se muestra en la Consola de la aplicación mientras está en ejecución. Sin embargo, se crea un registro de tareas y se visualiza en el **Registros de tareas** en la Consola de la aplicación. Se pueden aplicar directivas de Kaspersky Security Center para actualizar tareas creadas e iniciadas mediante el comando `KAVSHELL UPDATE` y para actualizar tareas creadas en la Consola de la aplicación. Para obtener información sobre el uso de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security para Windows en dispositivos protegidos, consulte la sección "Administración de Kaspersky Embedded Systems Security para Windows utilizando Kaspersky Security Center".

Se pueden usar variables del entorno al especificar la ruta a un origen de actualizaciones en esta tarea. Si se utiliza una variable de entorno del usuario, ejecute el comando `KAVSHELL UPDATE` como el usuario correspondiente.

Sintaxis del comando KAVSHELL UPDATE

```
KAVSHELL UPDATE <ruta al origen de actualizaciones | /AK | /KL> [/NOUSEKL] [/PROXY:
<dirección>:<puerto>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nombre de usuario>] [/PROXYPWD:
<contraseña>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/REG:<código
iso3166>] [/W:<ruta al archivo de registro de tareas>] [/ALIAS:<alias de la tarea>]
```

El comando KAVSHELL UPDATE tiene parámetros y opciones obligatorias y opcionales (consulte la tabla a continuación).

Ejemplos del comando KAVSHELL UPDATE

Para iniciar una tarea personalizada de Actualización de bases de datos, ejecute el comando siguiente:

```
KAVSHELL UPDATE
```

Para iniciar una tarea de Actualización de bases de datos mediante archivos de actualizaciones en la carpeta de red \\server\databases, ejecute el siguiente comando:

```
KAVSHELL UPDATE \\server\databases
```

Para iniciar una Actualización de bases de datos desde el servidor FTP ftp://dnl-ru1.kaspersky-labs.com/ y registrar todos los eventos de tareas a un archivo con nombre c:\update_report.log, ejecute el siguiente comando:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

Para descargar actualizaciones de la base de datos de Kaspersky Embedded Systems Security para Windows del servidor de actualizaciones de Kaspersky, conéctese al origen de actualizaciones a través de un servidor proxy (dirección del servidor proxy: proxy.company.com, puerto: 8080). Para acceder al dispositivo protegido mediante la autenticación NTLM integrada de Microsoft Windows con nombre de usuario "inetuser" y contraseña "123456", ejecute el siguiente comando:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

Parámetros y opciones de la línea de comandos KAVSHELL UPDATE

Parámetro y opción	Descripción
Origen de actualizaciones (parámetro obligatorio). Especifique una o más fuentes. Kaspersky Embedded Systems Security para Windows accederá a los orígenes en el orden en que están enumerados. Separar las fuentes con un espacio.	
<ruta en formato UNC>	Origen de actualizaciones definido por el usuario. Ruta a la carpeta de actualizaciones de red en formato UNC.
<URL>	Origen de actualizaciones definido por el usuario. Dirección del servidor HTTP o FTP donde se ubica la carpeta de actualización.
<Carpeta local>	Origen de actualizaciones definido por el usuario. Carpeta en el dispositivo protegido.
/AK	Usar el servidor de administración de Kaspersky Security Center como el origen de actualizaciones.
/KL	Usar los servidores de actualizaciones de Kaspersky como el origen de actualizaciones.
/NOUSEKL	No utilice los servidores de actualizaciones de Kaspersky si no hay otros orígenes de actualizaciones disponibles (se utiliza de manera predeterminada).
Configuración del servidor proxy	
/PROXY:<dirección>:<puerto>	Nombre de red o dirección IP del servidor proxy y su puerto. Si no se especifica este parámetro, Kaspersky Embedded Systems Security para Windows detectará automáticamente la configuración del servidor proxy utilizado en la red de área local.
/AUTHTYPE:<0-2>	Este parámetro especifica el método de autenticación utilizado para acceder al servidor proxy. Puede tener los valores siguientes: **0**: autenticación NTLM integrada de Microsoft Windows; Kaspersky Embedded Systems Security para Windows se comunicará con el servidor proxy a través de la cuenta **Sistema local** (**SYSTEM**) **1**: autenticación NTLM de Microsoft Windows; Kaspersky Embedded Systems Security para Windows se comunicará con el servidor proxy mediante el nombre de usuario y la contraseña especificados por los parámetros /PROXYUSER y /PROXYPWD **2**: autenticación con el nombre de usuario y la contraseña especificados por los parámetros /PROXYUSER y /PROXYPWD (autenticación básica) Si el servidor proxy no requiere autenticación, no es necesario especificar este parámetro.
/PROXYUSER:<nombre de usuario>	Nombre de usuario que se utilizará para acceder al servidor proxy. Si se especifica /AUTHTYPE:0, se ignorarán los parámetros /PROXYUSER:<nombre de usuario> y /PROXYPWD:<contraseña>.
/PROXYPWD:<contraseña>	Contraseña de usuario que se utilizará para acceder al servidor proxy. Si se especifica /AUTHTYPE:0, se ignorarán los parámetros /PROXYUSER:<nombre

