# ESET Small Business Security 18

## Manual de usuario

Haga clic aquí para ver la versión de la Ayuda de este documento

Digital Security
Progress. Protected.

ESET Small Business Security 18 está desarrollado por ESET, spol. s r.o.

Para obtener más información, visite https://www.eset.com.



Soporte técnico: https://support.eset.com

REV. 02/04/2025

# Small office products

# ESET Small Business Security

ESET Small Business Security representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ESET LiveGrid®, combinada con el cortafuegos personalizado y los módulos antispam, garantiza la protección del ordenador gracias a su velocidad y precisión. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que podrían amenazar su ordenador.

ESET Small Business Security es una solución de seguridad completa que combina la protección máxima con un impacto mínimo en el sistema. Nuestras tecnologías avanzadas utilizan la inteligencia artificial para evitar la infiltración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

## Características de ESET Small Business Security

| | |
|---|---|
| **Banca y navegación seguras** | Banca y navegación seguras proporciona un navegador protegido para acceder a pasarelas de banca o pago a través de Internet para asegurar que se realizan todas las transacciones en un entorno fiable y seguro. |
| **Compatibilidad con firmas de red** | Las firmas de red permiten una rápida identificación y bloquean el tráfico malicioso de entrada y salida de los dispositivos de usuarios, como bots y paquetes que aprovechan vulnerabilidades. Esta característica puede considerarse como una mejora de la Protección contra botnets. |
| **Cortafuegos inteligente** | Impide que los usuarios no autorizados tengan acceso a su ordenador y se aprovechen de sus datos personales. |
| **Antispam del cliente de correo electrónico** | Representa hasta el 50 % de todas las comunicaciones por correo electrónico. El Antispam del cliente de correo electrónico protege de este problema. |
| **Antirrobo** | Antirrobo amplía la seguridad en el nivel del usuario en el caso de que el ordenador se pierda o lo roben. Cuando instala ESET Small Business Security y Antirrobo, el dispositivo se incluye en la interfaz web. La interfaz web le permite gestionar la configuración de Antirrobo y administrar las funciones de Antirrobo en su dispositivo. |
| **Password Manager** | Password Manager que protege y almacena sus contraseñas y datos personales. |
| **Secure Data** | Secure Data le permite cifrar datos en su ordenador y unidades extraíbles para evitar el uso indebido de información privada y confidencial. |
| **ESET LiveGuard** | Detecta y detiene amenazas nunca vistas y procesa información de cara a detecciones futuras. |
| **VPN** | Mantenga los datos seguros, evite el seguimiento no deseado y mejore la privacidad con la seguridad adicional que ofrece una dirección IP anónima. |

Una suscripción debe estar activa para que las funciones de ESET Small Business Security estén operativas. Le recomendamos que renueve su suscripción varias semanas antes de que caduque la suscripción a ESET Small Business Security.

# Novedades

## Novedades de ESET Small Business Security 18.1

- Gestión de extensiones que no son de confianza en Banca y navegación seguras
- Actualizaciones de nuevos elementos en el menú desplegable Archivos de registro
- Estructura de configuración avanzada mejorada
- Corrección de errores y otras pequeñas mejoras

Para desactivar **las notificaciones de novedades**:
1. Abra Configuración avanzada > **Notificaciones** > **Notificaciones en el escritorio**.
2. Haga clic en **Editar** junto a **Notificaciones en el escritorio**.
3. Desmarque la casilla **Mostrar notificaciones de novedades**. A continuación, haga clic en **Aceptar**.
Para obtener más información sobre las notificaciones, consulte la sección Notificaciones.

Para obtener una lista detallada de los cambios realizados en ESET Small Business Security, consulte los registros de cambios de ESET Small Business Security.

# ¿Qué producto tengo?

ESET ofrece diversos niveles de seguridad con nuevos productos, desde una solución antivirus rápida y potente, hasta una solución de seguridad integral que ocupa un espacio mínimo en el sistema:

- **ESET Safe Server**
- **ESET Small Business Security**

Para saber el producto que tiene instalado, abra la ventana principal del programa y verá el nombre del producto en la parte superior de la ventana (consulte el artículo de la Base de conocimiento).

---

En la siguiente tabla se detallan las funciones disponibles en cada uno de los productos.

| | ESET Safe Server | ESET Small Business Security |
|---|---|---|
| Motor de detección | ✔ | ✔ |
| Aprendizaje automático avanzado | ✔ | ✔ |
| Bloqueador de exploits | ✔ | ✔ |
| Protección contra ataques basados en scripts | ✔ | ✔ |
| Anti-Phishing | ✔ | ✔ |
| Protección del acceso a la Web | ✔ | ✔ |
| HIPS (incluida la Protección contra ransomware) | ✔ | ✔ |
| Antispam | | ✔ |
| Cortafuegos | | ✔ |

| | ESET Safe Server | ESET Small Business Security |
|---|---|---|
| Inspector de red | | ✔ |
| Protección de cámara web | | ✔ |
| Protección contra los ataques de red | | ✔ |
| Protección contra botnets | | ✔ |
| Banca y navegación seguras | | ✔ |
| Privacidad y seguridad del navegador | | ✔ |
| Antirrobo | | ✔ |
| Password Manager | | ✔ |
| ESET Secure Data | | ✔ |
| ESET LiveGuard | | ✔ |
| ESET Folder Guard | | ✔ |
| VPN | | ✔ |

Puede que algunos de los productos anteriores no estén disponibles para su idioma o zona geográfica. Consulte la disponibilidad de ESET Small Business Security para obtener más información.

# Requisitos del sistema

Para que ESET Small Business Security funcione de forma óptima, su sistema debe cumplir los siguientes requisitos de hardware y software:

## Procesadores compatibles

Procesador Intel o AMD, de 32 bits (x86) con conjunto de instrucciones SSE2 o de 64 bits (x64), 1 GHz o más procesador de tipo ARM64, 1 GHz o superior

## El sistema operativo es compatible

Microsoft® Windows® 11

Microsoft® Windows® 10

La compatibilidad con Azure Code Signing debe estar instalada en todos los sistemas operativos Windows para instalar o actualizar los productos ESET publicados a partir de julio de 2023. Más información.

Intente siempre mantener actualizado su sistema operativo.

## Requisitos de las funciones de ESET Small Business Security

Consulte los requisitos del sistema para funciones de ESET Small Business Security concretas en la tabla que aparece a continuación:

| Característica | Requisitos |
|---|---|
| Intel® Threat Detection Technology | Consulte los procesadores compatibles. |

| Característica | Requisitos |
| --- | --- |
| Banca y navegación seguras | Consulte los navegadores web compatibles. |
| Fondo transparente | Versión para Windows 10 RS4 o posteriores. |
| Limpieza del sistema | Procesador que no está basado en ARM64. |
| Bloqueador de exploits | Procesador que no está basado en ARM64. |
| Análisis profundo de inspección de comportamiento | Procesador que no está basado en ARM64. |

### Otros

Para que la activación y las actualizaciones de ESET Small Business Security funcionen correctamente, se necesita conexión a Internet.

La ejecución simultánea de dos programas antivirus en un mismo dispositivo provoca conflictos inevitables de recursos del sistema, como una ralentización del sistema que lo hace inservible.

# Prevención

Cuando trabaje con el ordenador y, especialmente, cuando navegue por Internet, tenga en cuenta que ningún sistema antivirus del mundo puede eliminar completamente el riesgo de que se produzcan amenazas detectadas y ataques remotos. Para disfrutar de una protección y una comodidad máximas, es esencial usar correctamente su solución antivirus y cumplir varias reglas útiles:

## Actualización regular

De acuerdo con las estadísticas de ESET LiveGrid®, cada día se crean miles de nuevas amenazas únicas para burlar las medidas de seguridad existentes y proporcionar un beneficio a sus autores, todo ello a costa de otros usuarios. Los especialistas del laboratorio de investigación de ESET analizan estas amenazas diariamente y preparan y publican actualizaciones para mejorar continuamente el nivel de protección para los usuarios.

Para garantizar la máxima eficacia de estas actualizaciones es importante que estén bien configuradas en el sistema. Para obtener más información sobre cómo configurar las actualizaciones, consulte el capítulo Configuración de actualizaciones.

## Descarga de parches de seguridad

Los autores de software malintencionado con frecuencia explotan varias vulnerabilidades del sistema para aumentar la eficacia de la propagación de códigos malintencionados. Por ello, las empresas de software vigilan de cerca las nuevas vulnerabilidades en las aplicaciones y publican actualizaciones de seguridad para eliminar amenazas potenciales periódicamente.

Es importante descargar estas actualizaciones de seguridad a medida que se publican. Microsoft Windows y los navegadores web como Internet Explorer son dos ejemplos de programas que publican de forma periódica actualizaciones de seguridad.

## Copia de seguridad de los datos importantes

Normalmente, a los autores de código malicioso no les importan las necesidades de los usuarios y, con frecuencia, la actividad de los programas malintencionados provoca un funcionamiento incorrecto del sistema operativo y la

pérdida de datos importantes.

Es importante realizar copias de seguridad periódicas de sus datos importantes y confidenciales en una fuente externa, como un DVD o un disco duro externo. Estas precauciones facilitan y aceleran la recuperación de los datos en caso de fallo del sistema.

## Análisis regular del ordenador en busca de virus

El módulo de protección del sistema de archivos en tiempo real se encarga de la detección de los virus, gusanos, troyanos y rootkits, conocidos o no. Esto significa que cada vez que entra en un archivo o lo abre, este se analiza en busca de actividad de código malicioso. Recomendamos que realice un análisis completo del ordenador al menos una vez al mes, ya que las firmas de códigos maliciosos pueden variar y el motor de detección se actualiza todos los días.

## Seguimiento de las reglas de seguridad básicas

Esta es la regla más útil y eficaz de todas: sea siempre cauto. Actualmente, muchas amenazas requieren la intervención del usuario para su ejecución y distribución. Si es precavido a la hora de abrir archivos nuevos, se ahorrará mucho tiempo y esfuerzo en la desinfección de amenazas. Estas son algunas directrices útiles:

- No visite sitios web sospechosos con varios elementos y anuncios emergentes.
- Tenga cuidado al instalar programas gratuitos, paquetes codec, etc. Use únicamente programas seguros y solo visite sitios web seguros.
- Tenga cuidado a la hora de abrir archivos adjuntos de correo electrónico, especialmente los de mensajes masivos y de remitentes desconocidos.
- No use la cuenta de administrador para realizar su trabajo diario en el ordenador.

# Páginas de Ayuda

Le damos la bienvenida a la guía del usuario de ESET Small Business Security. Esta información se proporciona para que presentarle el producto y como ayuda para que el ordenador sea más seguro.

## Introducción

Antes de usar ESET Small Business Security, puede buscar información sobre los diversos tipos de detecciones y ataques remotos que puede encontrarse al utilizar el ordenador.

Comience instalando ESET Small Business Security. Si ya ha instalado ESET Small Business Security, consulte Trabajo con ESET Small Business Security.

## Cómo utilizar las páginas de Ayuda de ESET Small Business Security

La ayuda en línea se divide en varios capítulos y subcapítulos. Pulse **F1** en ESET Small Business Security para consultar información sobre la ventana abierta actualmente.

El programa le permite buscar un tema de ayuda por palabra clave, así como escribir palabras o frases para realizar búsquedas de contenido. La diferencia entre estos dos métodos es que una palabra clave puede estar

relacionada de forma lógica con las páginas de Ayuda que no contienen esa palabra clave determinada en el texto. La búsqueda por palabras y frases se realiza en el contenido de todas las páginas y muestra únicamente las que contienen la palabra o fase buscada en el texto real.

Por motivos de coherencia y para evitar confusiones, la terminología empleada en esta guía se basa en los nombres de parámetros de la interfaz de usuario de ESET Small Business Security. Además, utilizamos una serie de símbolos uniformes para destacar temas de interés o importancia especial.

Una nota es simplemente una breve observación. A pesar de que puede omitirlas, las notas contienen información valiosa como características específicas o un vínculo a un tema relacionado.

Este tipo de notas requieren su atención, y le recomendamos no omitir la información que incluyen. Normalmente ofrece información que no es vital, pero sí importante.

Se trata de información que requiere más atención y cautela. Las advertencias se incluyen específicamente para evitar que cometa errores potencialmente peligrosos. Lea y comprenda el texto, ya que hace referencia a una configuración del sistema muy delicada o a algún aspecto del sistema que conlleva ciertos riesgos.

Este es un caso o ejemplo práctico cuyo objetivo es ayudarle a comprender cómo se utiliza una determinada función o característica.

| Convención | Significado |
|---|---|
| **Negrita** | Nombre de elementos de la interfaz, como recuadros y botones de opción. |
| *Cursiva* | Marcadores de posición de la información que proporcione. Por ejemplo, nombre de archivo o ruta de acceso significa que debe escribir la ruta de acceso real o un nombre de un archivo. |
| `Courier New` | Ejemplos de código o comandos. |
| Hipervínculo | Permite acceder de un modo rápido y sencillo a temas con referencias cruzadas o a una ubicación web externa. Los hipervínculos aparecen resaltados en color azul, y pueden estar subrayados. |
| *%ProgramFiles%* | El directorio del sistema Windows en el que se encuentran los programas instalados en Windows. |

La **ayuda en línea** es la fuente principal de contenido de ayuda. Siempre que tenga una conexión a Internet activa, se mostrará la versión más reciente de la ayuda en línea.

# Instalación

Hay varios métodos para instalar ESET Small Business Security en su ordenador. Los métodos de instalación pueden variar en función del país y del medio de distribución:

- Live Installer: se descarga del sitio web de ESET o se obtiene de un CD o DVD. El paquete de instalación es universal para todos los idiomas (elija el idioma correspondiente). El Live Installer es un archivo pequeño; los archivos adicionales necesarios para la instalación de ESET Small Business Security se descargan automáticamente.

- Instalación sin conexión: utiliza un archivo .exe más grande que el archivo de Live Installer y no necesita una conexión a Internet ni archivos adicionales para completar la instalación.

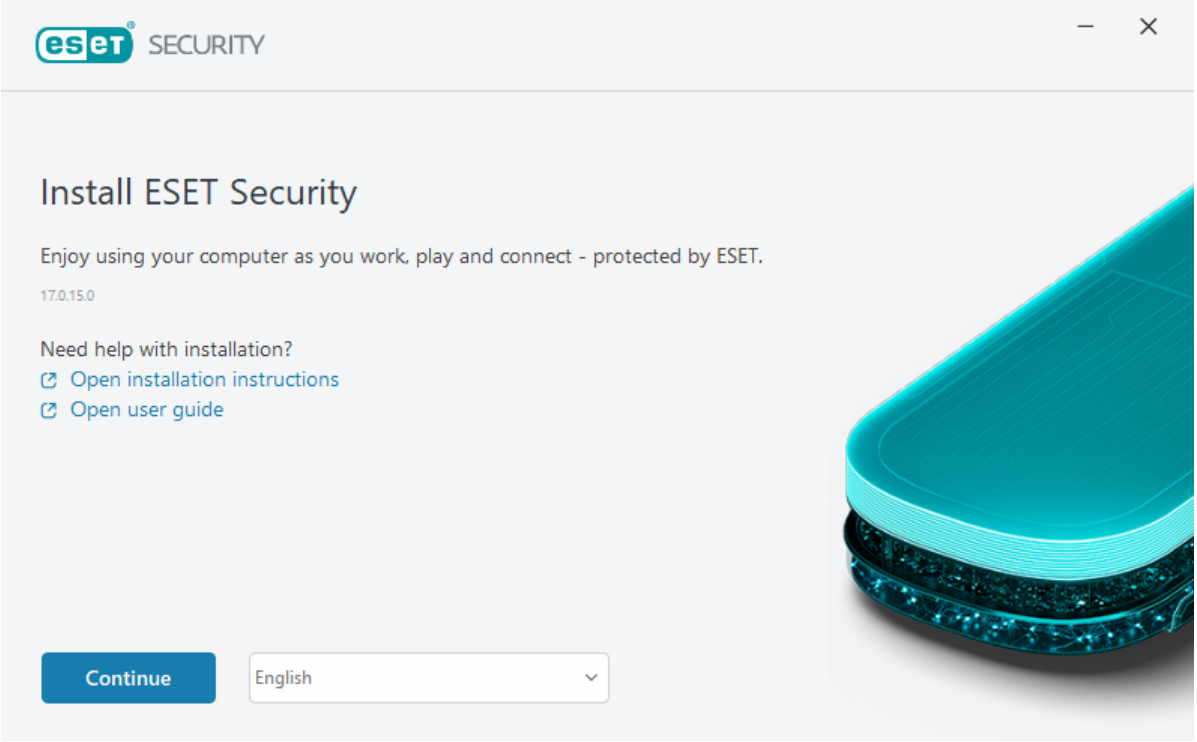
Asegúrese de que no tenga instalados otros programas antivirus en el ordenador antes de instalar ESET Small Business Security. Si instala más de dos soluciones antivirus en un solo ordenador, estas pueden entrar en conflicto. Le recomendamos que desinstale del sistema uno de los programas antivirus. Consulte nuestro artículo de la base de conocimiento para ver una lista de herramientas de desinstalación para software antivirus habitual (disponible en inglés y algunos otros idiomas).

En este video, ESET le guía durante el proceso de descarga e instalación de ESET Small Business Security para proteger su pequeña empresa:

# Live installer

Cuando haya descargado el paquete de instalación de Live installer, haga doble clic en el archivo de instalación y siga las instrucciones paso a paso del Asistente de instalación.

Para este tipo de instalación debe estar conectado a Internet.




1. Seleccione el idioma correspondiente en el menú desplegable y haga clic en **Continuar**.

Si está instalando una versión más reciente sobre la versión anterior con ajustes protegidos mediante contraseña, escriba la contraseña. Puede configurar la contraseña de configuración en la Configuración de acceso.

2. Seleccione su preferencia para las siguientes funciones, lea el Acuerdo de licencia para el usuario final y la Política de privacidad, y haga clic en **Continuar**, o haga clic en **Permitir todo y continuar** para activar todas las funciones:

- Sistema de respuesta de ESET LiveGrid®
- Aplicaciones potencialmente indeseables
- Programa de mejora de la experiencia de los clientes

Al hacer clic en **Continuar** o en **Permitir todo y continuar**, acepta el Acuerdo de licencia para el usuario final y la Política de privacidad.

3. Para activar, administrar y ver la seguridad del dispositivo desde ESET HOME, conecte el dispositivo a la cuenta de ESET HOME. Haga clic en **Omitir inicio de sesión** para continuar sin conectarse a ESET HOME. Puede conectar su dispositivo a su cuenta de ESET HOME más tarde.

4. Si sigue sin conectarse a ESET HOME, elija una opción de activación. Si está instalando una versión más reciente sobre la anterior, su **clave de activación** se introducirá automáticamente.

5. El Asistente de instalación determina qué producto de ESET se instala según su suscripción. Se preselecciona la versión con más funciones de seguridad. Haga clic en **Continuar** para iniciar el proceso de instalación. Podría llevarle unos momentos.

Si quedan restos (archivos o carpetas) de productos de ESET desinstalados anteriormente, se le pedirá que permita su eliminación. Haga clic en **Instalar** para continuar.

6. Haga clic en **Hecho** para salir del Asistente de instalación.

Solucionador de problemas de instalación.

Una vez instalado y activado el producto, empiezan a descargarse los módulos. La protección se está inicializando, y es posible que algunas funciones no estén totalmente disponibles hasta que se complete la descarga.

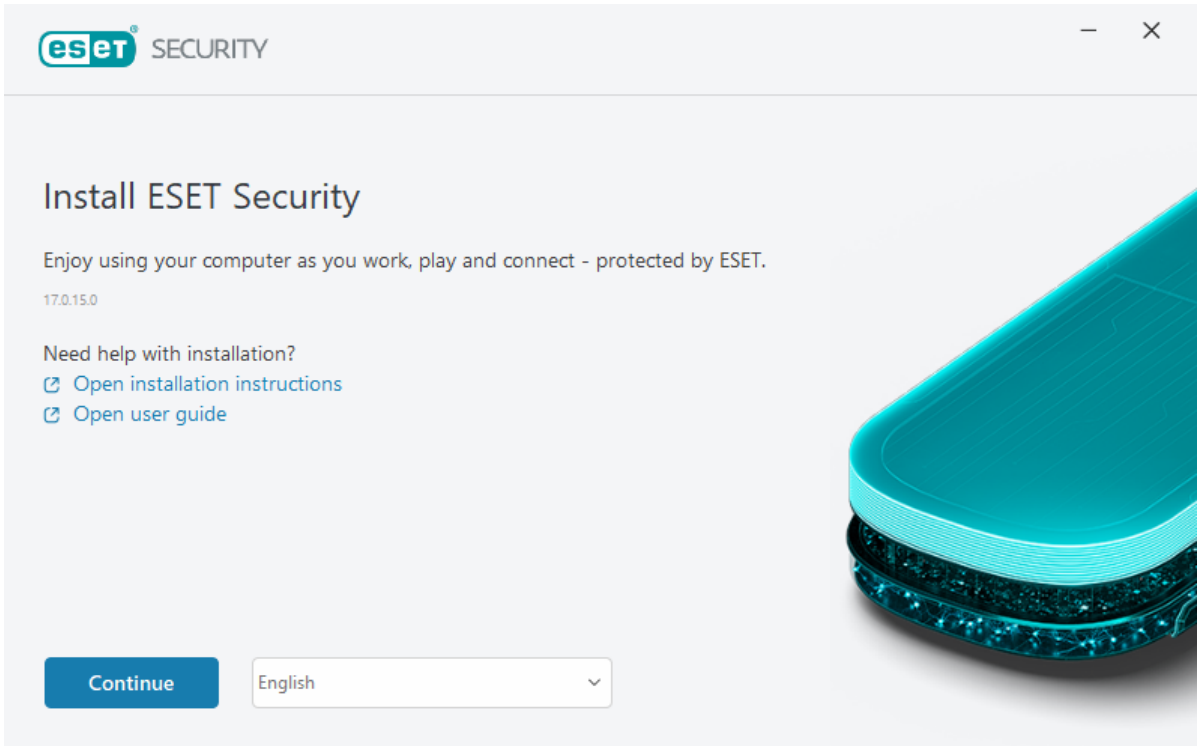
# Instalación sin conexión

Descargue e instale su producto para oficina pequeña de ESET para Windows utilizando el instalador sin conexión (.exe) que aparece a continuación. Elija la versión del producto de ESET para oficina pequeña que desea descargar (32 bits, 64 bits o ARM).

| ESET Safe Server | ESET Small Business Security |
|---|---|
| Descargar versión para 64 bits<br>Descargar versión para 32 bits<br>Descargar ARM | Descargar versión para 64 bits<br>Descargar versión para 32 bits<br>Descargar ARM |

Si tiene una conexión a Internet activa, instale el producto de ESET con un Live Installer.

Una vez iniciada la instalación sin conexión (.exe), el Asistente de instalación le guía durante el proceso de configuración.




1. Seleccione el idioma correspondiente en el menú desplegable y haga clic en **Continuar**.

Si está instalando una versión más reciente sobre la versión anterior con ajustes protegidos mediante contraseña, escriba la contraseña. Puede configurar la contraseña de configuración en la Configuración de acceso.

2. Seleccione su preferencia para las siguientes funciones, lea el Acuerdo de licencia para el usuario final y la Política de privacidad, y haga clic en **Continuar**, o haga clic en **Permitir todo y continuar** para activar todas las funciones:

- Sistema de respuesta de ESET LiveGrid®
- Aplicaciones potencialmente indeseables
- Programa de mejora de la experiencia de los clientes

Al hacer clic en **Continuar** o en **Permitir todo y continuar**, acepta el Acuerdo de licencia para el usuario final y la Política de privacidad.

3. Haga clic en **Omitir inicio de sesión**. Si tiene una conexión a Internet, puede conectar su dispositivo a su cuenta de ESET HOME.

4. Haga clic **Omitir activación**. ESET Small Business Security debe activarse después de su instalación para que sea totalmente funcional, debe activarse después de la instalación. La activación del producto requiere una conexión a Internet activa.

5. El Asistente de instalación muestra qué producto de ESET se instalará según el instalador sin conexión descargado. Haga clic en **Continuar** para iniciar el proceso de instalación. Podría llevarle unos momentos.

Si quedan restos (archivos o carpetas) de productos de ESET desinstalados anteriormente, se le pedirá que permita su eliminación. Haga clic en **Instalar** para continuar.

6. Haga clic en **Hecho** para salir del Asistente de instalación.

Solucionador de problemas de instalación.

# Solucionador de problemas de instalación

Si se producen problemas durante la instalación, el asistente de instalación proporciona un solucionador de problemas que, si es posible, resuelve el problema.

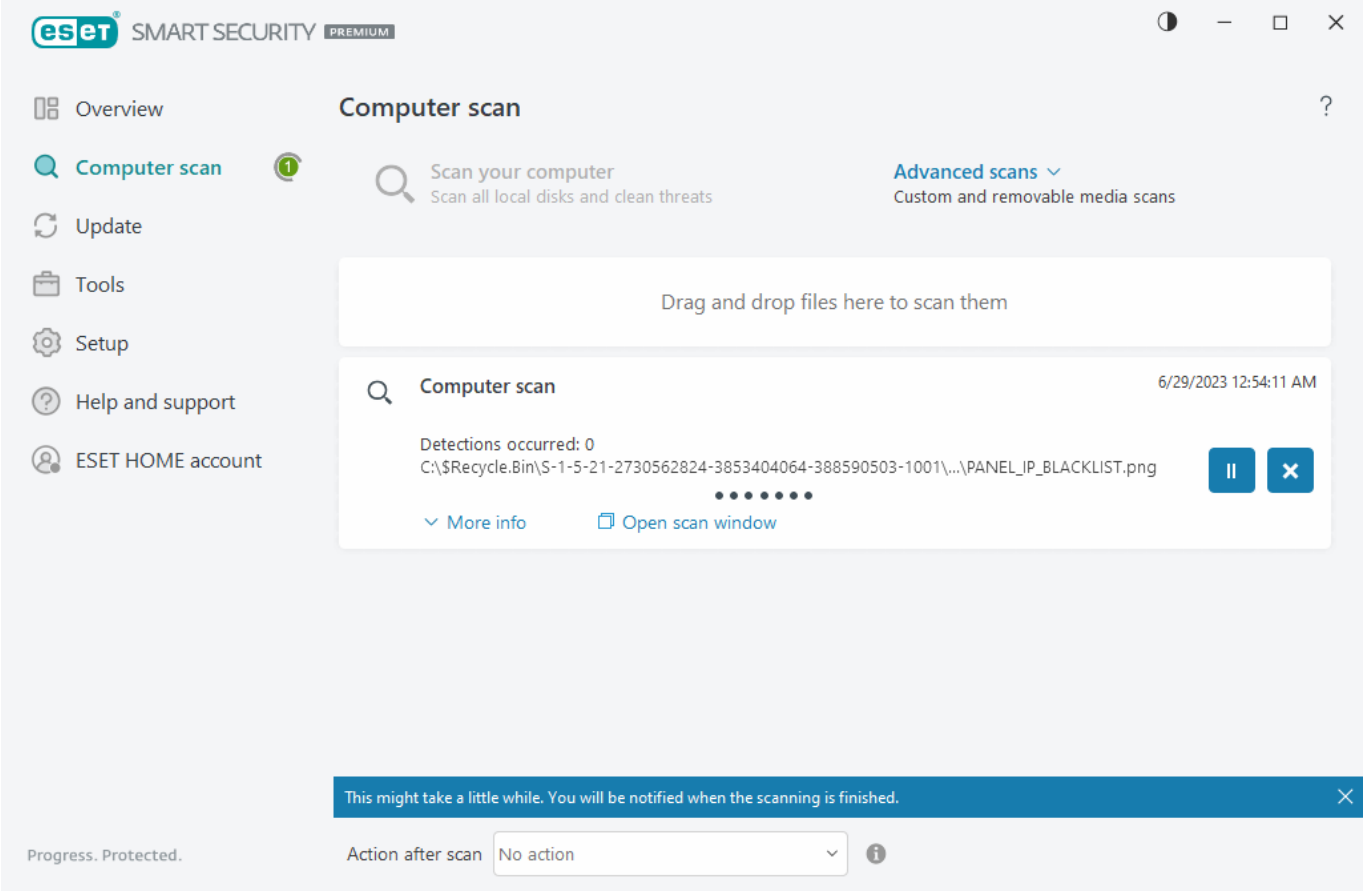
Haga clic en **Ejecutar el solucionador de problemas** para iniciar el solucionador de problemas. Cuando termine el solucionador de problemas, siga la solución recomendada.

Si el problema persiste, consulte la lista de errores de instalación comunes y resoluciones.

# Analizar primero tras la instalación

Después de instalar ESET Small Business Security, comenzará automáticamente un análisis del ordenador después de la primera actualización realizada con éxito para comprobar si existe código malicioso.

También puede iniciar un análisis del ordenador manualmente desde la ventana principal del programa > **Análisis del ordenador** > **Análisis del ordenador**. Encontrará más información sobre los análisis del ordenador en Análisis del ordenador.



# Actualización a una versión más reciente

Las versiones nuevas de ESET Small Business Security implementan mejoras o solucionan problemas que no se pueden arreglar con las actualizaciones automáticas de los módulos de programa. La actualización a una versión posterior se puede realizar de varias maneras:

1. Actualización automática mediante una actualización del programa.
Las actualizaciones del programa se distribuyen a todos los usuarios y pueden afectar a determinadas configuraciones del sistema, de modo que se envían tras un largo periodo de pruebas que garantizan su funcionalidad en todas las configuraciones posibles del sistema. Si necesita instalar una versión más reciente en cuanto se publica, utilice uno de los métodos que se indican a continuación.
Asegúrese de que ha activado **Actualizaciones de características de la aplicación** en Configuración avanzada > **Actualizar** > **Perfiles** > **Actualizaciones**.

2. Manualmente, en la ventana principal del programa, haciendo clic en **Buscar actualizaciones** en la sección **Actualización**.

3. Actualización manual mediante la descarga e instalación de una versión más reciente sobre la instalación existente.

Si desea obtener información adicional e instrucciones con ilustraciones, consulte:

- Actualizar productos de ESET: buscar los módulos más recientes de los productos
- ¿Cuáles son los diferentes tipos de versiones y actualizaciones de los productos de ESET?

# Actualización automática de productos anteriores

La versión de su producto de ESET ya no es compatible y su producto se ha actualizado a la versión más reciente.

Problemas de instalación comunes

Cada nueva versión de productos de ESET contiene numerosas correcciones de errores y mejoras. Los clientes existentes que tengan una suscripción válida para un producto de ESET pueden actualizar a la versión más reciente del mismo producto de forma gratuita.

Para finalizar la instalación:

1. Haga clic en **Aceptar y continuar** para aceptar Acuerdo de licencia para el usuario final y la Política de privacidad. Si no acepta el Acuerdo de licencia para el usuario final, haga clic en **Desinstalar**. No puede volver a la versión anterior.

2. Haga clic en **Permitir todo y continuar** para permitir tanto el Sistema de respuesta ESET LiveGrid® como el Programa de mejora de la experiencia de los clientes, o haga clic en **Continuar** si no quiere participar.

3. Tras activar el nuevo producto de ESET con la clave de activación, se mostrará la página Información general. Si no se encuentra la información de su suscripción, continúe con una versión de prueba gratuita. Si su suscripción utilizada en el producto anterior no es válida, active su producto de ESET.

4. Es necesario reiniciar el dispositivo para completar la instalación.

# Se instalará ESET Small Business Security

Este cuadro de diálogo puede mostrarse:

- Durante el proceso de instalación: haga clic en **Continuar** para instalar ESET Small Business Security.
- Al cambiar una suscripción en ESET Small Business Security: haga clic en **Activar** para cambiar la suscripción y activar ESET Small Business Security.

# Registro

Rellene los campos del formulario de registro y haga clic en **Activar** para registrar su suscripción. Los campos marcados entre paréntesis son obligatorios. La información se utilizará exclusivamente para cuestiones relacionadas con su suscripción de ESET.

# Progreso de la activación

El dispositivo tardará unos segundos en completar el proceso de activación (el tiempo necesario puede variar en función de la velocidad de la conexión a Internet o su ordenador).

# La activación se ha realizado correctamente

El proceso de activación está completado. Siga el asistente posterior a la instalación para finalizar la configuración de ESET Small Business Security.

En unos segundos se procederá a actualizar el módulo. Las actualizaciones periódicas de ESET Small Business Security se iniciarán inmediatamente.

Se realizará un análisis inicial automáticamente durante los 20 minutos posteriores a la actualización del módulo.

> El proceso de activación se puede interrumpir si la oferta no está asociada con ESET HOME. Inicie sesión en su ESET HOME o cree una cuenta.

# Activación del producto

Hay varios métodos disponibles para activar su producto. La disponibilidad de una situación concreta de activación en la ventana de activación puede variar en función del país y de los medios de distribución (CD/DVD, página web de ESET, etc.):

- Si ha adquirido una versión en caja física del producto o ha recibido un mensaje de correo electrónico con los datos de la suscripción, haga clic en **Utilizar la clave de activación adquirida** para activar su producto. Para una correcta activación, la clave de activación se debe introducir tal como se proporciona. Clave de activación: se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX y sirve para identificar al propietario de la suscripción y activar la suscripción. Normalmente, la clave de activación se encuentra en el interior o en la parte posterior del paquete del producto.

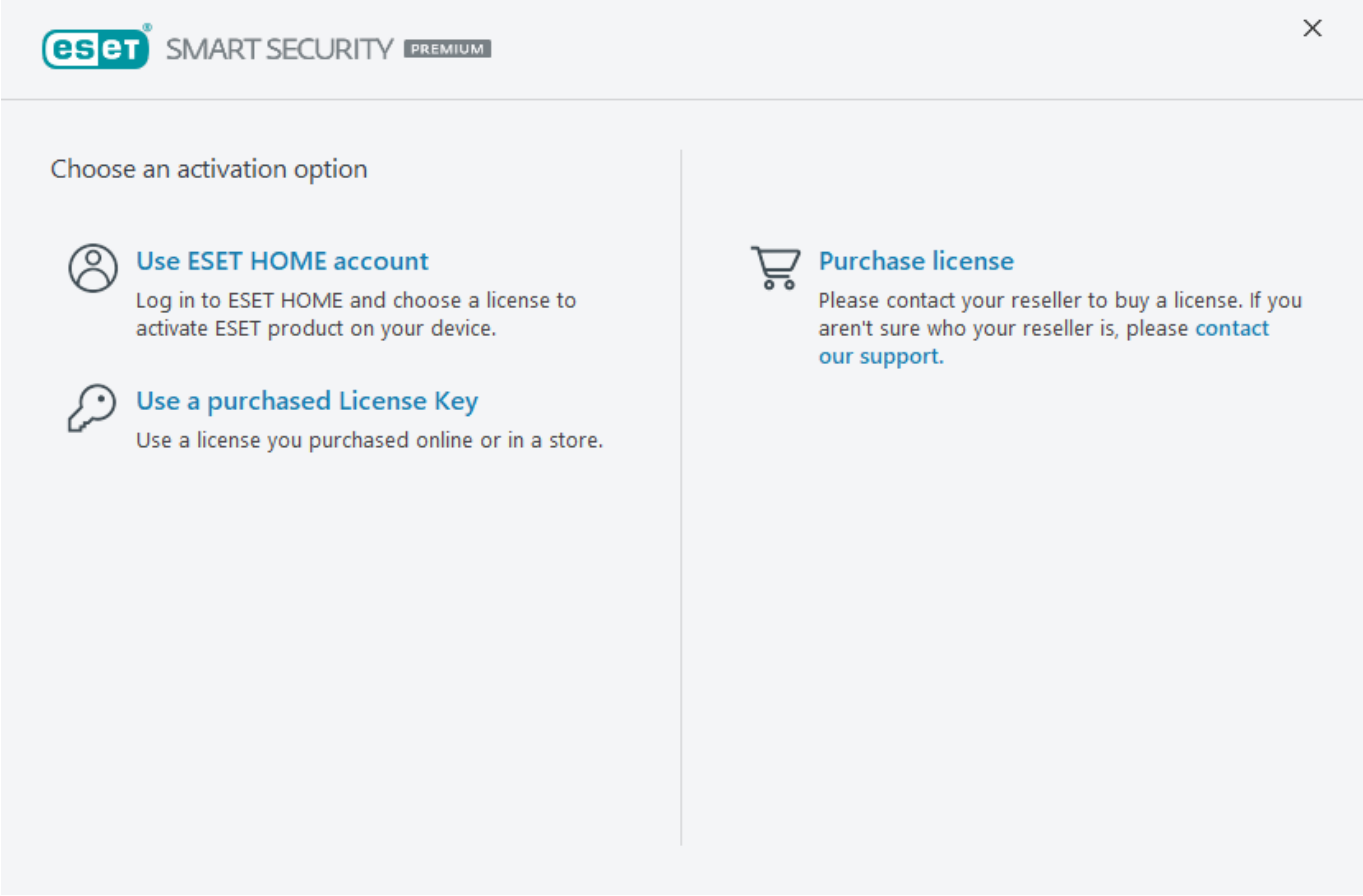
• Tras seleccionar Utilizar una cuenta de ESET HOME, se le pedirá que inicie sesión en su cuenta de ESET HOME.

• Si desea evaluar ESET Small Business Security antes de adquirir el producto, seleccione la opción Prueba gratuita. Introduzca su dirección de correo electrónico y el país para activar ESET Small Business Security durante un período de tiempo limitado. Se le enviará por correo electrónico su versión de prueba gratuita. Las versiones de prueba gratuitas solo se pueden activar una vez por cliente.

• Si no tiene una suscripción y quiere comprar una, haga clic en **Comprar una suscripción**. Se le redirigirá al sitio web del distribuidor local de ESET. Las suscripciones a productos para oficina pequeña de ESET para Windows no son gratuitas.

Puede cambiar su suscripción al producto en cualquier momento. Para ello, haga clic en **Ayuda y soporte** > **Cambiar suscripción** en la ventana principal del programa. Verá el ID público utilizado para identificar su suscripción en el soporte de ESET.

⚠ ¿Se produjo un error durante la activación del producto?




# Introducir la clave de activación durante la activación

Las actualizaciones automáticas son importantes para su seguridad. ESET Small Business Security solo recibirá las actualizaciones cuando se active.

Cuando introduzca su **Clave de activación**, es importante que la escriba exactamente tal y como está escrita. La clave de activación es una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la suscripción y activarla.

Se recomienda copiar y pegar su clave de activación desde el correo electrónico de registro para garantizar la exactitud.