	de usuario> y /PROXYPWD:<contraseña>. Si se especifica el parámetro /PROXYUSER y se omite el parámetro /PROXYPWD, la contraseña se considerará una cadena vacía.
/NOPROXYFORKL	No use la configuración del servidor proxy para conectarse con los servidores de actualizaciones de Kaspersky (se utiliza de manera predeterminada).
/USEPROXYFORCUSTOM	Utilice la configuración del servidor proxy para conectarse con los orígenes de actualizaciones definidos por el usuario (no se utiliza de manera predeterminada).
/USEPROXYFORLOCAL	Utilice la configuración del servidor proxy para conectarse con los orígenes de actualizaciones locales. Si no se especifica, se aplicará la configuración **No usar el servidor proxy para las direcciones locales**.
Configuración general de los servidores FTP y HTTP	
/NOFTPPASSIVE	Si se especifica esta clave, Kaspersky Embedded Systems Security para Windows usará el modo de servidor FTP activo para conectarse con el dispositivo protegido. Si no se especifica esta clave, Kaspersky Embedded Systems Security para Windows usará el modo de equipo FTP pasivo, si es posible.
/TIMEOUT:<cantidad de segundos>	Tiempo de espera de conexión del servidor FTP o HTTP. Si no especifica este parámetro, Kaspersky Embedded Systems Security para Windows usará el valor predeterminado de 10 segundos. El valor del parámetro debe ser un número entero.
/REG:<código iso3166>	Configuración regional. Este parámetro se utiliza cuando se reciben actualizaciones de los servidores de actualizaciones de Kaspersky. Kaspersky Embedded Systems Security para Windows minimiza la carga en el dispositivo protegido seleccionando el servidor de actualizaciones más cercano. El valor de este parámetro debe ser el código ISO 3166-1 alfa-2 del país donde se encuentra el dispositivo protegido, por ejemplo /REG: gr o /REG:US. Si se omite esta opción o se especifica un código del país inválido, Kaspersky Embedded Systems Security para Windows detectará la ubicación del dispositivo protegido a través de la configuración regional del dispositivo protegido en el que se encuentre instalada la Consola de la aplicación.
/ALIAS:<alias de la tarea>	Este parámetro le permite asignar un nombre temporal a la tarea, lo que le permite hacer referencia a la tarea mientras se ejecuta. Por ejemplo, se pueden ver las estadísticas de la tarea mediante el comando TASK. El alias de tarea debe ser único entre los alias de tarea de todos los componentes de Kaspersky Embedded Systems Security para Windows. Si no se especificó esta clave, se utiliza un nombre temporal como update_<pid_de_kavshell>, por ejemplo, update_1234. En la Consola de la aplicación, a la tarea se le asigna el nombre "Update-databases <fecha hora>", por ejemplo, Update-databases 16/08/2007 5:41:02 p. m.
/W:<ruta del archivo de registro de tareas>	Si se especifica este parámetro, Kaspersky Embedded Systems Security para Windows guardará el archivo de registro de tareas usando el nombre definido por el valor del parámetro. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos que ocurrieron durante la tarea. El registro se utiliza para registrar eventos definidos por la configuración del registro de tareas y del registro de eventos de Kaspersky Embedded Systems Security para Windows en Visor de eventos. Puede especificar tanto la ruta relativa como la ruta absoluta del archivo de registro. Si se especifica solo un nombre de un archivo sin una ruta, el archivo de registro se creará en la carpeta actual.

	Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo **Registros de tareas** de la Consola de la aplicación. Si Kaspersky Embedded Systems Security para Windows no puede crear el archivo de registro, se mostrará un mensaje de error, pero aun así ejecutará el comando.

Códigos de devolución para el comando KAVSHELL UPDATE.

Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security para Windows: KAVSHELL ROLLBACK

El comando `KAVSHELL ROLLBACK` se puede utilizar para realizar una tarea local del sistema Reversión de la actualización de bases de datos (regresa las bases de datos de Kaspersky Embedded Systems Security para Windows a la versión anteriormente instalada). El comando se realiza sincrónicamente.

Sintaxis del comando

```
KAVSHELL ROLLBACK
```

Códigos de devolución para el comando KAVSHELL ROLLBACK.

Administración de la inspección de registros: KAVSHELL TASK LOG-INSPECTOR

El comando `KAVSHELL TASK LOG-INSPECTOR` puede usarse para supervisar la integridad del entorno a través de un análisis del Registro de eventos de Windows.

Sintaxis del comando

```
KAVSHELL TASK LOG-INSPECTOR
```

Ejemplos del comando

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Opciones o parámetros de línea de comandos para KAVSHELL TASK LOG-INSPECTOR

Parámetro y opción	Descripción
/START	Iniciar la tarea especificada en modo asíncrono.
/STOP	Detener la tarea especificada.
/STATE	Muestra el estado de la tarea actual (por ejemplo, *En ejecución*, *Completada*, *En pausa*, *Detenida*, *Error*, *Iniciando*, *Reanudando*)

/STATISTICS	Recuperar las estadísticas de la tarea: información acerca de la cantidad de objetos procesados desde el inicio de la tarea.

Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR.

Activación de la aplicación. KAVSHELL LICENSE

Las claves de seguridad y los códigos de activación de Kaspersky Embedded Systems Security para Windows se pueden administrar mediante el comando `KAVSHELL LICENSE`.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<archivo de clave | código de activación> [/R] | /DEL:<clave | número de código de activación>]
```

Ejemplos del comando KAVSHELL LICENSE

Para activar la aplicación, ejecute el comando:

```
KAVSHELL.EXE LICENSE /ADD: <código o clave de activación>
```

Para ver información sobre claves agregadas, ejecute el comando:

```
KAVSHELL LICENSE
```

Para eliminar una clave agregada con el número 0000-000000-00000001, ejecute el comando:

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

El comando `KAVSHELL LICENSE` se puede ejecutar con teclas o sin ellas (consulte la tabla a continuación).

Parámetros y opciones de la línea de comandos para KAVSHELL LICENSE

Configuración	Descripción
Sin claves	El comando devuelve la siguiente información sobre las claves agregadas: • Clave. • Tipo de licencia (comercial). • Duración de la licencia asociada a la clave. • Estado de la clave (activa o adicional). Si el estado es *, la clave se agregó como clave adicional.
/ADD:<nombre del archivo de clave o código de activación>	Agregue una clave con el archivo especificado o un código de activación. Se pueden usar variables del entorno del sistema al especificar la ruta a un archivo de clave; no se permiten variables del entorno del usuario.

/R	El código o clave de activación /R es adicional al código o clave de activación /ADD e indica que el código o clave de activación que se agrega es un código o clave de activación adicional.
/DEL:<clave o código de activación>	Elimina la clave con el número o código de activación especificado.

Códigos de devolución para el comando KAVSHELL LICENSE.

Habilitar, configurar y deshabilitar los registros de seguimiento. KAVSHELL TRACE

El comando `KAVSHELL TRACE` se puede utilizar para habilitar y deshabilitar el registro de seguimiento para todos los subsistemas de Kaspersky Embedded Systems Security para Windows y para establecer el nivel de detalle del registro.

Kaspersky Embedded Systems Security para Windows escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado.

Sintaxis del comando KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<ruta a la carpeta con los archivos de seguimiento> [/S:<tamaño máximo del archivo de registro en megabytes>] [/LVL: debug|info|warning|error|critical] [/r:<número máximo de archivos de seguimiento para rotar>] | /OFF>
```

Si el registro de rastreo está habilitado y desea cambiar sus ajustes, ingrese el comando `KAVSHELL TRACE` con la opción /ON y utilice los parámetros /S y /LVL para especificar la configuración del registro de rastreo (consulte la tabla a continuación).

Claves del comando KAVSHELL TRACE

Clave	Descripción
`/ON`	Habilita el registro de rastreo.
`/F:<carpeta con archivos de seguimiento>`	Este parámetro especifica la ruta completa a la carpeta donde se guardarán los archivos de registro de rastreo (obligatorio). Si se especifica la ruta de una carpeta inexistente, no se creará ningún archivo de registro. No es posible especificar las rutas a carpetas en las unidades de red de otros dispositivos protegidos. Si la ruta especificada por el parámetro tiene un espacio, debe estar entre comillas, por ejemplo, /F: "C:\Trace Folder". Se pueden usar variables del entorno del sistema al especificar la ruta a los archivos de registro de rastreo; no se permiten variables del entorno del usuario.
`/S: <tamaño máximo del archivo de registro en megabytes>`	Esta clave establece el tamaño máximo de un único archivo de registro de rastreo. Tan pronto como el archivo de registro alcanza el tamaño máximo, Kaspersky Embedded Systems Security para Windows comenzará

	a registrar información en un archivo nuevo; y el archivo de registro anterior se guardará. Si no se especifica el valor de este parámetro, el tamaño máximo de un archivo de registro será 50 MB.
`/LVL:debug|info|warning|error|critical`	Este parámetro define el nivel de detalle de registro desde máximo (**Toda la información de depuración**) en el que todos los eventos se graban en el registro, hasta mínimo (**Eventos críticos**) en el que solo se registran los eventos críticos. Si no se especifica este parámetro, todos los eventos incluidos en el nivel de detalle **Toda la información de depuración** se registrarán en el registro de rastreo.
`/r:<número máximo de archivos de seguimiento para rotar>`	Esta opción habilita la rotación de archivos de seguimiento. Si la rotación de archivos de seguimiento está habilitada y se alcanza el `<número máximo de archivos de seguimiento para rotar>`, el archivo más antiguo se elimina antes de que se cree un archivo nuevo. Valores disponibles: de 1 a 999. Si no se especifica ningún valor, no se habilita la rotación de archivos de seguimiento y la aplicación devuelve un error.
/OFF	Esta opción deshabilita el registro de rastreo.

Ejemplo del comando KAVSHELL TRACE

*Para habilitar el registro de rastreo mediante el nivel de detalle **Toda la información de depuración** y un tamaño máximo del registro de 200 MB y guardar el archivo de registro en la carpeta C:\Trace Folder, ejecute el comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*Para habilitar el registro de rastreo mediante el nivel de detalle **Eventos importantes** y guardar el archivo de registro en la carpeta C:\Trace Folder, ejecute el comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

*Para habilitar el registro de rastreo con el nivel de detalle **Eventos importantes**, guardar el archivo de registro en la carpeta "C:\Trace Folder" y habilitar la rotación de archivos de rastreo una vez que se alcance un número máximo de 50 archivos de rastreo, ejecute el siguiente comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

Para deshabilitar el registro de rastreo, ejecute el comando:

```
KAVSHELL TRACE /OFF
```

Códigos de devolución para el comando KAVSHELL TRACE.

Desfragmentar los archivos de registro de Kaspersky Embedded Systems Security para Windows. KAVSHELL VACUUM

Puede utilizar el comando `KAVSHELL VACUUM` para desfragmentar los archivos de registro de aplicaciones. Esto ayuda a evitar errores del sistema y de la aplicación debido al almacenamiento de un gran número de archivos de registro que contienen eventos de la aplicación.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Le recomendamos aplicar el comando `KAVSHELL VACUUM` para optimizar el almacenamiento de archivos de registro en caso de que se ejecuten con frecuencia las tareas Actualización y Análisis a pedido. Este comando provoca que Kaspersky Embedded Systems Security para Windows actualice la estructura lógica de los archivos de registro de la aplicación almacenados en un dispositivo protegido en la ruta de acceso especificada.