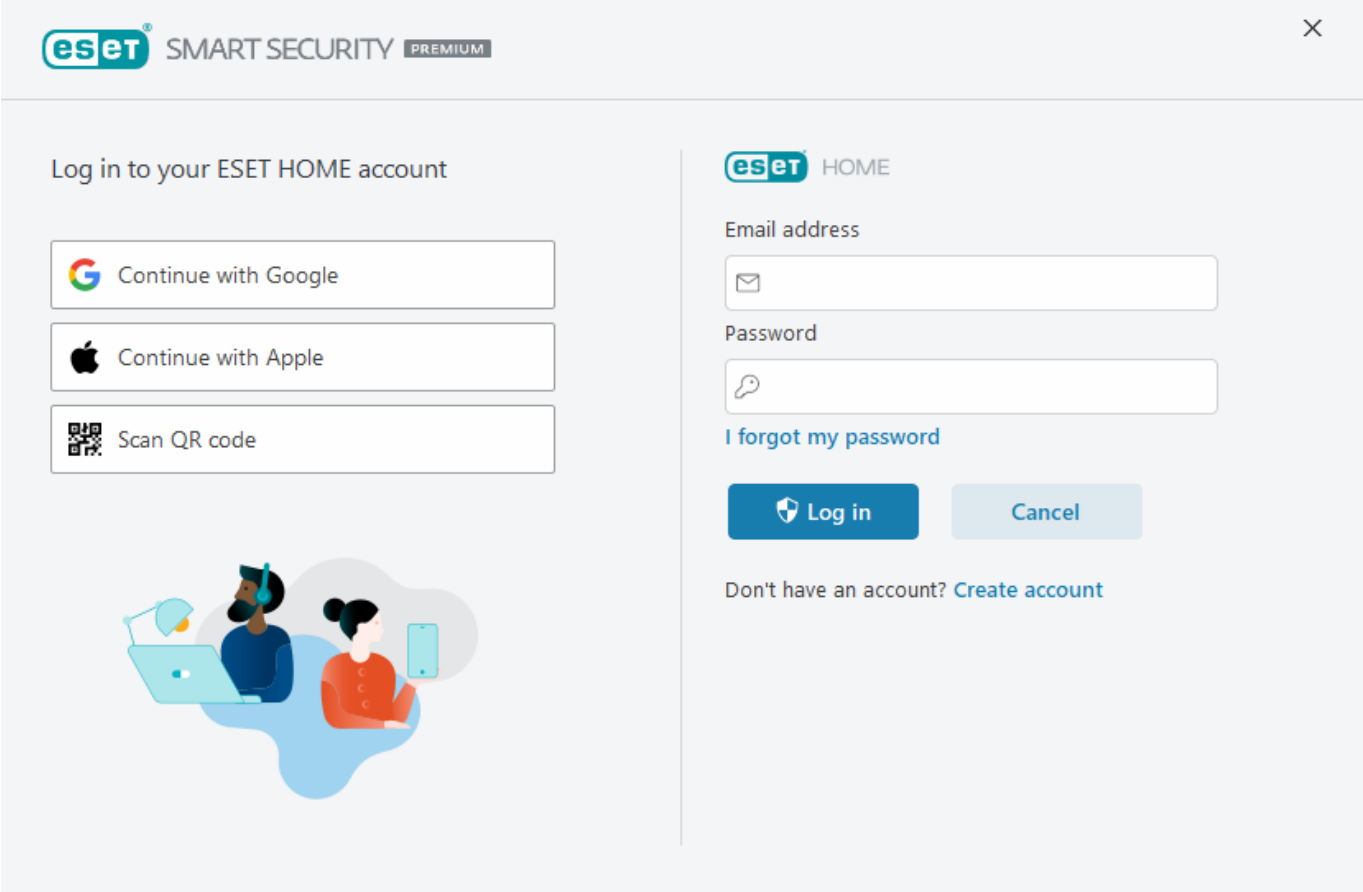
Si no introduce la Clave de activación tras la instalación del producto, este no se activará. Puede activar ESET Small Business Security en la ventana principal del programa > **Ayuda y asistencia técnica** > **Activar la suscripción**.

Las suscripciones a productos para oficina pequeña de ESET para Windows no son gratuitas.

# Cuenta de ESET HOME

Conecte el dispositivo a ESET HOME para ver y administrar todas las suscripciones ESET activadas y los dispositivos. Puede renovar, actualizar o ampliar la suscripción y ver detalles importantes sobre ella.

En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar suscripciones distintas, descargar productos en sus dispositivos, consultar el estado de seguridad del producto o compartir suscripciones por correo electrónico. Para obtener más información, visite la ayuda en línea de ESET HOME.




Tras seleccionar **Usar cuenta de ESET HOME** como método de activación o al conectar a la cuenta de ESET HOME durante la instalación:

1. Inicie sesión en su cuenta ESET HOME.

Si no tiene una cuenta de ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de ESET HOME.
Si ha olvidado su contraseña, haga clic en **He olvidado mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la Ayuda en línea de ESET HOME.

2. Configure el **Nombre del dispositivo** que se utilizará en todos los servicios ESET HOME y haga clic en **Continuar**.

3. Elija una suscripción para la activación o agregue una nueva suscripción. Haga clic en **Continuar** para activar ESET Small Business Security.

# Activar el periodo de prueba gratuito

Para activar su versión de prueba de ESET Small Business Security, escriba una dirección de correo electrónico válida en los campos **Dirección de correo electrónico** y **Confirmar dirección de correo electrónico**. Tras la activación, se generará la suscripción de ESET, y se le enviará por correo electrónico. Esta dirección de correo electrónico también se utilizará para las notificaciones de caducidad del producto y otro tipo de información de ESET. La versión de prueba gratuita solo puede activarse una vez.

Seleccione el país en el menú desplegable **País** para registrar ESET Small Business Security con su distribuidor local, que le proporcionará asistencia técnica.

# Clave de activación gratuita de ESET

La suscripción a ESET Small Business Security no es gratuita. La clave de activación de ESET es una secuencia única de letras y números separados por un guion que ESET facilita para permitir el uso legal de ESET Small Business Security conforme al Acuerdo de licencia para el usuario final.

Cada usuario final tiene derecho a utilizar la clave de activación solo en la medida en que tiene derecho a utilizar ESET Small Business Security según el número de puestos concedidos por ESET. La clave de activación se considera confidencial y no se puede compartir. Sin embargo, puede compartir una suscripción mediante ESET HOME.

Es posible que encuentre en Internet claves de activación de ESET "gratuitas", pero recuerde:

- Si hace clic en un anuncio de «Suscripción gratuita de ESET", puede poner en peligro su ordenador o su dispositivo e infectarlos con malware. El malware puede estar oculto en contenido web no oficial (como vídeos), sitios web en los que se muestren anuncios para ganar dinero por sus visitas, etc. Normalmente, esto es una trampa.

- ESET puede desactivar las suscripción pirateadas, y lo hace.

- Tener una Clave de activación pirateada no cumple el Acuerdo de licencia para el usuario final que debe aceptar para instalar ESET Small Business Security.

- Compre la suscripción a ESET solo a través de canales oficiales, como www.eset.com o distribuidores de ESET (no compre una suscripción en sitios web no oficiales de terceros como eBay ni una suscripción compartida de terceros).

- La descarga de un ESET Small Business Security es gratuita, pero la activación durante la instalación requiere una clave de activación de ESET válida (puede descargar e instalar el producto, pero, si no lo activa, no funcionará).

- No comparta su suscripción en Internet ni en redes sociales (puede llegar a muchas personas).

Para identificar y denunciar suscripciónes de ESET pirateadas, visite el artículo de la Base de conocimiento.

---

Si tiene dudas a la hora de comprar un producto de seguridad ESET, puede utilizar una versión de prueba hasta que se decida:

1. Active ESET Small Business Security con una versión de prueba
2. Participe en el Programa BETA de ESET
3. Instale ESET Mobile Security si utiliza un dispositivo móvil Android: es freemium

Para obtener un descuento o ampliar su suscripción, renueve ESET.

# Error de activación: situaciones habituales

Si la activación de ESET Small Business Security no se realiza correctamente, las causas más habituales son:

- La clave de activación ya está en uso.
- Ha introducido una clave de activación no válida.
- La información en el formulario de activación no existe o no es válida.
- Error al establecer la comunicación con el servidor de activación.
- Sin conexión con los servidores de activación de ESET o con conexión desactivada.

Compruebe que ha introducido la clave de activación correcta y que su conexión a Internet está activa. Intente activar ESET Small Business Security de nuevo. Si utiliza una cuenta de ESET HOME para la activación, consulte la ayuda en línea sobre las suscripciones y la administración de suscripciones a ESET HOME.

> Si recibe un error específico (por ejemplo, suscripción suspendida o suscripción sobreutilizada), siga las instrucciones que se indican en el estado de la suscripción.

Si sigue sin poder activarla ESET Small Business Security, el Solucionador de problemas de activación de ESET le guía por preguntas habituales, errores y problemas de activación y licencia (disponible en inglés y en otros idiomas).

# Estado de suscripción

Su suscripción puede tener diferentes estados. Puede encontrar el estado de su suscripción en ESET HOME. Para agregar la suscripción a su cuenta de ESET HOME, consulte Agregar una suscripción.

> Si no tiene la cuenta de ESET HOME, puede crear una nueva cuenta de ESET HOME.

Si el estado de la suscripción no es **Activo**, recibirá un error durante la activación o una notificación en la ventana principal del programa.

Para desactivar las notificaciones del estado de la suscripción, abra Configuración avanzada > **Notificaciones** > **Estados de la aplicación**. Haga clic en **Editar** junto a **Estados de la aplicación**, expanda **Licencias** y desmarque la casilla de verificación situada junto a la notificación que quiera desactivar. Desactivar la notificación no soluciona el problema.

Consulte descripciones y soluciones recomendadas para diferentes estados de la suscripción en la siguiente tabla:

| Estado de suscripción | Descripción | Solución |
|---|---|---|
| Activo | La suscripción es válida, por lo que no es necesario que haga nada. ESET Small Business Security puede activarse, y usted puede consultar los detalles de la suscripción en la ventana principal del programa > **Ayuda y asistencia técnica**. | |
| Sobreutilizada | Esta suscripción la están utilizando más dispositivos que los que permite. Recibirá un error de activación. | Consulte Error de activación debido a suscripción sobreutilizada para obtener más información. |
| Suspendida | Su suscripción se ha suspendido debido a problemas de pago. Para usar la suscripción, asegúrese de que sus datos de pago en ESET HOME estén actualizados o póngase en contacto con el distribuidor de la suscripción. Puede recibir este error durante la activación o en la ventana principal del programa. | Producto instalado: si tiene una cuenta de ESET HOME, en la notificación mostrada en la ventana principal del programa, haga clic en **Administrar suscripción en ESET HOME** y revise sus datos de pago. De lo contrario, póngase en contacto con el distribuidor de la suscripción.<br><br>Error de activación: si tiene una cuenta de ESET HOME, en la ventana del error de activación, haga clic en **Abrir ESET HOME** y revise sus datos de pago. De lo contrario, póngase en contacto con el distribuidor de la suscripción. |
| Expiró | La suscripción ha caducado, por lo que no puede utilizarla para activar ESET Small Business Security. Puede recibir este error durante la activación o en la ventana principal del programa. Si ya tiene instalado ESET Small Business Security, el ordenador no está protegido ni actualizado. | Producto instalado: en la notificación que se muestra en la ventana principal del programa, haga clic en **Renovar la suscripción** y siga las instrucciones en ¿Cómo renuevo la suscripción?. También puede hacer clic en **Activar producto** y escoger un método de activación.<br><br>Error de activación: en la ventana del error de activación, haga clic en **Renovar la suscripción** y siga las instrucciones en ¿Cómo renuevo la suscripción?. También puede escribir una clave de activación nueva o renovada y hacer clic en **Renovar suscripción**. |

| Estado de suscripción | Descripción | Solución |
|---|---|---|
| Cancelada | Su suscripción ha sido cancelada por ESET o por su distribuidor de suscripciones. | Si recibe un error: Suscripción cancelada en la ventana principal del programa o durante la activación y su suscripción debería funcionar correctamente, póngase en contacto con su distribuidor de suscripciones. |

# Error de activación debido a suscripción sobreutilizada

## Problema

- Es posible que haya abusado de su suscripción o esté sobreutilizada.
- Error de activación debido a suscripción sobreutilizada

## Solución

Esta suscripción la están utilizando más dispositivos que los que permite la misma. Puede que sea víctima de pirateo o falsificación de software. La suscripción no se puede usar para activar ningún otro producto de ESET.

Puede resolver este problema directamente si tiene la posibilidad de gestionar la suscripción en su cuenta de ESET HOME o de comprar la suscripción desde una fuente legítima. Si aún no tiene una cuenta, cree una.

Si es el propietario de una licencia y no se le ha solicitado que introduzca su dirección de correo electrónico:

1. Para administrar su suscripción de ESET, abra un navegador web y vaya a https://home.eset.com. Acceda a ESET License Manager y quite o desactive puestos. Si desea obtener más información, consulte Qué hacer en caso de suscripción sobreutilizada.

2. Para identificar y denunciar suscripciones de ESET pirateadas, visite el artículo sobre cómo identificar y notificar suscripciones de ESET pirateadas para ver instrucciones.

3. Si no está seguro, haga clic en **Atrás** y envíe un mensaje de correo electrónico al equipo de asistencia técnica de ESET.

Si no es el propietario de una suscripción, póngase en contacto con el propietario de esta suscripción e indique que no puede activar el producto de ESET debido a la sobreutilización de la suscripción. El propietario puede resolver el problema en el portal ESET HOME.

Si se le pide que confirme su dirección de correo electrónico (solo varios casos), introduzca la dirección de correo que usó inicialmente para comprar o activar su ESET Small Business Security.

# Introducción

En este capítulo se proporciona una descripción general inicial de ESET Small Business Security y su configuración básica.

# Icono en la bandeja del sistema

Algunas de las opciones y características de configuración más importantes están disponibles al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema .

**Pausar protección**: muestra el cuadro de diálogo de confirmación que desactiva el Motor de detección, que protege el sistema frente a ataques maliciosos al sistema mediante el control de archivos, Internet y la comunicación por correo electrónico. En el menú desplegable **Intervalo de tiempo** puede especificar durante cuánto tiempo se desactivará la protección.


**Pausar cortafuegos (permitir todo el tráfico)**: pone el cortafuegos en un estado inactivo. Consulte Red para obtener más información.

**Bloquear todo el tráfico de red**: bloquea todo el tráfico de red. Puede activarlo de nuevo al hacer clic en **Detener bloqueo de todo el tráfico de red**.

**Configuración avanzada**: abre la configuración avanzada de ESET Small Business Security. Para abrir la configuración avanzada desde la ventana principal del producto, pulse F5 en el teclado o haga clic en **Configuración** > **Configuración avanzada**.

Archivos de registro: los archivos de registro contienen información acerca de todos los sucesos importantes del programa y proporcionan información general acerca de las detecciones.

**Abrir ESET Small Business Security**: abre la ventana principal del programa de ESET Small Business Security.

**Restablecer disposición de la ventana**: esta opción restablece el tamaño y la posición predeterminados de la ventana de ESET Small Business Security.

**Modo de color**: abre los ajustes de la interfaz de usuario, donde puede cambiar el color.

**Buscar actualizaciones**: inicia un módulo o una actualización del producto para garantizar su protección. ESET Small Business Security busca actualizaciones automáticamente varias veces al día.

Acerca de: contiene información del sistema y detalles acerca de la versión instalada de ESET Small Business Security, los módulos del programa instalados, el sistema operativo y los recursos del sistema.

# Accesos directos del teclado

Para facilitar la navegación por ESET Small Business Security, puede utilizar los siguientes accesos directos del teclado:

| Accesos directos del teclado | Acción |
|---|---|
| F1 | abre las páginas de ayuda |
| F5 | abre la Configuración avanzada |
| Flecha arriba/flecha abajo | Navegación por los elementos del menú desplegable |
| TAB | Ir al siguiente elemento de la interfaz gráfica de usuario en una ventana |
| Shift+TAB | Ir al elemento anterior de la interfaz gráfica de usuario en una ventana |
| ESC | cierra el cuadro de diálogo activo |
| Ctrl+U | muestra información sobre la suscripción de ESET y su ordenador (detalles para el servicio de soporte técnico) |
| Ctrl+R | restablece la ventana del producto al tamaño y la posición predeterminados en la pantalla |
| ALT + Flecha izquierda | Volver |
| ALT + Flecha derecha | Ir hacia delante |
| ALT+Home | Ir a inicio |

También puede utilizar los botones del ratón hacia atrás o hacia delante para la navegación.

# Perfiles

El administrador de perfiles se utiliza en dos secciones de ESET Small Business Security: en **Análisis a petición** y en **Actualización**.

## Análisis del ordenador

Hay 4 perfiles de análisis predefinidos en ESET Small Business Security:

- **Análisis inteligente** – este es el perfil de análisis avanzado predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se han comprobado estaban desinfectados en un análisis anterior y no se han modificado desde ese análisis. Esto permite reducir el tiempo de análisis y la repercusión en la seguridad del sistema.

- **Análisis del menú contextual** – puede iniciar un análisis a petición de cualquier archivo desde el menú contextual. El perfil de análisis del menú contextual le permite definir la configuración del análisis que se utilizará cuando active el análisis de esta forma.

- **Análisis exhaustivo** – De forma predeterminada, el perfil de análisis exhaustivo no utiliza la optimización inteligente, por lo que no se excluye ningún archivo del análisis con este perfil.

- **Análisis del ordenador** – este es el perfil predeterminado que se utiliza en el análisis estándar del ordenador.

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Análisis a petición** > **Lista de perfiles** > **Editar**. En la ventana **Administrador de perfiles** encontrará el menú desplegable **Perfil**

**seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

> Supongamos que desea crear su propio perfil de análisis y parte de la configuración de **Análisis del ordenador** es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar la opción **Reparar la detección siempre**. Introduzca el nombre del nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione un perfil nuevo en el menú desplegable **Perfil seleccionado**, ajuste los demás parámetros según sus requisitos y haga clic en **Aceptar** para guardar el nuevo perfil.

## Actualización

El editor de perfiles de Configuración de actualizaciones le permite crear nuevos perfiles de actualización. Cree y utilice sus propios perfiles personalizados (es decir, distintos al predeterminado **Mi perfil**) únicamente si su ordenador utiliza varios medios para conectarse a servidores de actualización.

Por ejemplo, un ordenador portátil que normalmente se conecta a un servidor local (Mirror) de la red local, pero descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (en viajes de negocios) podría utilizar dos perfiles: el primero para conectarse al servidor local y el segundo, a los servidores de ESET. Una vez configurados estos perfiles, seleccione **Herramientas** > **Planificador de tareas** y modifique los parámetros de la tarea de actualización. Designe un perfil como principal y el otro, como secundario.

**Perfil de actualización**: el perfil de actualización utilizado actualmente. Para cambiarlo, seleccione un perfil en el menú desplegable.