De forma predeterminada, los archivos de registro de aplicación se almacenan en "C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.3\Reports". Si ha especificado manualmente otra ruta para almacenar registros, el comando `KAVSHELL VACUUM` desfragmenta los archivos en la carpeta especificada en la configuración de registros de Kaspersky Embedded Systems Security para Windows.

Los archivos de gran tamaño aumentan el tiempo requerido para que el comando `KAVSHELL VACUUM` complete la operación de desfragmentación.

Las tareas Protección en tiempo real y Control del equipo no están disponibles al ejecutar el comando `KAVSHELL VACUUM`. El proceso de desfragmentación impide acceder al registro de Kaspersky Embedded Systems Security para Windows e impide que se registren eventos. Para evitar una reducción de protección, le recomendamos planificar cuándo se ejecutará el comando `KAVSHELL VACUUM`.

Para desfragmentar archivos de registro de Kaspersky Embedded Systems Security para Windows, ejecute el comando siguiente:

```
KAVSHELL VACUUM
```

Este comando requiere derechos de cuenta de sistema local.

Limpieza de la base de iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security para Windows emplea la tecnología iSwift, que permite que la aplicación evite que se vuelvan a analizar los archivos que no se modificaron desde el último análisis (**Usar la tecnología iSwift**).

Kaspersky Embedded Systems Security para Windows crea archivos klamfb.dat y klamfb2.dat en la carpeta "%SYSTEMDRIVE%\\System Volume Information". Estos archivos contienen información sobre objetos limpios que ya se han analizado. El archivo klamfb.dat (klamfb2.dat) aumenta con la cantidad de archivos que analiza Kaspersky Embedded Systems Security para Windows. Solo contiene información actual sobre los archivos en el sistema: si un archivo se elimina, Kaspersky Embedded Systems Security para Windows purga la información correspondiente sobre fidbox.dat.

Para borrar un archivo, utilice el comando `KAVSHELL FBRESET`.

Tenga en cuenta las siguientes especificaciones al usar el comando `KAVSHELL FBRESET`:

- Al utilizar el comando KAVSHELL FBRESET para borrar el archivo klamfb.dat, Kaspersky Embedded Systems Security para Windows no pausa la protección (a diferencia de lo que sucede si klamfb.dat se elimina manualmente).

- Kaspersky Embedded Systems Security para Windows puede aumentar la carga de trabajo del dispositivo protegido después de que se borran los datos en klamfb.dat. En este caso, Kaspersky Embedded Systems Security para Windows analiza todos los archivos a los que se accede por primera vez después de borrar klamfb.dat. Después del análisis, Kaspersky Embedded Systems Security para Windows devuelve la información sobre cada objeto analizado a klamfb.dat. Si hay nuevos intentos de acceso a un objeto, la tecnología iSwift previene que se vuelva a analizar el archivo si no se ha modificado.

El comando `KAVSHELL FBRESET` solo está disponible si el intérprete de línea de comando se inicia mediante la cuenta de SYSTEM.

Habilitar y deshabilitar la creación de archivos de volcado. KAVSHELL DUMP

Puede utilizar el comando `KAVSHELL DUMP` para activar o desactivar la creación de instantáneas (archivos de volcado) de los procesos de Kaspersky Embedded Systems Security para Windows si finalizan de manera anormal (consulte la tabla a continuación). Además, puede crear un archivo de volcado de los procesos en ejecución de Kaspersky Embedded Systems Security para Windows en cualquier momento.

Para crear un archivo de volcado correctamente, el comando `KAVSHELL DUMP` se debe ejecutar mediante la cuenta de sistema local (SYSTEM).

Kaspersky Embedded Systems Security para Windows escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado.

El comando KAVSHELL DUMP no se puede utilizar para procesos de x64.

Sintaxis del comando KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<carpeta con el archivo de volcado>|/SNAPSHOT /F:<carpeta con el archivo de volcado> /P:<pid> | /OFF>
```

Parámetros y opciones de la línea de comandos KAVSHELL DUMP

Clave	Descripción
/ON	Permite la creación de un archivo de volcado si un proceso finaliza de manera anormal.
/F:<ruta de la carpeta con archivos de volcado>	Este parámetro es obligatorio. Especifica la ruta a la carpeta donde se guardará el archivo de volcado. No se permiten las rutas de acceso a carpetas en las unidades de red de otros dispositivos no protegidos. Se pueden usar variables del entorno del sistema al especificar la ruta de acceso a la carpeta para el archivo de volcado; no se permiten variables del entorno del usuario.
/SNAPSHOT	Toma una instantánea de la memoria del proceso en ejecución con el PID especificado y guarda el archivo de volcado en la carpeta especificada por el parámetro /F.

/P	El identificador de proceso (PID) se muestra en el Administrador de tareas de Microsoft Windows.
/OFF	Desactiva la creación de un archivo de volcado si un proceso finaliza de manera anormal.

Códigos de devolución para el comando KAVSHELL DUMP.

Ejemplo del comando KAVSHELL DUMP

Para habilitar la creación de un archivo de volcado y guardar el archivo de volcado en la carpeta "C:\Dump Folder", ejecute el comando:

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

Para realizar un volcado para el proceso con el Id. 1234 en la carpeta "C:/Dumps", ejecute el comando:

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

Para deshabilitar la creación de archivos de volcado, ejecute el comando:

```
KAVSHELL DUMP /OFF
```

Importar ajustes. KAVSHELL IMPORT

El comando `KAVSHELL IMPORT` le permite importar la configuración de Kaspersky Embedded Systems Security para Windows y sus tareas actuales de un archivo de configuración a una copia de Kaspersky Embedded Systems Security para Windows en el dispositivo protegido. Se puede crear un archivo de configuración mediante el comando `KAVSHELL EXPORT`.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL IMPORT