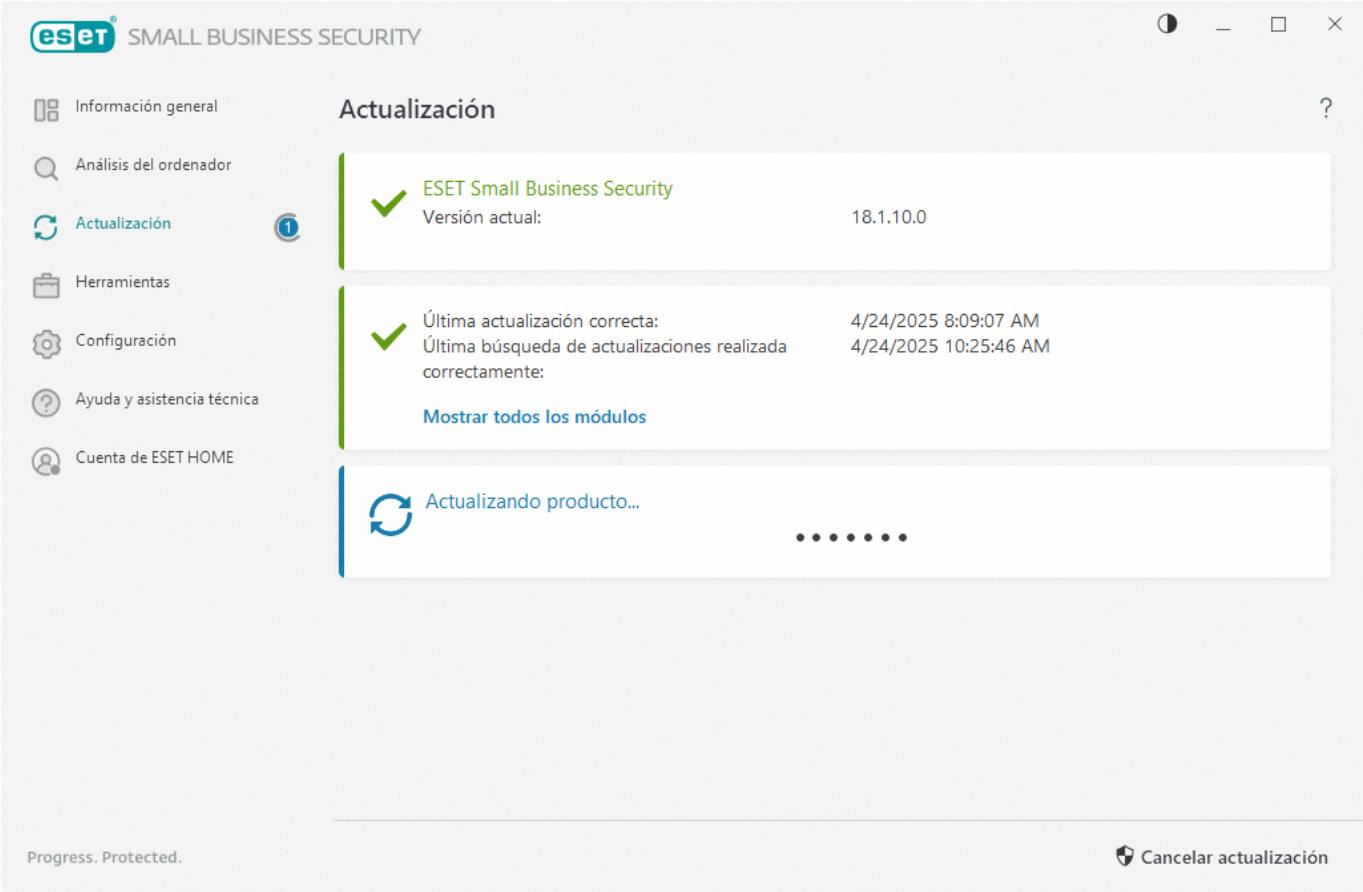
**Lista de perfiles**: cree perfiles de actualización nuevos o quite los actuales.

# Actualizaciones

La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar ESET Small Business Security de forma periódica. El módulo de actualización garantiza que los módulos del programa y los componentes del sistema están siempre actualizados.

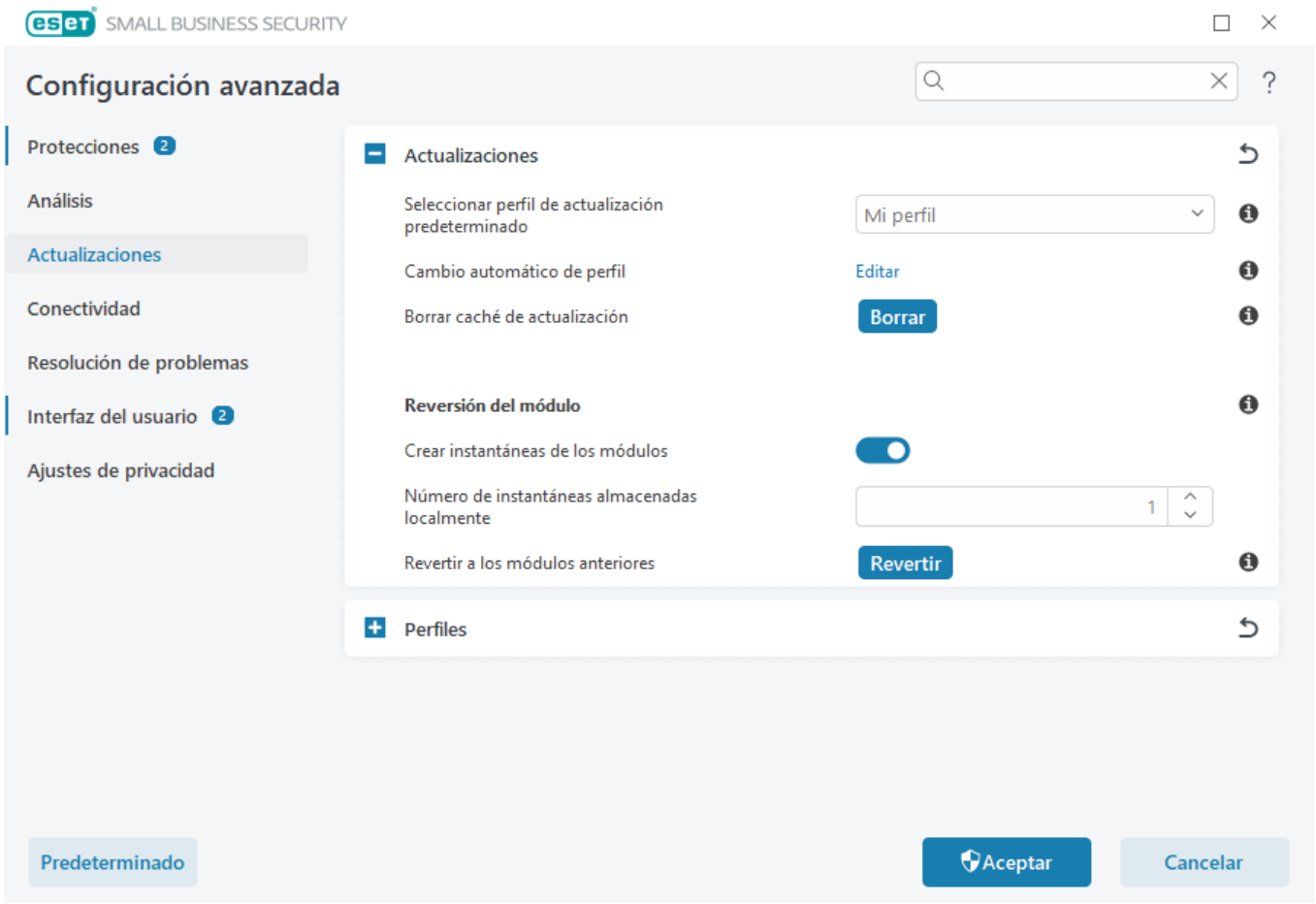
Haga clic en **Actualizar** en la ventana principal del programa para consultar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa.

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual.



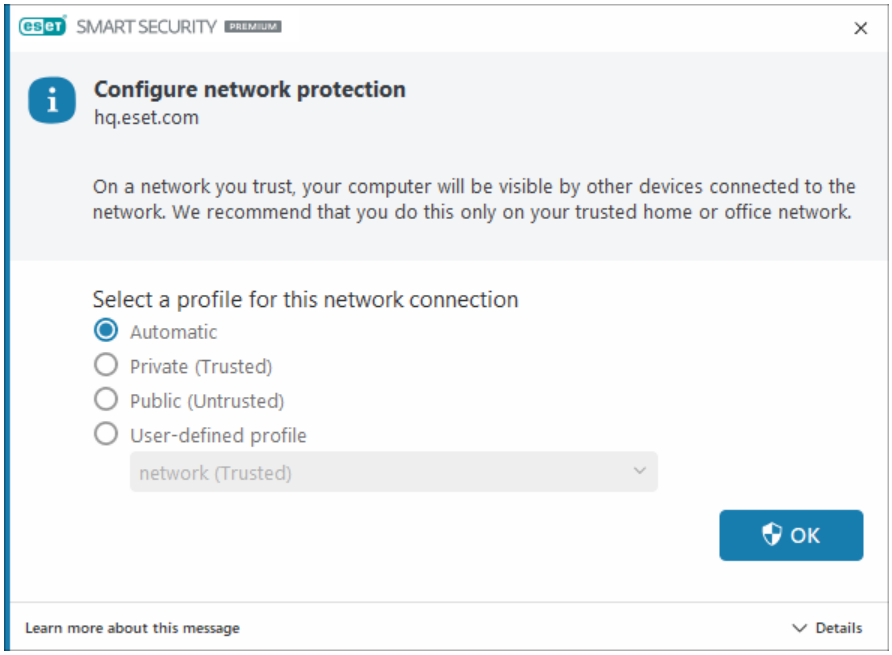

Configuración avanzada > **Actualización** contiene opciones de actualización adicionales, como el modo de actualización, el acceso al servidor proxy y las conexiones LAN.

Si está experimentando problemas con una actualización, haga clic en **Borrar** para borrar la caché de actualización. Si aún así no puede actualizar los módulos del programa, consulte la sección Solución de problemas para el mensaje "Error de actualización de los módulos".




# Configurar protección de la red

De forma predeterminada, ESET Small Business Security utiliza la configuración de Windows cuando se detecta una nueva conexión de red. Para mostrar una ventana de diálogo cuando se detecta una nueva red, cambie la Asignación del perfil de protección de la red a **Preguntar**. La configuración de la protección de la red se muestra siempre que el ordenador se conecta a una red nueva.




Puede elegir entre los siguientes Perfiles de conexión de red:

**Automático**: ESET Small Business Security seleccionará el perfil automáticamente, en función de los Activadores configurados para cada perfil.

**Privado**: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible).

Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Pública**: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado.

Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

**Perfil definido por el usuario**: puede seleccionar un perfil que haya creado en el menú desplegable. Esta opción solo está disponible si ha creado al menos un perfil personalizado.

⚠ Una configuración de red incorrecta puede exponer su ordenador a riesgos para la seguridad.

# Activar Antirrobo

Los dispositivos personales están en constante riesgo de pérdida o robo en los desplazamientos diarios de casa al trabajo u otros lugares públicos. Antirrobo es una es una función que amplía la seguridad a nivel del usuario en caso de robo o pérdida del dispositivo. Antirrobo le permite supervisar el uso del dispositivo y rastrear el dispositivo que le falta por medio de la localización a través de dirección IP en ESET HOME, lo que le ayuda a recuperar su dispositivo y proteger los datos personales.

Mediante el uso de tecnologías modernas como búsqueda geográfica de direcciones IP, captura de imágenes de cámaras web, protección de la cuenta de usuario y supervisión del dispositivo, Antirrobo puede colaborar con usted y las fuerzas del orden para encontrar su ordenador o dispositivo perdido o robado. En ESET HOME, puede ver la actividad que tiene lugar en el ordenador o el dispositivo.

Para obtener más información sobre Antirrobo en ESET HOME, consulte la Ayuda en línea de ESET HOME.

Antirrobo puede no funcionar correctamente en los ordenadores de los dominios debido a restricciones en la administración de cuentas de usuario.

Para activar Antirrobo y proteger su dispositivo en caso de pérdida o robo, elija una de las siguientes opciones:

- En la ventana principal del programa > **Información general**, haga clic en **CONFIGURAR** junto a **Antirrobo**.
- Si aparece el mensaje "Antirrobo está disponible" en la ventana principal del programa > pantalla **Visión general**, haca clic en **Activar Antirrobo**.
- En la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad**. Active el interruptor **Antirrobo** y siga las instrucciones que se indican en pantalla.

Si su dispositivo no está conectado a ESET HOME, debe:
1. Iniciar sesión en su cuenta de ESET HOME al activar Antirrobo.
2. Defina el nombre del dispositivo.

Antirrobo no es compatible con Microsoft Windows Home Server.

Tras Activar Antirrobo, puede optimizar la seguridad del dispositivo desde la ventana principal del programa > **Configuración** > **Herramientas de seguridad** > **Antirrobo**.

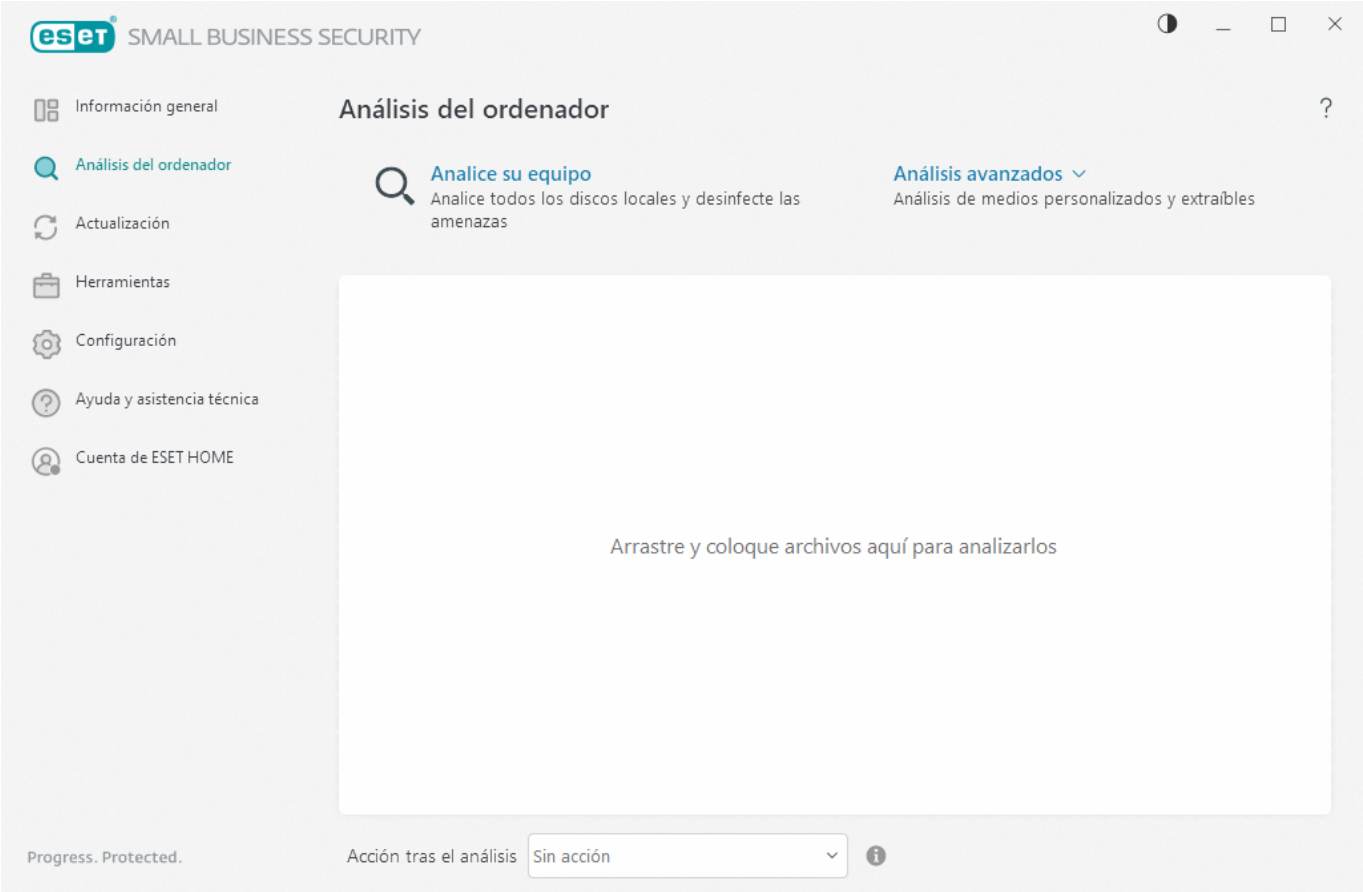
# Trabajo con ESET Small Business Security

La ventana principal del programa de ESET Small Business Security está dividida en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.

### Instrucciones con ilustraciones
Consulte Abrir la ventana principal del programa de los productos de ESET para Windows para obtener instrucciones con ilustraciones disponibles en inglés y en otros idiomas.

Puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET Small Business Security en la esquina superior derecha de la ventana principal del programa. Haga clic en el icono **Esquema de colores** (el icono cambia en función del esquema de colores seleccionado actualmente) junto al icono **Minimizar** y seleccione el esquema de colores en el menú desplegable:

- **Igual que el color del sistema**: define el esquema de colores de ESET Small Business Security según la configuración del sistema operativo.
- **Oscuro**: ESET Small Business Security tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**: ESET Small Business Security tendrá un esquema de colores estándar y claro.




Opciones del menú principal:

Información general: proporciona información sobre el estado de protección de ESET Small Business Security.

Análisis del ordenador: configure e inicie un análisis de su ordenador o cree un análisis personalizado.

Actualización: muestra información sobre las actualizaciones del módulo y el motor de detección.

Herramientas: proporciona acceso a Inspector de red y otras funciones que ayudan a simplificar la administración del programa y ofrecen opciones adicionales para usuarios avanzados.

Configuración: proporciona opciones de configuración para las funciones de protección de ESET Small Business Security (Protección del ordenador, Protección de Internet, Protección de la red y Herramientas de seguridad) y acceso a la Configuración avanzada.

Ayuda y asistencia técnica: muestra información sobre la suscripción, el producto de ESET instalado y vínculos a la ayuda en línea, la base de conocimiento de ESET y el soporte técnico.

Cuenta de ESET HOME: conecte su dispositivo a ESET HOME o revise el estado de conexión de la cuenta de ESET HOME. Utilice ESET HOME para ver y administrar la configuración de Antirrobo y las suscripciónes y dispositivos ESET activados.

# Visión general

En la ventana **Información general** se muestra información sobre la protección actual del ordenador junto con vínculos rápidos a las funciones de seguridad de ESET Small Business Security.

En la ventana **Información general** se muestran notificaciones con información detallada y soluciones

recomendadas para mejorar la seguridad de ESET Small Business Security, activar funciones adicionales o garantizar la máxima protección. Si hay más notificaciones, haga clic en **X más notificaciones** para ampliarlas todas.

**Password Manager**: abre las instrucciones de configuración de Password Manager.

**Inspector de red** – Compruebe la seguridad de su red.

**Secure Data**: Abre las Herramientas de seguridad. Haga clic en el interruptor situado junto a **Secure Data** para activarlo. Si ya tiene Secure Data activado, el vínculo rápido abre la página de Secure Data.

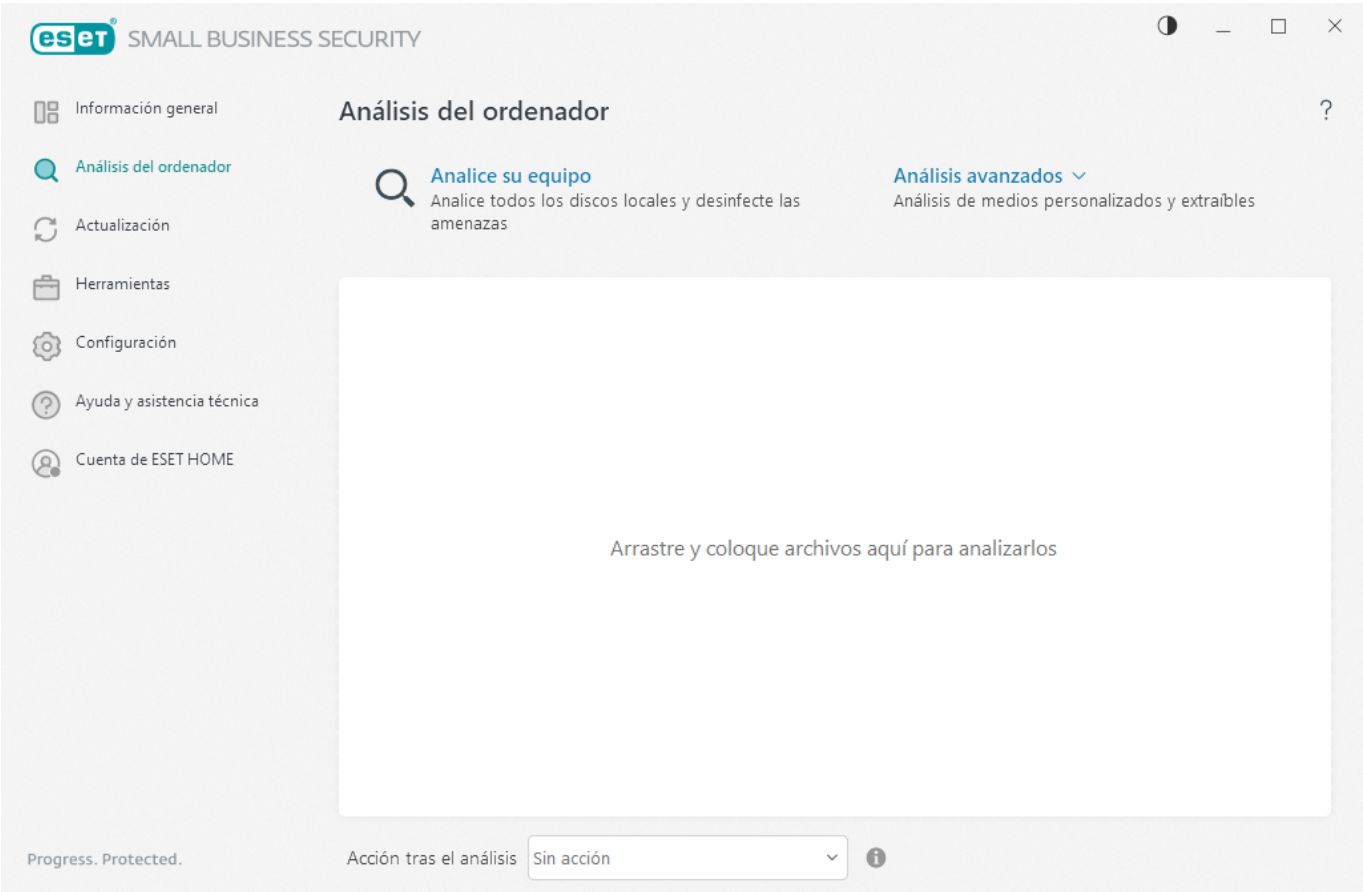
**Banca y navegación seguras**: abre el navegador establecido de forma predeterminada en Windows en modo seguro.