```
KAVSHELL IMPORT <nombre del archivo de configuración y ruta del archivo>
```

Ejemplos del comando KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Parámetro de la línea de comandos KAVSHELL IMPORT

Configuración	Descripción
<nombre del archivo de configuración y ruta del archivo>	Nombre del archivo de configuración utilizado como el origen de importación de la configuración. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo; no se permiten variables del entorno del usuario.

Códigos de devolución para el comando KAVSHELL IMPORT.

Exportar ajustes. KAVSHELL EXPORT

El comando `KAVSHELL EXPORT` le permite exportar todos los valores de configuración de Kaspersky Embedded Systems Security para Windows y sus tareas actuales a un archivo de configuración, a fin de importarlos más tarde a copias de Kaspersky Embedded Systems Security para Windows instaladas en otro dispositivo protegido.

Sintaxis del comando KAVSHELL EXPORT

```
KAVSHELL EXPORT <nombre del archivo de configuración y ruta del archivo>
```

Ejemplos del comando KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Parámetros de la línea de comandos KAVSHELL EXPORT

Configuración	Descripción
<nombre del archivo de configuración y ruta del archivo>	Nombre del archivo de configuración que contendrá la configuración. Cualquier extensión de archivo se puede asignar al archivo de configuración. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo; no se permiten variables del entorno del usuario.

Códigos de devolución para el comando KAVSHELL EXPORT.

Integración con Microsoft Operations Management Suite. KAVSHELL OMSINFO

El comando KAVSHELL OMSINFO permite revisar el estado de la aplicación y ver información sobre las amenazas detectadas por las bases de datos antivirus. La información sobre amenazas se obtiene de los registros de eventos disponibles.

Sintaxis del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <ruta de acceso completa al archivo generado con nombre de archivo>
```

Ejemplos del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Parámetro de la línea de comandos KAVSHELL OMSINFO

Configuración	Descripción
<ruta de acceso al archivo generado con nombre de archivo>	El nombre del archivo generado que contendrá información sobre el estado de aplicación y cualquier amenaza detectada.

Administración de la tarea Monitor comparativo de integridad de archivos: KAVSHELL FIM /BASELINE

Puede usar el comando `KAVSHELL FIM /BASELINE` para configurar el modo en el cual la tarea Monitor comparativo de integridad de archivos se ejecuta y supervisa la carga de módulos DLL.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL FIM /BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<área de supervisión> | /L:<ruta a un archivo TXT con una lista de áreas de supervisión>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<id. de línea de base> | /ALIAS:<alias existente>]] | [/EXPORT:<ruta al archivo TXT> [/BL:<id. de línea de base> | /ALIAS:<alias existente>]] | [/SHOW [/BL:<id. de línea de base> | /ALIAS:<alias existente>]] | [/SCAN [/BL:<id. de línea de base> | /ALIAS:<alias existente>]] | [/PWD:<contraseña>]
```

Ejemplos del comando KAVSHELL FIM /BASELINE

Para eliminar una línea base, ejecute el siguiente comando:

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<ID de línea de base>
```

Puede ajustar la configuración de la tarea de Monitor comparativo de integridad de archivos con las opciones para la línea de comandos (vea la tabla a continuación).

Parámetros y opciones de la línea de comandos `KAVSHELL FIM /BASELINE`

Parámetro y opción	Descripción
`/CREATE`	Cree una nueva tarea del Monitor comparativo de integridad de archivos. Kaspersky Embedded Systems Security para Windows iniciará la nueva tarea del Monitor comparativo de integridad de archivos para crear una línea base.
`/L`	Especifique la ruta al archivo TXT que contenga la lista de áreas de supervisión.
`/MD5`	Especifique el algoritmo MD5 para calcular una suma de control (parámetro opcional). El parámetro `/MD5` no puede usarse junto con `/SHA256`. El algoritmo MD5 se usa de forma predeterminada.
`/SHA256`	Especifique el algoritmo SHA256 para calcular una suma de control (parámetro opcional). El parámetro `/SHA256` no puede usarse junto con `/MD5`. El algoritmo MD5 se usa de forma predeterminada.

/SF	Incluye todas las subcarpetas en el área de la tarea del Monitor comparativo de integridad de archivos (parámetro opcional). De forma predeterminada, todas las subcarpetas están excluidas del área de la tarea del Monitor comparativo de integridad de archivos.
/CLEAR	Elimine la línea base con la <ID de línea de base> especificada o la línea base de la tarea con el <alias existente> especificado. Elimine todas las líneas base si no se ha especificado una <ID de línea de base> ni un <alias existente>. Parámetro opcional.
/BL	Especifique la ID exclusiva de una línea base (parámetro opcional).
/EXPORT	Exporte los datos sobre todas las líneas base en un archivo TXT.
/SHOW	Muestre los datos sobre todas las líneas base.
/SCAN	Inicie la nueva tarea del Monitor comparativo de integridad de archivos con la <ID de línea de base> especificada o con el <alias existente> especificado.
/ALIAS	Especifique el nombre de una tarea existente o el nombre de una nueva tarea.
<área de supervisión>	Especifique el archivo o la carpeta que desee incluir en el área de la tarea Monitor comparativo de integridad de archivos. Este parámetro permite especificar solo un área.
<ruta a un archivo TXT con una lista de áreas de supervisión>	Especifique la ruta al archivo TXT que contenga la lista de áreas de supervisión. El archivo debe usar la codificación UTF-8, y cada ruta a un área de supervisión debe estar en una fila distinta.
<ruta de acceso al archivo TXT>	Especifique la ruta al archivo en el que desea exportar los datos sobre todas las líneas base.
<ID de línea de base>	Especifique la ID exclusiva de una línea base. Puede usar el parámetro /SHOW para conocer la ID de una línea base.
<alias existente>	Especifique el nombre de una tarea existente.
<alias nuevo>	Especifique el nombre de una nueva tarea.

Códigos de devolución de comandos

Código de devolución para los comandos KAVSHELL START y KAVSHELL STOP

Código de devolución para los comandos KAVSHELL START y KAVSHELL STOP

Código de devolución	Descripción
0	Operación finalizada correctamente

-3	Error de permisos
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, el servicio de Kaspersky Security ya está en ejecución o detenido)
-7	Servicio no registrado
-8	El inicio de Servicio automático está deshabilitado.
-9	Error en el intento de inicio del dispositivo protegido desde otra cuenta de usuario (de manera predeterminada, el servicio de Kaspersky Security se ejecuta desde la cuenta de usuario Sistema local)
-99	Error desconocido

Código de devolución para los comandos KAVSHELL SCAN y KAVSHELL SCANCRITICAL

Código de devolución para los comandos KAVSHELL SCAN y KAVSHELL SCANCRITICAL

Código de devolución	Descripción
0	La operación se completó correctamente (no se detectaron amenazas)
1	Operación cancelada
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró el archivo con la lista de áreas de análisis)
-5	Sintaxis de comando no válida o área del análisis sin definir
-80	Objetos infectados y otros objetos detectados
-81	Objetos probablemente infectados detectados
-82	Errores de proceso detectados
-83	Objetos sin analizar detectados
-84	Objetos dañados detectados
-85	Error al crear el registro de tareas
-99	Error desconocido
-301	Clave no válida

Código de devolución para el comando KAVSHELL TASK LOG-INSPECTOR

Código de devolución para el comando KAVSHELL TASK LOG-INSPECTOR

Código de devolución	Descripción
0	Operación finalizada correctamente
-6	Operación no válida (por ejemplo, el servicio de Kaspersky Security ya está en ejecución o detenido)

402	La tarea ya se está ejecutando (para la opción /STATE)

Códigos de devolución para el comando KAVSHELL TASK

Códigos de devolución para el comando KAVSHELL TASK

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la tarea)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la tarea no se está ejecutando, ya se está ejecutando o no se puede pausar)
-99	Error desconocido
-301	Clave no válida
401	La tarea no se está ejecutando (para la opción /STATE)
402	La tarea ya se está ejecutando (para la opción /STATE)
403	La tarea ya está en pausa (para la opción /STATE)
-404	Operación fallida (debido a un cambio en el estado de la tarea)

Códigos de devolución para el comando KAVSHELL RTP

Códigos de devolución para el comando KAVSHELL RTP

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró ninguna de las tareas Protección del equipo en tiempo real)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la tarea ya está en ejecución o detenida)
-99	Error desconocido
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL UPDATE

Códigos de devolución para el comando KAVSHELL UPDATE

Código de devolución	Descripción
0	Operación finalizada correctamente
200	Todos los objetos están actualizados (base de datos o componentes del programa actuales)
-2	El servicio no está en ejecución
-3	Error de permisos
-5	Sintaxis de comando no válida
-99	Error desconocido
-206	Faltan archivos de extensión en la fuente especificada o estos tienen un formato desconocido
-209	Error al conectarse al origen de la actualización
-232	Error de autenticación al conectarse al servidor proxy
-234	Error al conectarse a Kaspersky Security Center
-235	Kaspersky Embedded Systems Security para Windows no fue autenticado al conectarse al origen de la actualización
-236	Las bases de datos de la aplicación están dañadas
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL ROLLBACK

Códigos de devolución para el comando KAVSHELL ROLLBACK

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-99	Error desconocido
-221	Copia de seguridad de la base de datos no encontrada o dañada
-222	Copia de seguridad de la base de datos dañada

Códigos de devolución para el comando KAVSHELL LICENSE

Códigos de devolución para el comando KAVSHELL LICENSE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Privilegios insuficientes para administrar claves

-4	No se encontró la clave con el número especificado
-5	Sintaxis de comando no válida
-6	Operación no válida (clave ya agregada)
-99	Error desconocido
-301	Clave no válida
-303	La licencia se aplica a una aplicación diferente

Códigos de devolución para el comando KAVSHELL TRACE

Códigos de devolución para el comando KAVSHELL TRACE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la ruta especificada para la carpeta de registros de rastreo)
-5	Sintaxis de comando no válida
-6	Operación no válida (intento de ejecutar el comando KAVSHELL TRACE /OFF cuando los registros de rastreo ya están deshabilitados)
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL FBRESET

Códigos de devolución para el comando KAVSHELL FBRESET

Código de devolución	Descripción
0	Operación finalizada correctamente
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL DUMP

Códigos de devolución para el comando KAVSHELL DUMP

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la ruta especificada para la carpeta del archivo de volcado; no se encontró el proceso con el PID especificado)

-5	Sintaxis de comando no válida
-6	Operación no válida (intento de ejecución del comando KAVSHELL DUMP/OFF si la creación de archivos de volcado ya está deshabilitada)
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL IMPORT

Códigos de devolución para el comando KAVSHELL IMPORT

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se puede encontrar un archivo de configuración que pueda importarse)
-5	Sintaxis no válida
-99	Error desconocido
501	La operación finalizó correctamente con un error/comentario, por ejemplo, Kaspersky Embedded Systems Security para Windows no importó los parámetros para algunos componentes funcionales
-502	Falta el archivo de importación o el formato no se reconoce
-503	Configuración incompatible (archivo de configuración exportado desde un programa diferente o desde una versión posterior e incompatible de Kaspersky Embedded Systems Security para Windows)