**Privacidad y seguridad del navegador**: puede buscar los resultados del análisis, eliminar sus datos de navegación o configurar limpiezas periódicas.

**ESET Folder Guard**: Inicia la configuración de ESET Folder Guard. Si ya ha configurado ESET Folder Guard, el vínculo rápido abre la página de ESET Folder Guard.

**Antirrobo**: inicia la configuración de Antirrobo. Si ya ha configurado Antirrobo, el vínculo rápido abre la página de Antirrobo.

**VPN** – Mantenga los datos seguros, evite el seguimiento no deseado y mejore la privacidad con la seguridad adicional que ofrece una dirección IP anónima.

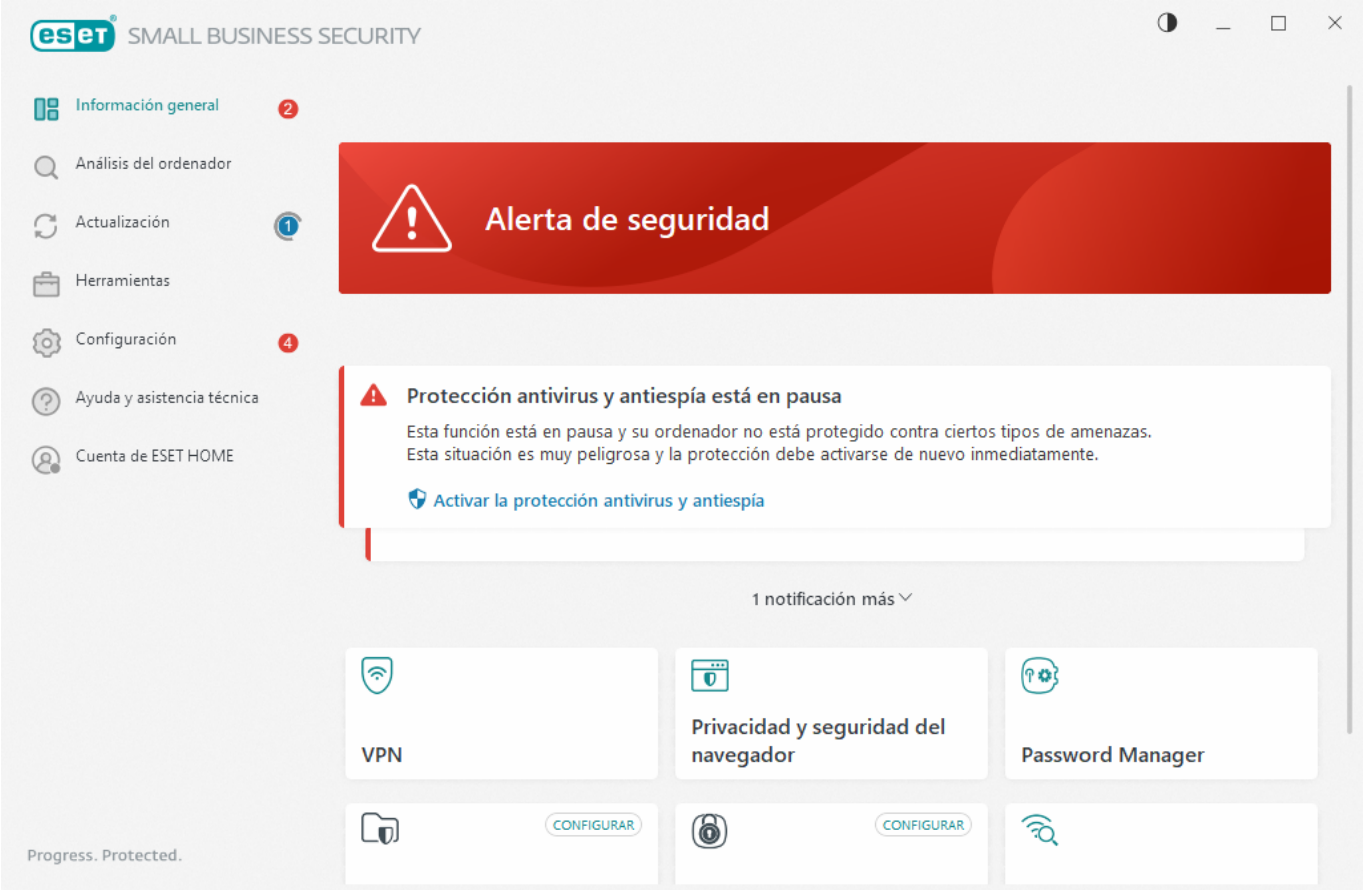



El icono de color verde y el estado **Está protegido** verde indican que se garantiza la máxima protección.

# Qué hacer si el programa no funciona correctamente

Si un módulo de protección activa funciona correctamente, su icono de estado de la protección será verde. Un signo de exclamación rojo o un icono de notificación naranja indican que no se garantiza el nivel de protección máximo.

En la ventana **Información general** se mostrará como notificación la información adicional acerca del estado de protección de cada módulo, así como soluciones sugeridas para restaurar la protección completa. Para cambiar el estado de módulos individuales, haga clic en **Configuración** y seleccione el módulo que desee.




El icono de color rojo y el estado de color rojo **Alerta de seguridad** indican problemas graves. Existen varios motivos para que se muestre este estado, por ejemplo:

- **El producto no está activado** o **La suscripción ha caducado**: esto se indica mediante un icono de estado de protección. Una vez que caduque la suscripción, el programa no se puede actualizar. Siga las instrucciones de la ventana de alerta para renovar la suscripción.
- **El Motor de detección está obsoleto**: este error aparecerá tras varios intentos sin éxito de actualizar el motor de detección. Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.
- **La protección del sistema de archivos en tiempo real está desactivada**: el usuario desactivó la protección en tiempo real. Su ordenador no está protegido frente a amenazas. Haga clic en **Activar la protección del sistema de archivos en tiempo real** para volver a activar esta funcionalidad.
- **La protección antivirus y antiespía está desactivada**: puede volver a activar la protección antivirus y antiespía haciendo clic en **Activar la protección antivirus y antiespía**.

- **Cortafuegos personal de ESET desactivado**: este problema también se indica mediante una notificación de seguridad junto al elemento **Red** del escritorio. Puede volver a activar la protección de red haciendo clic en **Activar cortafuegos**.

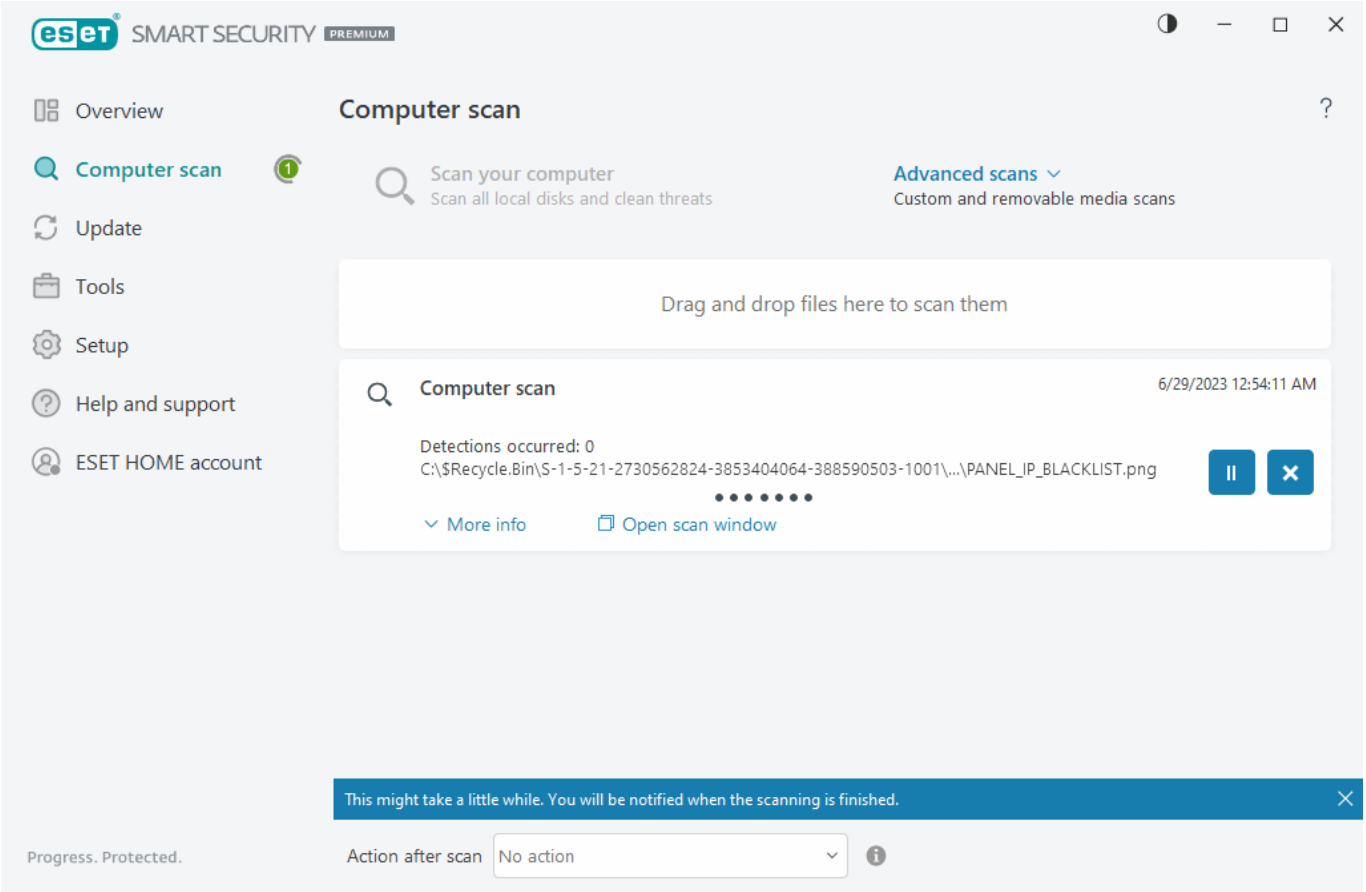
 El icono naranja indica protección limitada. Por ejemplo, podría existir un problema al actualizar el programa o la suscripción puede estar cerca de la fecha de expiración.
Existen varios motivos para que se muestre este estado, por ejemplo:

- **Alerta de optimización Antirrobo**: este dispositivo no está optimizado para Antirrobo. Por ejemplo, es posible que no pueda crearse una cuenta fantasma (una característica de seguridad que se activa automáticamente al marcar un dispositivo como perdido). Puede crear una cuenta fantasma utilizando la característica Optimización en la interfaz web de Antirrobo.
- **Modo de presentación activo**: la activación del Modo de presentación es un posible riesgo para la seguridad. Al activar esta función se desactivan todas las ventanas de notificación o alerta y se detiene cualquier tarea planificada.
- **La suscripción caduca en breve/Su suscripción caduca hoy**: esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación junto al reloj del sistema. Cuando expire la suscripción, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.

Si no consigue solucionar el problema con estas sugerencias, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o realice una búsqueda en la base de conocimiento de ESET. Si todavía necesita ayuda, puede enviar una solicitud de soporte. El servicio de soporte técnico de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

# Análisis del ordenador

El análisis a petición es una parte importante de su solución antivirus. Se utiliza para realizar análisis de archivos y carpetas en su ordenador. Desde el punto de vista de la seguridad, es esencial que los análisis del ordenador se ejecuten periódicamente como parte de las medidas de seguridad rutinarias, y no solo cuando se sospecha que existe una infección. Le recomendamos que realice un análisis en profundidad de su sistema periódicamente para detectar posibles virus que la Protección del sistema de archivos en tiempo real no haya encontrado cuando se registraron en el disco. Este fallo puede deberse a que la protección del sistema de archivos en tiempo real no estaba activada en ese momento, a que el motor de detección está obsoleto o a que el archivo no se detectó como un virus cuando se guardó en el disco.




Están disponibles dos tipos de **Análisis del ordenador**. **Análisis del ordenador** analiza rápidamente el sistema sin especificar parámetros de análisis. El **Análisis personalizado** (bajo Análisis avanzados) le permite seleccionar perfiles de análisis predefinidos para ubicaciones específicas, así como elegir objetos de análisis específicos.

Consulte Progreso del análisis para obtener más información sobre el proceso de análisis.

De forma predeterminada, ESET Small Business Security intenta desinfectar o eliminar automáticamente las detecciones encontradas durante el análisis del ordenador. En algunos casos, si no se puede realizar ninguna acción, recibe una alerta interactiva y debe seleccionar una acción de desinfección (por ejemplo, eliminar o ignorar). Para cambiar el nivel de desinfección y obtener información más detallada, consulte Desinfección. Para revisar análisis anteriores, consulte Archivos de registro.

## Analice su equipo

**Análisis del ordenador** le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin la intervención del usuario. La ventaja de este tipo de **análisis del ordenador** es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis comprueba todos los archivos de las unidades locales y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece automáticamente en el valor predeterminado. Para obtener más información detallada sobre los tipos de desinfección, consulte Desinfección.

También puede utilizar la función **Análisis mediante arrastrar y colocar** para analizar un archivo o una carpeta manualmente al hacer clic en el archivo o la carpeta, desplazar el cursor del ratón hasta la zona marcada mientras se mantiene pulsado el botón del ratón, para después soltarlo. Después, la aplicación pasa al primer plano.

En **Análisis avanzados** están disponibles las siguientes opciones de análisis:

## Análisis personalizado

La opción **Análisis personalizado** le permite especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del **Análisis personalizado** es que puede configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis definidos por el usuario, que pueden resultar útiles si el análisis se realiza varias veces con los mismos parámetros.

## Análisis de medios extraíbles

Al igual que **Análisis del ordenador**, inicia rápidamente el análisis de medios extraíbles (como CD/DVD/USB) que están actualmente conectados al ordenador. Esto puede resultar útil cuando conecta una unidad flash USB a un ordenador y desea analizar su contenido por si contiene código malicioso u otras posibles amenazas.

Este tipo de análisis también se puede iniciar haciendo clic en **Análisis personalizado**, en **Medios extraíbles** en el menú desplegable **Objetos de análisis** y, a continuación, en **Analizar**.

## Repetir el último análisis

Permite iniciar rápidamente el análisis realizado previamente con los mismos ajustes con los que se ejecutó.

En el menú desplegable **Acción tras el análisis** puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Sin acciones**: cuando el análisis concluya no se realizará ninguna acción.
- **Apagar**: el ordenador se apaga cuando finaliza el análisis.
- **Reiniciar si es necesario**: el ordenador se reinicia solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Reiniciar**: cierra todos los programas abiertos y reinicia el ordenador cuando concluye el análisis.
- **Forzar reinicio si es necesario**: el ordenador fuerza el reinicio solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el ordenador cuando concluye el análisis.
- **Suspender**: guarda la sesión y establece el ordenador en un estado de bajo consumo para que pueda retomar su trabajo rápidamente.
- **Hibernar**: recopila todos los programas y archivos que se encuentran en ejecución en la RAM y los guarda en un archivo especial de su disco duro. El ordenador se apaga, pero la próxima vez que lo encienda presentará el estado anterior al apagado.

> Las acciones **Suspender** o **Hibernar** estarán disponibles según la configuración de las opciones de encendido y suspensión del sistema operativo de su ordenador o las prestaciones correspondientes. Debe tener en cuenta que cuando el ordenador está en suspensión sigue en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad si funciona con la alimentación de la batería. Si desea ahorrar carga de la batería, por ejemplo al salir de la oficina, le recomendamos utilizar la opción Hibernar.

La acción seleccionada se iniciará cuando finalicen todos los análisis que se están ejecutando. Cuando se seleccione **Apagar** o **Reiniciar**, se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

> Le recomendamos que ejecute un análisis del ordenador una vez al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas** > **Tareas programadas**. ¿Cómo programar un análisis del ordenador semanal?

# Iniciador del análisis personalizado

Puede utilizar el Análisis personalizado para analizar la memoria operativa, la red o determinadas partes de un disco, en lugar del disco al completo. Para ello, haga clic en **Análisis avanzados** > **Análisis personalizado** y seleccione objetos específicos en la estructura de carpetas (árbol).

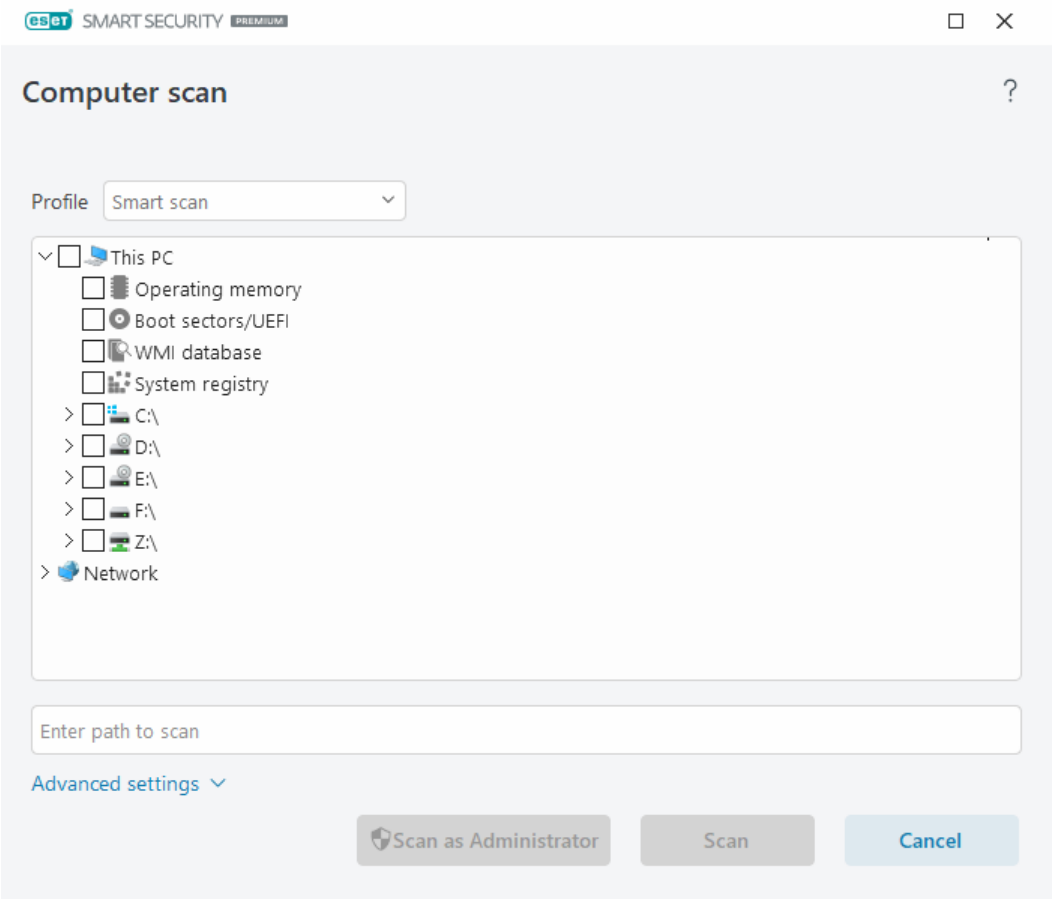
Puede elegir un perfil en el menú desplegable **Perfil** que se utilizará al analizar objetos concretos. El perfil predeterminado es **Análisis inteligente**. Hay otros tres perfiles de análisis predefinidos llamados **Análisis en profundidad**, **Análisis del menú contextual** y **Análisis del ordenador**. Estos perfiles de análisis estándar utilizan distintos parámetros de ThreatSense. Las opciones disponibles se describen en Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Análisis a petición** > ThreatSense.