Códigos de devolución para el comando KAVSHELL EXPORT

Códigos de devolución para el comando KAVSHELL EXPORT

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-5	Sintaxis no válida
-10	No es posible crear el archivo de configuración (por ejemplo, no hay acceso a la carpeta especificada en la ruta del archivo)
-99	Error desconocido
501	La operación finalizó correctamente con error/comentario, por ejemplo, Kaspersky Embedded Systems Security para Windows no exportó los parámetros para algunos componentes funcionales

Códigos de devolución para el comando KAVSHELL FIM /BASELINE

Códigos de devolución para el comando KAVSHELL FIM /BASELINE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la tarea)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la línea base ya se eliminó)
-10	No es posible crear el archivo de configuración (por ejemplo, no hay acceso a la carpeta especificada en la ruta del archivo)
-12	Contraseña no válida
-80	No coincide con los objetos de línea base detectados
-85	Error al crear el registro de tareas
-99	Error interno
-303	Clave de licencia no válida
-502	La tarea no se está ejecutando
200	Todos los objetos coinciden con la línea base
501	Tarea completada con éxito con un error/comentario

Comunicarse con el soporte técnico

Esta sección describe cómo se puede recibir soporte técnico y las condiciones en las cuales se encuentra disponible.

Cómo acceder al Servicio de soporte técnico

Si no encuentra una solución a su problema en la documentación de la aplicación ni en ninguna de las fuentes de información sobre la aplicación, le recomendamos que se comunique con el Servicio de soporte técnico. Los especialistas del soporte técnico responderán sus preguntas acerca de la instalación y el uso de la aplicación.

El soporte técnico se encuentra disponible solo para los usuarios que adquirieron una licencia comercial de la aplicación. El soporte técnico no está disponible para los usuarios que tienen una licencia de prueba.

Se brinda soporte para la aplicación de acuerdo con el ciclo de vida de la aplicación (consulte la página del ciclo de vida de la aplicación).

Antes de comunicarse con el Servicio de soporte técnico, lea rápidamente las reglas del Servicio de soporte técnico.

Puede contactar al soporte técnico enviando una solicitud al Servicio de soporte técnico de Kaspersky por medio del portal de Kaspersky CompanyAccount.

Soporte técnico mediante Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para empresas que usan aplicaciones de Kaspersky. Kaspersky CompanyAccount está diseñado para facilitar la interacción entre usuarios y especialistas de Kaspersky mediante solicitudes en línea. El portal de Kaspersky CompanyAccount le permite supervisar el progreso del procesamiento de solicitud electrónico por parte de especialistas de Kaspersky y almacenar un historial de solicitudes electrónicas.

Puede registrar a todos los empleados de su organización en una única cuenta de usuario en Kaspersky CompanyAccount. Una única cuenta le permite administrar de manera centralizada las solicitudes electrónicas de empleados registrados en Kaspersky y también gestionar los privilegios de dichos empleados mediante Kaspersky CompanyAccount.

Kaspersky CompanyAccount se encuentra disponible en los siguientes idiomas:

- Inglés
- Español
- Italiano
- Alemán
- Polaco
- Portugués

- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del Servicio de soporte técnico.

Uso de archivos de rastreo y scripts AVZ

Después de informar un problema a los especialistas del Servicio de soporte técnico de Kaspersky, es posible que le soliciten que genere un informe con datos sobre el funcionamiento de Kaspersky Embedded Systems Security para Windows y que lo envíe al Servicio de soporte técnico de Kaspersky. También es posible que los especialistas del servicio de soporte técnico de Kaspersky le pidan que cree un archivo de rastreo. El archivo de rastreo le permite seguir el proceso de cómo se llevan a cabo los comandos de la aplicación, paso a paso, a fin de determinar la etapa de funcionamiento de la aplicación en la que se produce el error.

Luego de analizar los datos que envíe, los especialistas de soporte técnico de Kaspersky pueden crear un script AVZ y enviárselo. Mediante los scripts AVZ es posible analizar procesos activos en busca de amenazas, analizar el dispositivo protegido en busca de amenazas, desinfectar o eliminar archivos infectados y crear informes de análisis del sistema.

Glosario

Actualización

El proceso de sustituir o agregar archivos nuevos (bases de datos o módulos de la aplicación) obtenidos de los servidores de actualizaciones de Kaspersky.

Analizador heurístico

Una tecnología para detectar amenazas sobre la información que aún no se ha agregado a las bases de datos de Kaspersky. El analizador heurístico detecta objetos que, por su comportamiento, pueden ser una amenaza para la seguridad del sistema operativo. Los objetos detectados por el analizador heurístico se consideran probablemente infectados. Por ejemplo, un objeto se puede considerar posiblemente infectado si contiene secuencias de comandos que son habituales de objetos maliciosos (abrir archivo, escribir en el archivo).

Archivo comprimido

Uno o varios archivos empaquetados en un solo archivo a través de la compresión. Se requiere una aplicación dedicada, denominada archivador, para comprimir y descomprimir los datos.

Archivo infectable

Un archivo que, debido a su estructura o formato, puede ser utilizado por criminales como "contenedor" para almacenar y extender código malicioso. Como regla general, se trata de archivos ejecutables con extensiones de archivo como .exe, .com y .dll. El riesgo de que se introduzca código malicioso en estas clases de archivos es bastante elevado.