La estructura (de árbol) de carpetas también contiene objetos de análisis específicos.

- **Memoria operativa**: analiza todos los procesos y datos que actualmente utiliza la memoria operativa.
- **Sectores de inicio/UEFI**: analiza los sectores de inicio y la UEFI en busca de malware. Puede obtener más información sobre el análisis UEFI en el glosario.
- **Base de datos de WMI**: analiza toda la base de datos de Windows Management Instrumentation (WMI), todos los espacios de nombres, todas las instancias de clase y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
- **Registro del sistema**: analiza todo el registro del sistema, todas las claves y todas las subclaves. Busca referencias a archivos infectados o malware incrustados como datos. Durante la desinfección de las detecciones, la referencia permanece en el registro para garantizar que no se pierda ningún dato importante.

Para ir rápidamente a un objeto de análisis (archivo o carpeta), escriba su ruta en el campo de texto que aparece debajo de la estructura de árbol. La ruta distingue entre mayúsculas y minúsculas. Para incluir el objeto en el análisis, marque su casilla de verificación en la estructura de árbol.

> Cómo programar un análisis del ordenador semanal
> Para programar una tarea periódica, lea el capítulo Cómo programar un análisis del ordenador semanal.




Puede configurar los parámetros de desinfección del análisis en Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Análisis a petición** > **ThreatSense** > **Desinfección**. Para ejecutar un análisis sin desinfección, haga clic en **Configuración avanzada** y seleccione **Analizar sin desinfectar**. El historial de análisis se guarda en el registro del análisis.

Cuando se selecciona **Ignorar exclusiones**, se analizan sin excepciones los archivos con extensiones excluidas anteriormente del análisis.

Haga clic en **Analizar** para ejecutar el análisis con los parámetros personalizados que ha definido.

**Analizar como administrador** le permite ejecutar el análisis con la cuenta de administrador. Utilice esta opción si el usuario actual no tiene privilegios para acceder a los archivos que desea analizar. Este botón no está disponible si el usuario actual no puede realizar operaciones de control de cuentas de usuario como administrador.

Si hace clic en Mostrar registro, se mostrará el registro de análisis del ordenador cuando dicho análisis concluya.

# Progreso del análisis

En la ventana de progreso del análisis se muestra el estado actual del análisis e información sobre el número de archivos en los que se ha detectado código malicioso.

Es normal que algunos archivos, como los archivos protegidos con contraseña o que son utilizados exclusivamente por el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar. Puede obtener más información en nuestro artículo de la base de conocimiento.

### Cómo programar un análisis del ordenador semanal

Para programar una tarea periódica, lea el capítulo Cómo programar un análisis del ordenador semanal.

**Progreso del análisis**: la barra de progreso muestra el estado del análisis en ejecución.

**Objeto**: el nombre y la ubicación del objeto que se está analizando.

**Detecciones realizadas**: muestra el número total de objetos analizados, las amenazas encontradas y las desinfectadas durante un análisis.

Haga clic en Más información para mostrar la siguiente información:

- **Usuario**: nombre de la cuenta de usuario que inició el análisis.
- **Objetos analizados**: número de objetos ya analizados.
- **Duración**: tiempo transcurrido.

Icono de pausa: pausa un análisis.

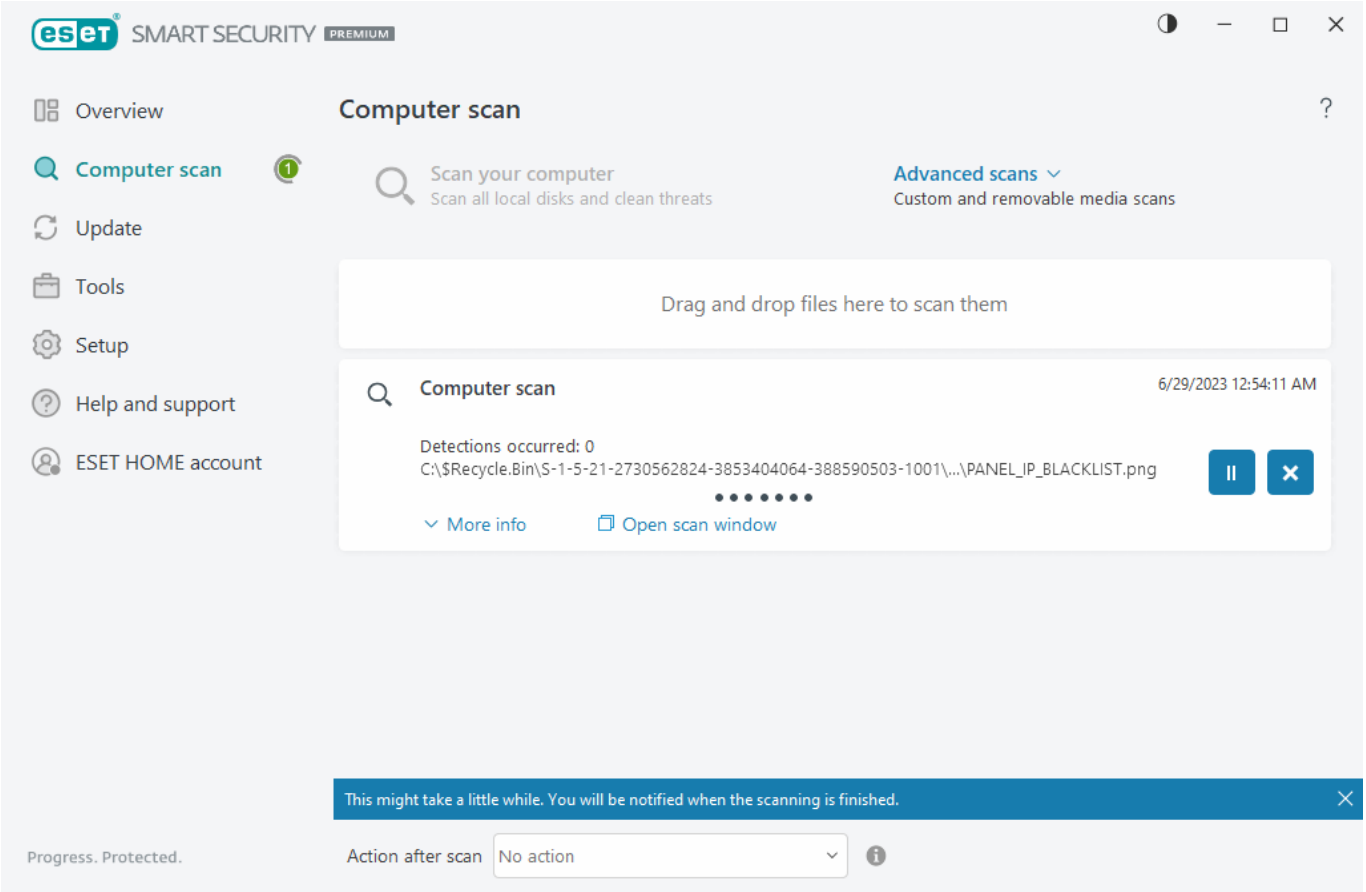
Icono de reanudación: esta opción está visible cuando el progreso del análisis está en pausa. Haga clic en el icono para seguir analizando.

Icono de detención: finaliza el análisis.

Haga clic en **Abrir ventana de análisis** para abrir el Registro de análisis del ordenador, donde puede consultar más detalles sobre el análisis.

**Desplazarse por el registro de exploración**: si esta opción está activada, el registro de análisis se desplaza automáticamente a medida que se añaden entradas nuevas, de modo que se visualizan las entradas más recientes.

Haga clic en la lupa o en la flecha para ver los detalles acerca del análisis que se está ejecutando en ese momento. Puede ejecutar otro análisis paralelo haciendo clic en **Análisis del ordenador** o **Análisis avanzados** > **Análisis personalizado**.




En el menú desplegable **Acción tras el análisis** puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Sin acciones**: cuando el análisis concluya no se realizará ninguna acción.
- **Apagar**: el ordenador se apaga cuando finaliza el análisis.
- **Reiniciar si es necesario**: el ordenador se reinicia solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Reiniciar**: cierra todos los programas abiertos y reinicia el ordenador cuando concluye el análisis.
- **Forzar reinicio si es necesario**: el ordenador fuerza el reinicio solo si es necesario para completar la desinfección de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el ordenador cuando concluye el análisis.
- **Suspender**: guarda la sesión y establece el ordenador en un estado de bajo consumo para que pueda retomar su trabajo rápidamente.
- **Hibernar**: recopila todos los programas y archivos que se encuentran en ejecución en la RAM y los guarda en un archivo especial de su disco duro. El ordenador se apaga, pero la próxima vez que lo encienda presentará el estado anterior al apagado.

Las acciones **Suspender** o **Hibernar** estarán disponibles según la configuración de las opciones de encendido y suspensión del sistema operativo de su ordenador o las prestaciones correspondientes. Debe tener en cuenta que cuando el ordenador está en suspensión sigue en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad si funciona con la alimentación de la batería. Si desea ahorrar carga de la batería, por ejemplo al salir de la oficina, le recomendamos utilizar la opción Hibernar.

La acción seleccionada se iniciará cuando finalicen todos los análisis que se están ejecutando. Cuando se seleccione **Apagar** o **Reiniciar**, se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

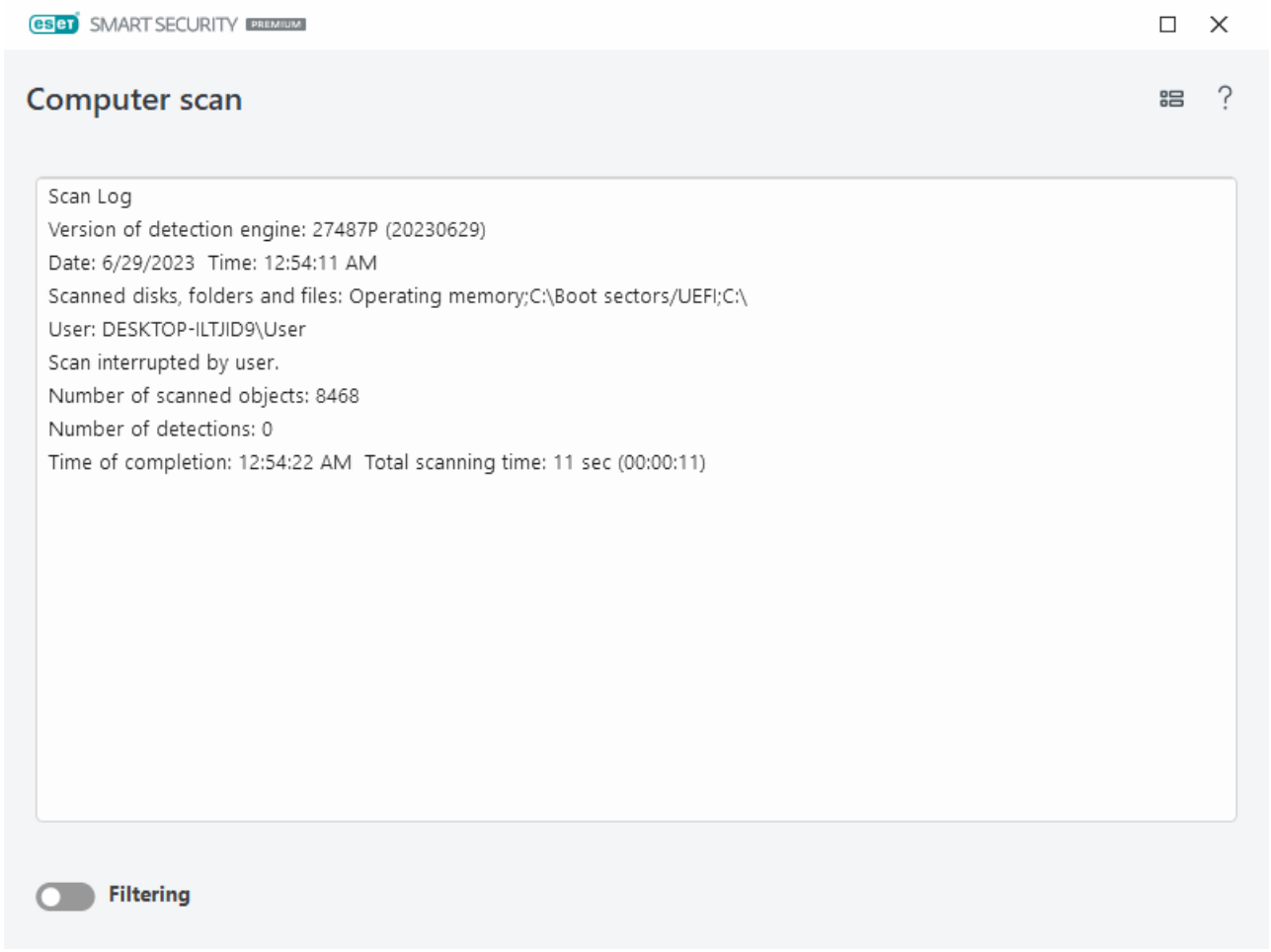
# Registro de análisis del ordenador

Puede ver información detallada relacionada con un análisis específico en Archivos de registro. El registro de análisis contiene la siguiente información:

- Versión del motor de detección
- Fecha y hora de inicio
- Lista de discos, carpetas y archivos analizados
- Nombre del análisis programado (solo análisis programado)
- Usuario que inició el análisis.
- Estado del análisis
- Número de objetos analizados
- Número de detecciones encontradas
- Hora de finalización
- Tiempo total de análisis

Se omite el nuevo inicio de una tarea programada de análisis del ordenador si sigue en ejecución la misma tarea programada que se ejecutó anteriormente. La tarea de análisis programado omitida creará un registro del análisis del ordenador con 0 objetos analizados y el estado **El análisis no se inició porque el análisis anterior aún se estaba ejecutando**.

Para encontrar registros de análisis anteriores en la ventana principal del programa, seleccione **Herramientas** > **Archivos de registro**. En el menú desplegable, seleccione **Análisis del ordenador** y haga doble clic en el registro deseado.




Para obtener más información sobre los registros "no se pudo abrir", "error al abrir" o "archivo comprimido dañado", consulte el artículo de la base de conocimiento de ESET.

Haga clic en el icono del interruptor **Filtrado** para abrir la ventana Filtrado de registros, donde puede acotar la búsqueda por criterios personalizados. Para ver el menú contextual, haga clic con el botón derecho del ratón en una entrada de registro específica:

| Acción | Uso |
|---|---|
| Filtrar los mismos registros | Activa el filtrado de registros. El registro solo mostrará los registros del mismo tipo que el seleccionado. |
| Filtro | Esta opción abre la ventana Filtrado de registros y le permite definir criterios para entradas de registro específicas. Acceso directo: `Ctrl+Shift+F` |
| Activar filtro | Activa los ajustes de filtro. Si activa el filtro por primera vez, debe definir ajustes y se abre la ventana Filtrado de registros. |
| Desactivar filtro | Desactiva el filtro (misma acción que hacer clic en el conmutador de la parte inferior). |
| Copiar | Copia los registros seleccionados en el portapapeles. Acceso directo: `Ctrl+C` |
| Copiar todo | Copia todos los registros en la ventana. |
| Exportar | Exporta los registros seleccionados al portapapeles en un archivo XML. |
| Exportar todo | Esta opción exporta todos los registros en la ventana a un archivo XML. |
| Descripción de la detección | Abre la Enciclopedia de amenazas de ESET, que contiene información detallada sobre los peligros y los síntomas de la infiltración resaltada. |

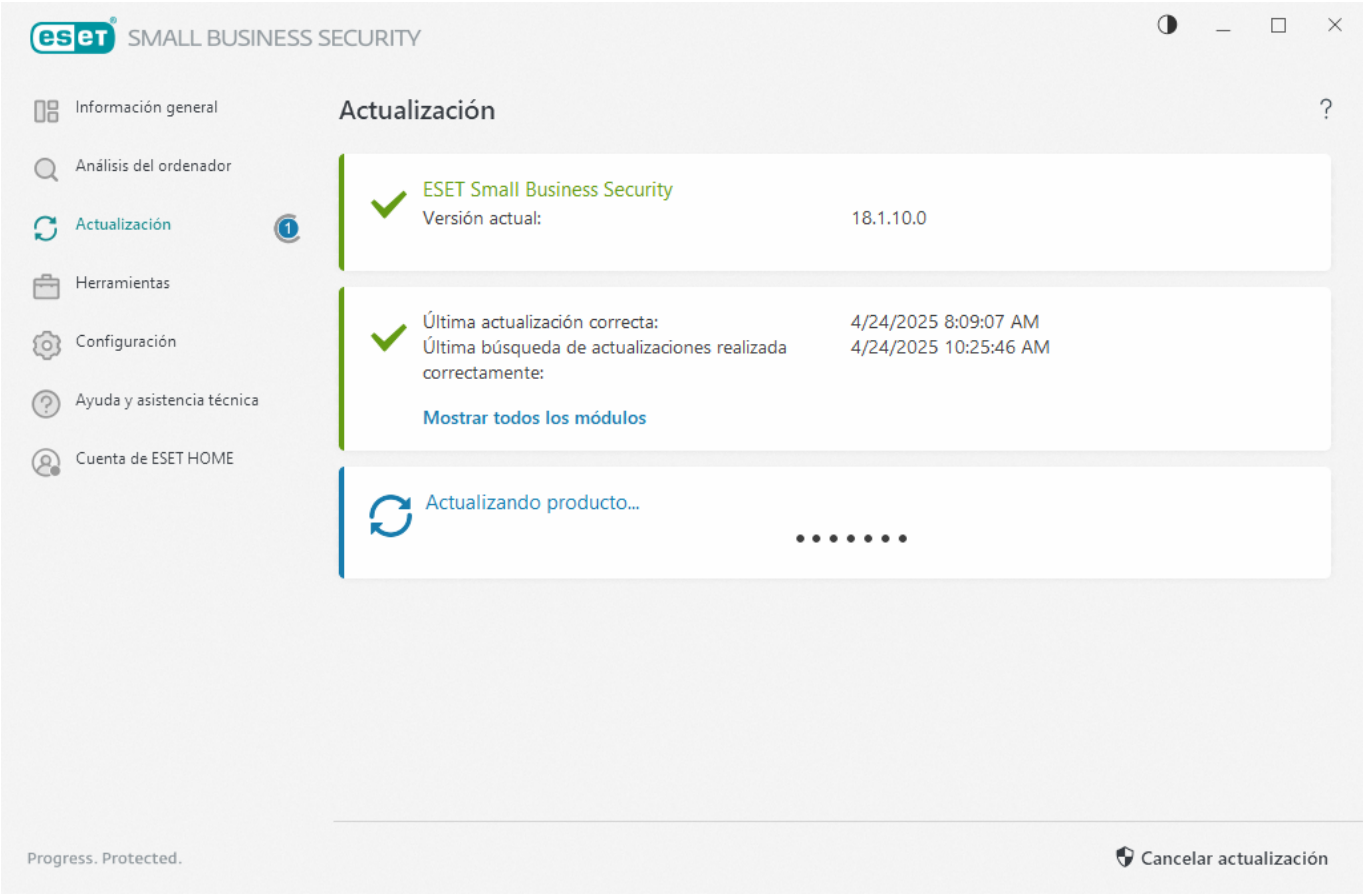
# Actualización

La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar ESET Small Business Security de forma periódica. El módulo de actualización garantiza que los módulos del programa y los componentes del sistema están siempre actualizados.

Haga clic en **Actualizar** en la ventana principal del programa para consultar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa.

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una

actualización manual. La actualización periódica de los módulos y los componentes del programa es un aspecto importante para mantener una protección completa contra el código malicioso. Preste atención a la configuración y el funcionamiento de los módulos del producto. Debe activar su producto con su clave de activación para recibir actualizaciones. Si no lo hizo durante la instalación, deberá activar ESET Small Business Security para acceder a los servidores de actualización de ESET. ESET le envía la clave de activación en un mensaje de correo electrónico tras la compra de ESET Small Business Security.




**Versión actual**: muestra el número de la versión actual que tiene instalada del producto.

**Última actualización correcta**: muestra la fecha de la última actualización correcta. Si no ve una fecha reciente, es posible que los módulos del producto no estén actualizados.

**Última búsqueda de actualizaciones correcta**: muestra la fecha de la última búsqueda de actualizaciones correcta.

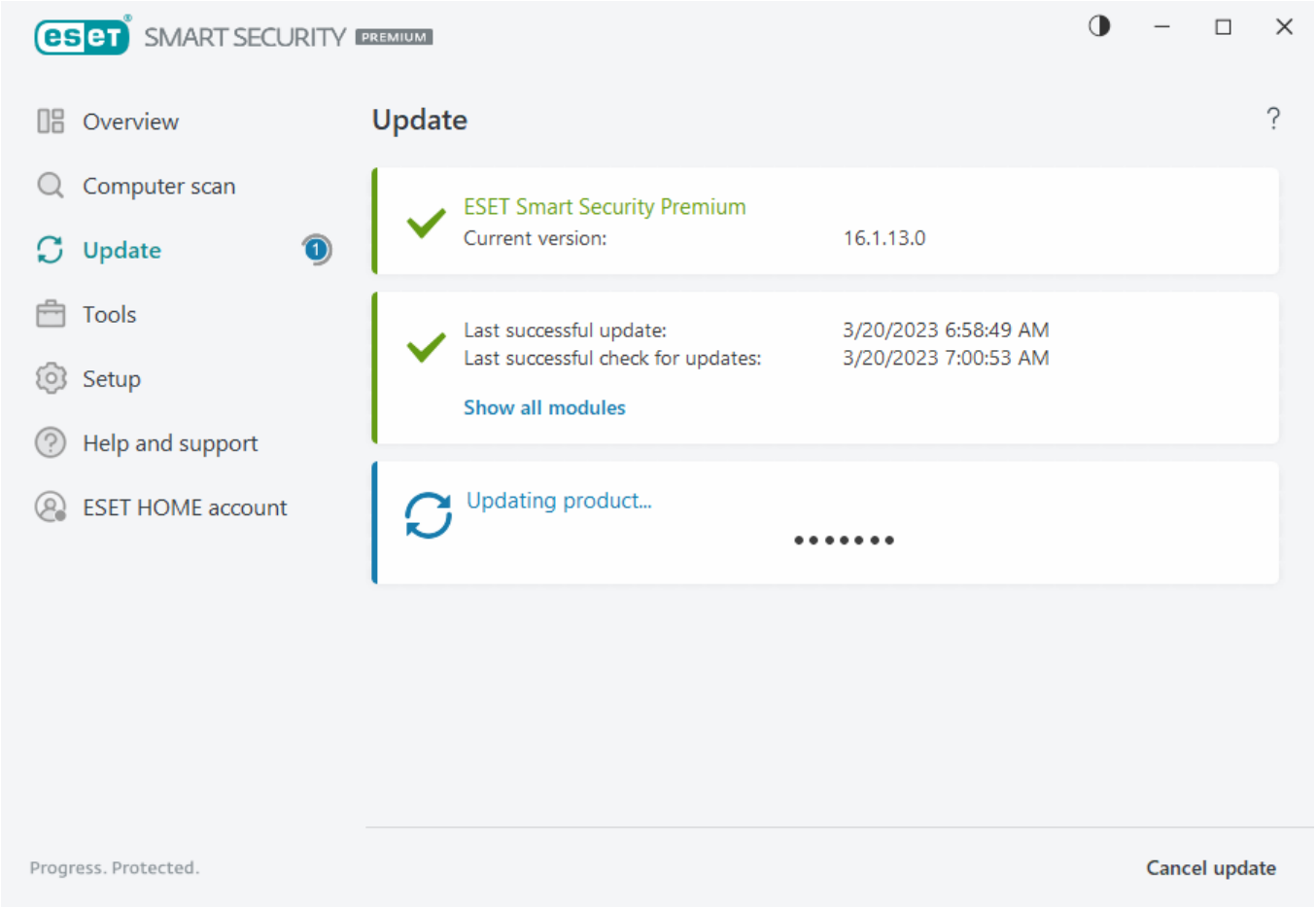
**Mostrar todos los módulos**: muestra la lista de los módulos del programa instalados.

Haga clic en **Buscar actualizaciones** para consultar cuál es la versión disponible más reciente de ESET Small Business Security.

---

## Proceso de actualización

La descarga se inicia al hacer clic en **Buscar actualizaciones**. Se muestran una barra de progreso de la descarga y el tiempo que falta para que finalice la descarga. Para interrumpir la actualización, haga clic en **Cancelar actualización**.




En circunstancias normales, verá la marca de verificación verde en la ventana **Actualización**, que indica que el programa está actualizado. Si no ve la marca de verificación verde, el programa no está actualizado y es más vulnerable a la infección. Actualice los módulos del programa lo antes posible.

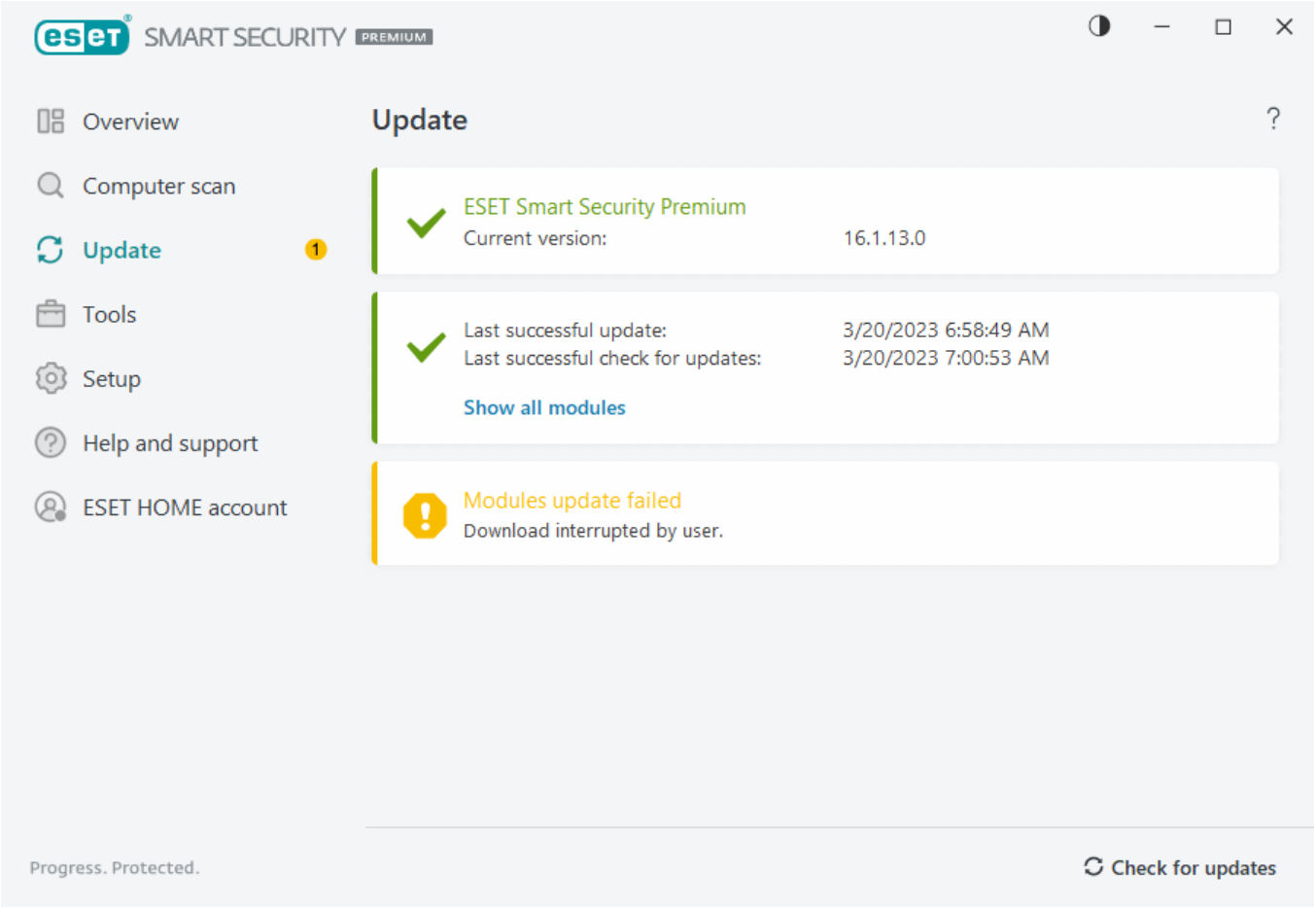
---

## Actualización incorrecta

Si recibe un mensaje de error de la actualización de módulos, puede deberse a los siguientes problemas:

1. **Suscripción no válida**: la suscripción utilizada para la activación no es válida o ha caducado. En la ventana principal del programa, haga clic en **Ayuda y asistencia técnica** > **Cambiar suscripción** y active el producto.

2. **Se ha producido un error al descargar los archivos de actualización**: puede deberse a una configuración de la conexión a Internet incorrecta. Es recomendable que compruebe la conectividad a Internet (por ejemplo, abriendo un sitio web en el navegador web). Si el sitio web no se abre, es probable que no se haya establecido ninguna conexión a Internet o que haya problemas de conectividad con el ordenador. Consulte a su proveedor de servicios de Internet (ISP) si no tiene una conexión activa a Internet.




Debe reiniciar el ordenador tras una actualización correcta de ESET Small Business Security a una versión más reciente del producto para asegurarse de que todos los módulos del programa se hayan actualizado correctamente. No es necesario reiniciar el ordenador después de llevar a cabo actualizaciones normales de módulos.

Visite Solución de problemas para el mensaje "Error de actualización de los módulos" para obtener más información.

# Cuadro de diálogo: es necesario reiniciar

Después de actualizar ESET Small Business Security a una nueva versión es necesario reiniciar el ordenador. Las versiones nuevas de ESET Small Business Security implementan mejoras o solucionan problemas que no se pueden resolver con las actualizaciones automáticas de los módulos de programa.

La nueva versión de ESET Small Business Security puede instalarse automáticamente, en función de la configuración de actualización del programa, o manualmente mediante la descarga e instalación de una versión más reciente sobre la anterior.

Haga clic en **Reiniciar ahora** para reiniciar el ordenador. Si tiene pensado reiniciar el ordenador más tarde, haga clic en **Recordármelo más tarde**. Posteriormente, puede reiniciar el ordenador manualmente desde la sección **Información general** de la ventana principal del programa.

# Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente al hacer clic en **Buscar actualizaciones** de la ventana principal que se muestra al hacer clic en **Actualización** en el menú principal.

Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Tareas programadas**. Las siguientes tareas de actualización están activadas de forma predeterminada en ESET Small Business Security:

- **Actualización automática de rutina**
- **Actualización automática después del registro del usuario**

Todas las tareas de actualización se pueden modificar en función de sus necesidades. Además de las tareas de actualización predeterminadas, se pueden crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más información acerca de la creación y la configuración de tareas de actualización, consulte la sección Planificador de tareas.

# Herramientas

El menú **Herramientas** incluye funciones que ofrecen seguridad adicional y ayudan a simplificar la administración de ESET Small Business Security. Están disponibles las herramientas siguientes:

 Archivos de registro

 Procesos en ejecución (si ESET LiveGrid® se ha activado en ESET Small Business Security)

 Informe de seguridad

 Conexiones de red (si el Cortafuegos está activado en ESET Small Business Security)

 ESET SysInspector

 Planificador de tareas

 Limpieza del sistema

 Inspector de red

 Enviar muestra para su análisis (puede que no esté disponible en función de la configuración de ESET LiveGrid®).

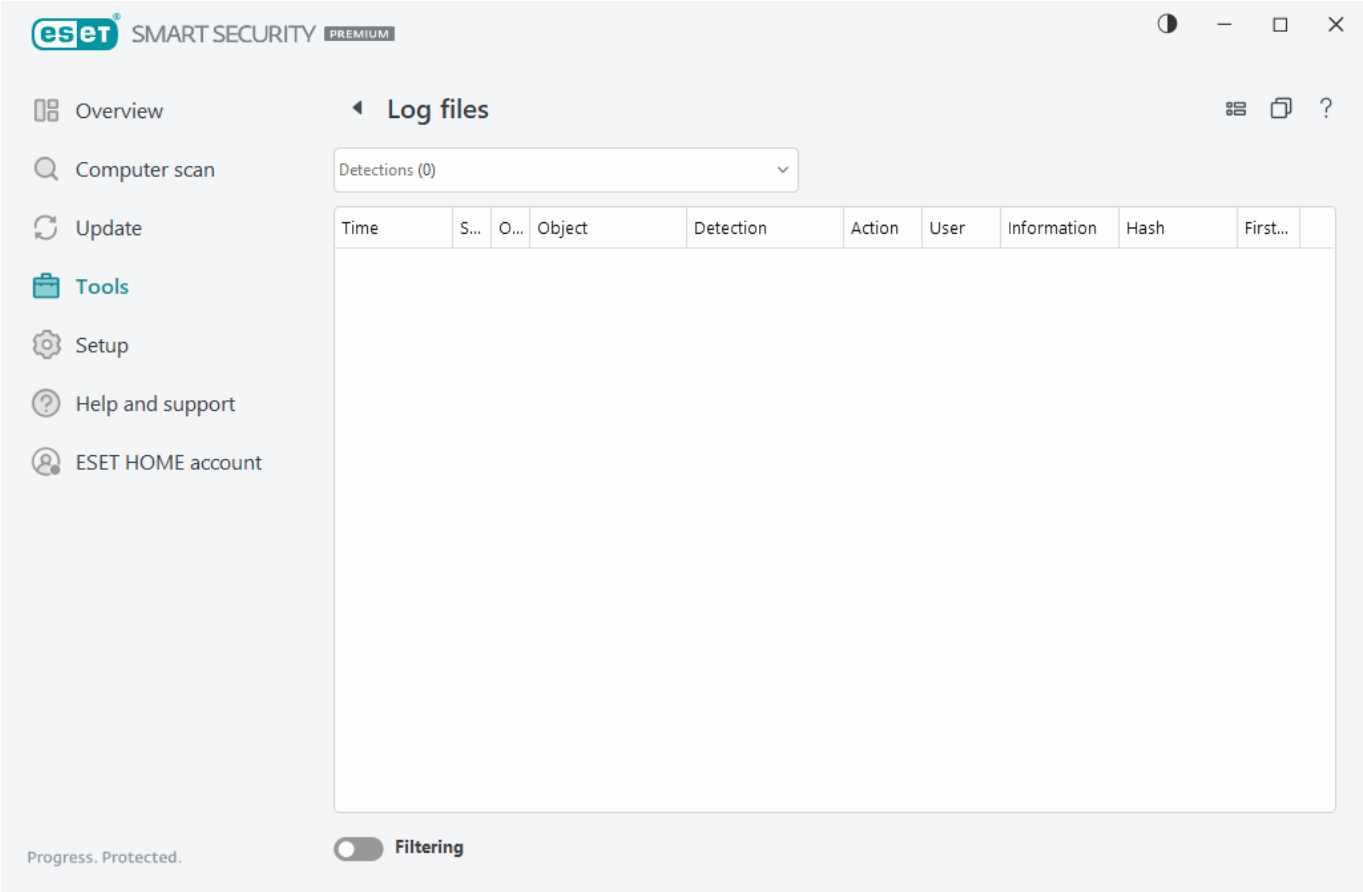
 Cuarentena


# Archivos de registro

Los archivos de registro contienen información relacionada con los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. El registro constituye una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas.

Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según el nivel de detalle de los registros.

Los mensajes de texto y los registros se pueden ver directamente desde el entorno de ESET Small Business Security, donde también se pueden archivar registros.




Se puede acceder a los archivos de registro desde ventana principal del programa de haciendo clic en **Herramientas** > **Archivos de registro**. Seleccione el tipo de registro que desee en el menú desplegable Registrar.

- **Amenazas detectadas**: este registro ofrece información detallada acerca de las amenazas y las infiltraciones detectadas por ESET Small Business Security. La información del registro incluye la hora de la detección, el tipo de escáner, el tipo de objeto, la ubicación del objeto, el nombre de la detección, la acción realizada, el nombre del usuario con sesión iniciada en el momento en el que se detectó la infiltración, el hash y la primera ocurrencia. Haga doble clic en cualquier entrada del registro para ver sus detalles en una ventana independiente. Las infiltraciones no desinfectadas siempre se marcan con texto rojo sobre fondo rojo claro. Las PUA o las aplicaciones potencialmente peligrosas no eliminadas se marcan con texto amarillo sobre fondo blanco.

- **Sucesos**: todas las acciones importantes realizadas por ESET Small Business Security se registran en el registro de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para que los administradores del sistema y los usuarios puedan solucionar problemas. Con frecuencia, la información aquí disponible puede ayudarle a encontrar una solución para un problema del programa.

- **Análisis del ordenador**: en esta ventana se muestran los resultados de todos los análisis completados. Cada línea se corresponde con una análisis del ordenador individual. Haga doble clic en cualquier entrada para ver los detalles del análisis seleccionado.

- **Archivos enviados**: contiene registros de las muestras enviadas a ESET LiveGuard.

- **HIPS**: contiene registros de reglas específicas de HIPS que se marcaron para su registro. El protocolo muestra la aplicación que activó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla.

• **Protección del navegador**: contiene registros de archivos no verificados o que no son de confianza cargados en el navegador.

• **Protección de la red**: el registro de protección de la red muestra todos los ataques remotos detectados por el cortafuegos, la protección contra ataques de red (IDS) y la protección contra botnets. Aquí encontrará información sobre todos los ataques a su ordenador. En la columna Suceso se incluyen los ataques detectados. En la columna Origen se proporciona más información sobre el atacante. En la columna Protocolo se indica el protocolo de comunicación que se utilizó para el ataque. El análisis del registro de protección de la red puede ayudarle a detectar a tiempo amenazas del sistema, para así poder evitar el acceso no autorizado al sistema. Para obtener más información sobre los ataques de red, consulte la sección Sistema de detección de intrusos y opciones avanzadas.