Bases de datos antivirus

Bases de datos que contienen información sobre amenazas a la seguridad de los equipos que son conocidas por Kaspersky a la fecha de publicación de las bases de datos antivirus. Las entradas de la base de datos antivirus permiten detectar código malicioso en los objetos analizados. Las bases de datos antivirus son creadas por los expertos de Kaspersky y se actualizan cada hora.

Clave activa

Una clave que está siendo utilizada por la aplicación.

Configuración de tareas

Configuración de la aplicación específica para cada tipo de tarea.

Copia de seguridad

Espacio de almacenamiento especial destinado a guardar copias de seguridad de los objetos antes de que se los desinfecte o elimine.

Cuarentena

Carpeta a la que la aplicación Kaspersky pasa los objetos probablemente infectados que se han detectado. Los objetos se almacenan en Cuarentena de forma cifrada con el fin de evitar cualquier efecto en el equipo.

Desinfección

Método de procesamiento de objetos infectados que produce una recuperación total o parcial de datos. No todos los objetos infectados se pueden desinfectar.

Directiva

Una directiva define la configuración de la aplicación y gestiona la capacidad de configurar la aplicación en los equipos de un grupo de administración. Debe crearse una directiva particular para cada aplicación. Puede crear múltiples directivas para aplicaciones instaladas en equipos en cada grupo de administración, pero solo se puede aplicar una directiva por vez a cada aplicación de forma simultánea dentro de un grupo de administración.

Estado de protección

El estado de protección vigente en un momento dado, el cual caracteriza el nivel de seguridad del dispositivo.

Falso positivo

Situación en la cual una aplicación de Kaspersky considera que un objeto no infectado lo está porque su código es similar al de un virus.

Importancia de un evento

Propiedad de un evento encontrada durante la operación de una aplicación de Kaspersky. Hay cuatro niveles de importancia:

- Evento crítico
- Fallo funcional
- Advertencia

- Información

Los eventos de un mismo tipo pueden tener niveles de gravedad diferentes según la situación en la cual ocurren.

Kaspersky Security Network (KSN)

Infraestructura de servicios en la nube que brinda acceso a la base de conocimientos en línea de Kaspersky sobre la reputación de archivos, recursos web y software. El uso de los datos de Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápido a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la posibilidad de encontrar falsos positivos.

Máscara de archivo

Representación de un nombre de archivo en la que se utilizan caracteres genéricos. Los caracteres que más se utilizan en las máscaras de archivo son * y ? (* representa una cadena de cualquier largo formada por caracteres cualesquiera, mientras que ? representa cualquier carácter individual).

Nivel de seguridad

Un nivel de seguridad es un conjunto predefinido de ajustes de configuración para los componentes.

Objeto infectado

Objeto en el que una sección de código coincide completamente con una sección del código de una amenaza conocida. Los expertos de Kaspersky recomiendan no trabajar con estos objetos.

Objeto OLE

Un objeto vinculado a otro archivo o integrado en otro archivo a través del uso de la tecnología Object Linking and Embedding (OLE). Un ejemplo de un objeto OLE es una hoja de cálculo de Microsoft Office Excel® integrada en un documento de Microsoft Office Word.

Objetos de inicio

Un conjunto de aplicaciones necesario para que el sistema operativo y el software que está instalado en el equipo se inicie y funcione correctamente. Estos objetos se ejecutan cada vez que se inicia el sistema operativo. Hay virus capaces de infectar específicamente estos objetos y que pueden conducir, por ejemplo, al bloqueo del inicio del sistema operativo.

Periodo de vigencia de la licencia

El período de tiempo durante el cual puede utilizar las funciones de la aplicación y los servicios adicionales. La cantidad de funciones y de servicios adicionales disponibles depende del tipo de licencia.

Servidor de administración

Un componente de Kaspersky Security Center que almacena de forma central información sobre todas las aplicaciones de Kaspersky que se instalan en la red corporativa y que administra esas aplicaciones.

SIEM

Siglas en inglés del término "administración de información y eventos de seguridad". Se trata de una solución para administrar la información y los eventos del sistema de seguridad de una organización.

Tarea

Las funciones realizadas por la aplicación de Kaspersky se implementan como tareas, por ejemplo: Protección de archivos en tiempo real, Análisis completo del equipo y Actualización de bases de datos.

Tarea local

Una tarea que se define y se ejecuta en un equipo cliente individual.

Vulnerabilidad

Una falla en un sistema operativo o una aplicación que pueden utilizar los programadores de malware para penetrar en el sistema operativo o la aplicación y corromper su integridad. La presencia de una gran cantidad de vulnerabilidades en el sistema operativo lo vuelven poco fiable, pues los virus que penetran en el sistema operativo pueden modificar el propio sistema y las aplicaciones que en él se instalan.

Información sobre código de terceros

La información sobre código de terceros se encuentra en el archivo denominado legal_notices.txt, en la carpeta de instalación de la aplicación.

Avisos de marcas registradas

Las marcas comerciales registradas y las marcas de servicio son propiedad de sus respectivos titulares.

Domino, Lotus y Lotus Notes son marcas comerciales de International Business Machines Corporation, registradas en muchas jurisdicciones en todo el mundo.

Intel y Pentium son marcas comerciales de Intel Corporation en los Estados Unidos y/u otros países.

Linux es la marca comercial registrada de Linus Torvalds en los Estados Unidos y otros países.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, PowerShell, Outlook, SharePoint, SQL Server, Windows, Windows Server, Windows Vista y Windows XP son marcas comerciales del grupo de empresas Microsoft.

CVE es una marca comercial registrada de The MITRE Corporation.

UNIX es una marca comercial registrada en los Estados Unidos y otros países, licenciada exclusivamente a través de X/Open Company Limited.