• **Sitios web filtrados**:Esta lista es útil si desea ver una lista de sitios web bloqueados por la Protección de acceso a la web. Cada registro incluye la hora, la dirección URL, el usuario y la aplicación que creó una conexión con un sitio web en cuestión.

• **Actualizaciones**: contiene registros de todos los registros del actualizador y de todas las actualizaciones de los módulos.

• **Antispam del cliente de correo electrónico**: contiene los registros relacionados con los mensajes de correo electrónico que se marcaron como correo no deseado.

• **Control de dispositivos**: contiene registros de los dispositivos o los soportes extraíbles conectados al ordenador. Solo los dispositivos con reglas de control de dispositivos correspondientes se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, no se creará una entrada de registro para un dispositivo conectado. Puede ver también detalles como el tipo de dispositivo, número de serie, nombre del fabricante y tamaño del medio (si está disponible).

• **Protección de cámara web**: contiene registros sobre las aplicaciones bloqueadas mediante la protección de la cámara web.

Seleccione el contenido de cualquier registro y pulse **CTRL + C** para copiarlo en el portapapeles. Mantenga pulsadas las teclas **CTRL** o **SHIFT** para seleccionar varias entradas.

Haga clic en **Filtrado** para abrir la ventana Filtrado de registros, donde puede definir los criterios de filtrado.

Haga clic con el botón derecho en un registro concreto para abrir el menú contextual. En este menú contextual, están disponibles las opciones siguientes:

• **Mostrar**: muestra información detallada sobre el registro seleccionado en una ventana nueva.

• **Filtrar los mismos registros**: tras activar este filtro, solo verá registros del mismo tipo (diagnósticos, advertencias, etc.).

• **Filtro**: después de hacer clic en esta opción, la ventana Filtrado de registros le permitirá definir los criterios de filtrado para entradas de registro específicas.

• **Activar filtro**: activa la configuración del filtro.

• **Desactivar filtro**: borra todos los ajustes del filtro (tal como se describe arriba).

• **Copiar/Copiar todo**: copia información sobre los registros seleccionados en la ventana.

- **Copiar celda**: copia el contenido de la celda en la que se hace clic con el botón derecho.

- **Eliminar/Eliminar todos**: elimina los registros seleccionados o todos los registros mostrados. Se necesitan privilegios de administrador para poder realizar esta acción.

- **Exportar/Exportar todo**: exporta información acerca de los registros seleccionados o de todos los registros en formato XML.

- **Buscar/Buscar siguiente/Buscar anterior**: después de hacer clic en esta opción, puede definir los criterios de filtrado para resaltar la entrada específica desde la ventana Filtrado de registros.

- **Descripción de la detección**: abre la Enciclopedia de amenazas de ESET, que contiene información detallada sobre los peligros y los síntomas de la infiltración registrada.

- **Crear exclusión**: cree una nueva Exclusión de detección con un asistente (no disponible para detecciones de malware).

# Filtrado de registros

Haga clic en **Filtrado** en **Herramientas** > **Archivos de registro** para definir los criterios de filtrado.

La característica de filtrado de registros le ayudará a encontrar la información que busca, especialmente cuando haya muchos registros. Le permite limitar las entradas de registro, por ejemplo, si busca un tipo específico de suceso, estado o periodo de tiempo.

Para filtrar las entradas de registro, especifique determinadas opciones de búsqueda, y solo los registros relevantes (según esas opciones de búsqueda) se mostrarán en la ventana Archivos de registro.

Escriba en el campo **Buscar texto** la palabra clave que busca. Utilice el menú desplegable **Buscar en columnas** para restringir su búsqueda. Elija uno o más registros en el menú desplegable **Tipos de registro**. Defina el **Periodo de tiempo** al que desee que pertenezcan los resultados que se muestren. También puede utilizar otras opciones de búsqueda, como **Solo palabras completas** o **Distinguir mayúsculas y minúsculas**.

## Buscar texto

Escriba una cadena (palabra o parte de una palabra). Solo se mostrarán los registros que contengan esta cadena. Los demás registros se omitirán.

## Buscar en columnas

Seleccione las columnas que se tendrán en cuenta al buscar. Puede marcar una o más columnas que se utilizarán en la búsqueda.

## Tipos de registro

Elija uno o más tipos de registro en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.

- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas

con éxito y todos los registros anteriores.

- **Advertencias**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus

## Periodo de tiempo

Define el período de tiempo para el que desea visualizar los resultados.

- **No especificado** (predeterminado): no busca en el periodo de tiempo, sino en todo el registro.
- **Último día**
- **Última semana**
- **Último mes**
- **Periodo de tiempo**: puede especificar el periodo de tiempo exacto (Desde: y Hasta:) para filtrar solo los registros del periodo de tiempo especificado.

## Solo palabras completas

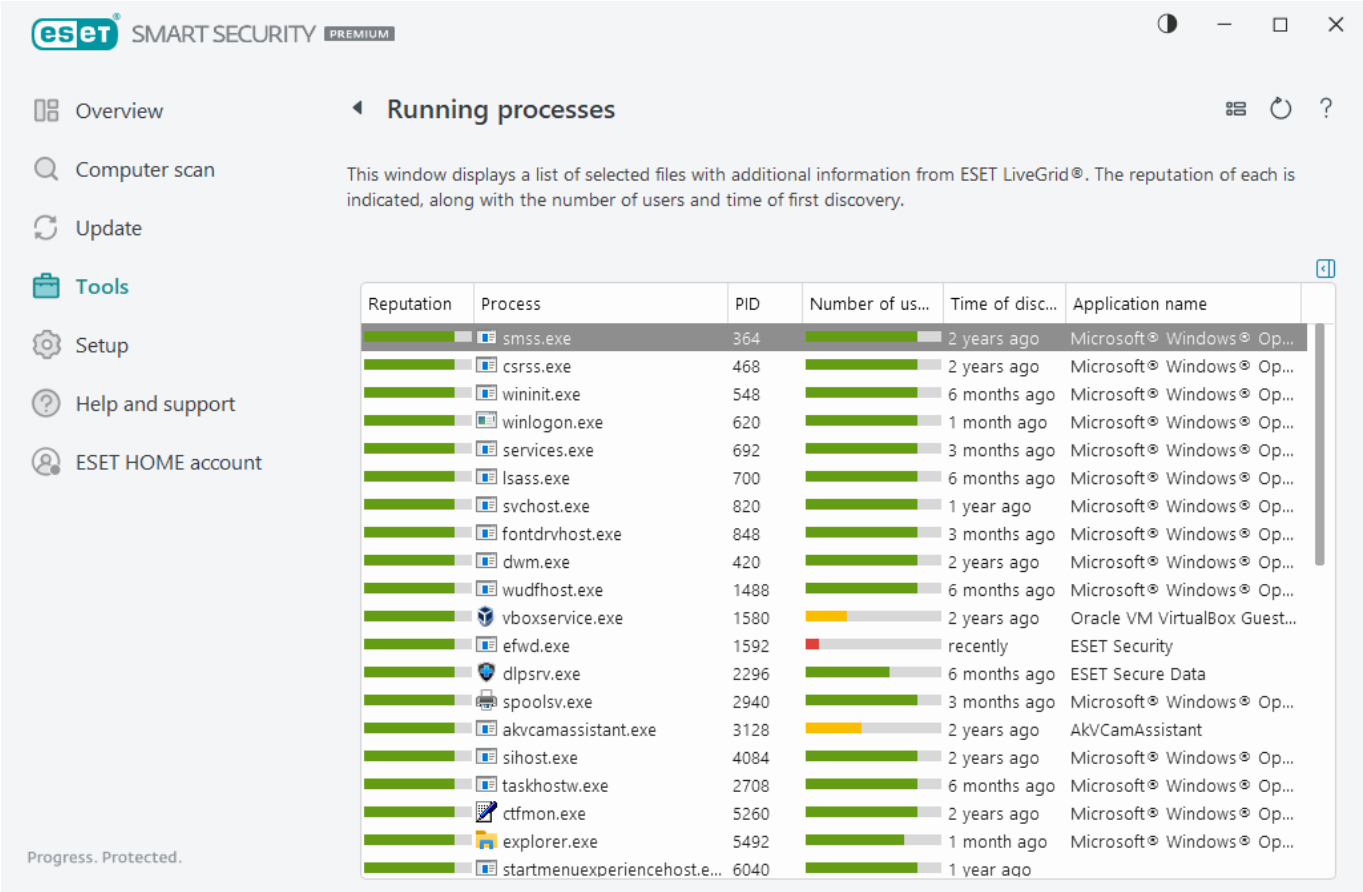
Utilice la casilla de verificación si desea buscar palabras completas para obtener resultados más precisos.

## Distinguir mayúsculas y minúsculas

Active esta opción si es importante utilizar letras mayúsculas o minúsculas al filtrar. Cuando haya configurado sus opciones de filtrado/búsqueda, haga clic en **Aceptar** para mostrar los registros filtrados o en **Buscar** para empezar a buscar. Los archivos de registro se buscan de arriba abajo, desde su posición (el registro resaltado). La búsqueda se detiene cuando se encuentra el primer registro que coincide con los criterios de dicha búsqueda. Pulse **F3** para buscar el siguiente registro o haga clic con el botón derecho y seleccione **Buscar** para restringir sus opciones de búsqueda.

# Procesos en ejecución

Procesos en ejecución indica los programas o procesos que se están ejecutando en el ordenador e informa a ESET de forma inmediata y continua de las nuevas amenazas. ESET Small Business Security proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET LiveGrid®.




**Reputación**: en la mayoría de los casos, ESET Small Business Security y la tecnología ESET LiveGrid® asignan niveles de riesgo a los objetos (archivos, procesos, claves de registro, etc.) con una serie de reglas heurísticas que examinan las características de cada objeto y, a continuación, evalúan su potencial para la actividad maliciosa. Según esta heurística, a los objetos se les asigna un nivel de riesgo de 1: seguro (verde) a 9: peligroso (rojo).

**Proceso**: nombre de la imagen del programa o proceso que se está ejecutando en el ordenador. También puede utilizar el Administrador de tareas de Windows para ver todos los procesos que están en ejecución en el ordenador. Para abrir el Administrador de tareas, haga clic con el botón derecho del ratón en una área vacía de la barra de tareas y, a continuación, haga clic en **Administrador de tareas**, o pulse la combinación **Ctrl**+**Mayús**+**Esc** en el teclado.

Las aplicaciones conocidas marcadas como Correcto (verde) en verde son totalmente seguras (incluidas en lista blanca) y no se analizarán para mejorar el rendimiento.

**PID**: el número identificador del proceso se puede utilizar como parámetro en diversas llamadas de función, como por ejemplo para ajustar la prioridad del proceso.

**Número de usuarios**: el número de usuarios que utilizan una aplicación determinada. La tecnología ESET LiveGrid® se encarga de recopilar esta información.

**Hora de la detección**: tiempo transcurrido desde que la tecnología ESET LiveGrid® detectó la aplicación.

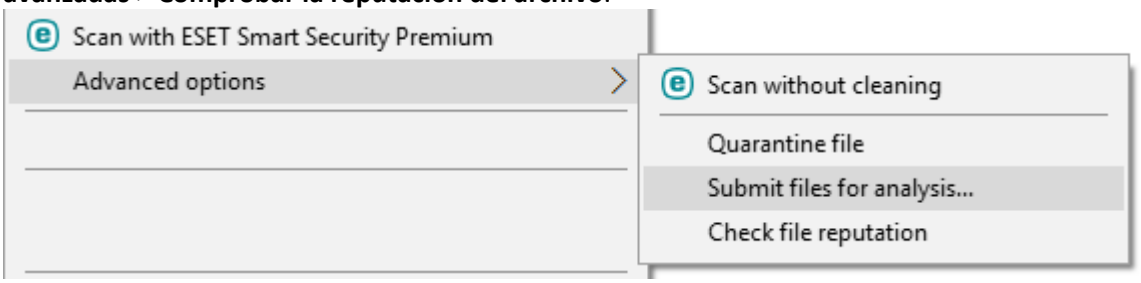
Una aplicación marcada como Desconocido (naranja) no tiene por qué ser software malicioso. Normalmente, se trata de una aplicación reciente. Si el archivo le plantea dudas, puede enviarlo para su análisis al laboratorio de investigación de ESET. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una actualización futura.

**Nombre de aplicación**: nombre de un programa o un proceso.

Haga clic en una aplicación para mostrar los siguientes detalles de dicha aplicación:

- **Ruta**: ubicación de una aplicación en el ordenador.
- **Tamaño**: tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Descripción**: características del archivo de acuerdo con la descripción del sistema operativo.
- **Empresa**: nombre del proveedor o el proceso de la aplicación.
- **Versión**: información sobre el editor de la aplicación.
- **Producto**: nombre de la aplicación o nombre comercial.
- **Fecha de creación/Fecha de modificación**: fecha y hora de creación (o modificación) de la aplicación.

También puede comprobar la reputación de los archivos que no actúan como programas o procesos en ejecución. Para hacerlo, haga clic con el botón derecho en un explorador de archivos y seleccione **Opciones avanzadas** > **Comprobar la reputación del archivo**.




# Informe de seguridad

Esta función ofrece una descripción general de las estadísticas para las siguientes categorías.

- **Páginas web bloqueadas**: muestra el número de páginas web bloqueadas (URL de PUA, phishing y router, IP o certificado hackeados en una lista negra).
- **Objetos de correo electrónico infectados detectados**: muestra el número de objetos de correo electrónico infectados detectados.
- **Aplicación potencialmente indeseable detectada**: muestra el número de aplicaciones potencialmente indeseables (PUA).
- **Correos electrónicos no deseados detectados**: muestra el número de mensajes de correo electrónico no deseados detectados.
- **Acceso a la webcam bloqueado**: muestra el número de accesos a la webcam que se han bloqueado.
- **Documentos analizados**: muestra el número de objetos de documento analizados.
- **Aplicaciones analizadas**: muestra el número de objetos ejecutables analizados.
- **Otros objetos analizados**: muestra el número de otros objetos analizados.
- **Objetos de página web analizados**: muestra el número de objetos de página web analizados.

- **Objetos de correo electrónico analizados**: muestra el número de objetos de correo electrónico analizados.

- **Archivos analizados por ESET LiveGuard**: muestra el número de muestras analizadas por ESET LiveGuard.

El orden de estas categorías se basa en el valor numérico, de más alto a más bajo. Las categorías que tienen un valor cero no se muestran. Haga clic en **Mostrar más** para desplegar y mostrar las categorías ocultas.

La última sección del informe de seguridad ofrece la posibilidad de activar las siguientes características:

- ESET LiveGuard
- Secure Data
- Antirrobo

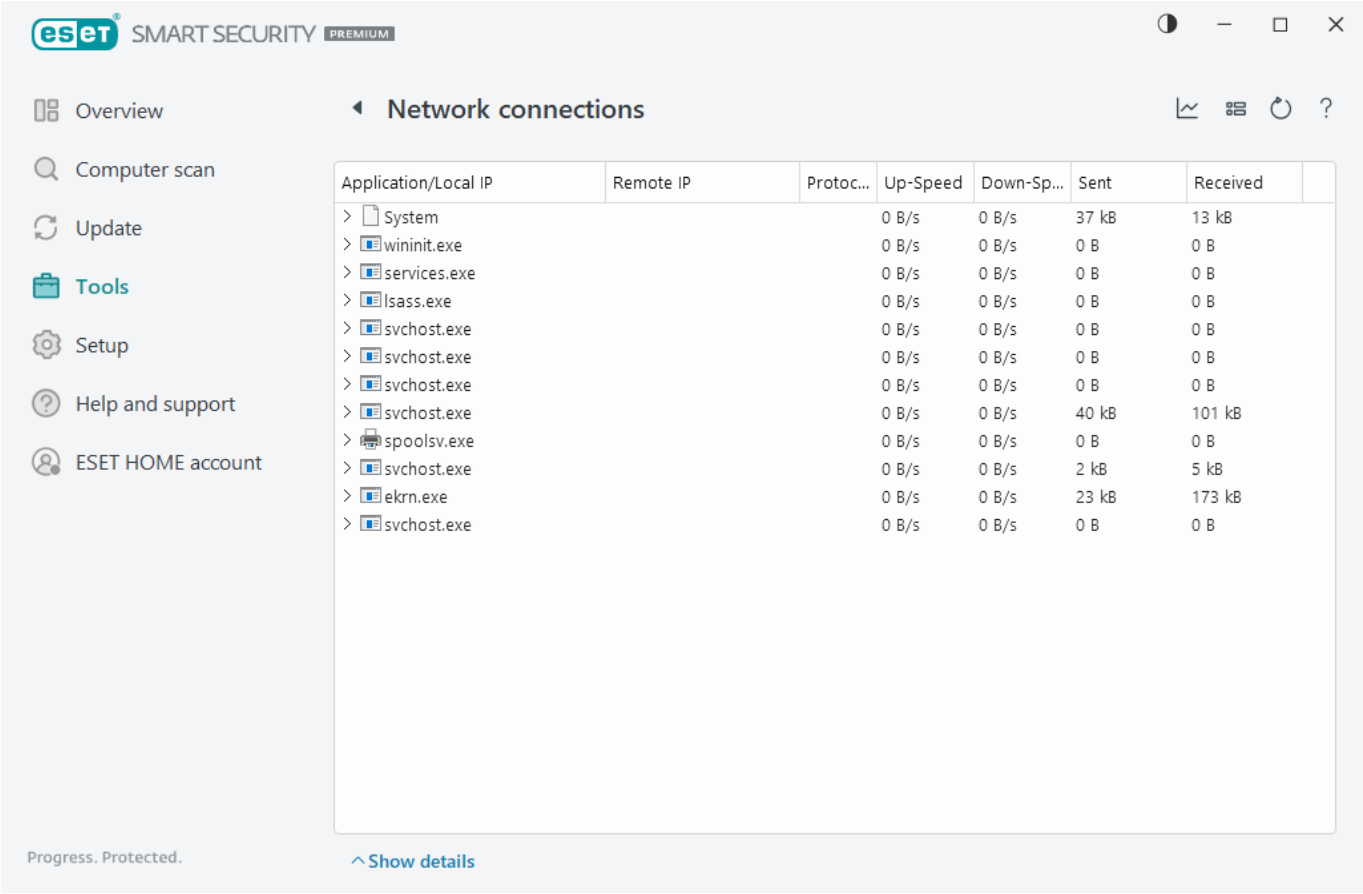
Cuando se active una función, dejará de aparecer como no operativa en el informe de seguridad.

Haga clic en la rueda del engranaje de la esquina superior derecha para **Activar/Desactivar notificaciones del informe de seguridad** o seleccione si se mostrarán datos de los últimos 30 días o desde que se activó el producto. Si ESET Small Business Security se instaló hace menos de 30 días, solo se podrá seleccionar el número de días que han transcurrido desde que se instaló. De forma predeterminada está establecido un periodo de 30 días.


**Restablecer datos** borrará todas las estadísticas y quitará los datos existentes en el informe de seguridad. Esta acción se debe confirmar, salvo si desea anular la selección de la opción **Preguntar antes de restablecer las estadísticas** en Configuración avanzada > **Notificaciones** > **Alertas interactivas** > **Mensajes de confirmación** > **Editar**.

# Conexiones de red

En la sección Conexiones de red, puede ver una lista de las conexiones activas y pendientes. Esto le ayuda a controlar todas las aplicaciones que establecen conexiones salientes.




Haga clic en el icono de gráfico para abrir la actividad de red.

En la primera línea se muestran el nombre de la aplicación y la velocidad de transferencia de datos. Para ver la lista de conexiones establecidas por la aplicación y obtener más información, haga clic en **>**.

## Columnas

**Aplicación/IP local**: nombre de la aplicación, direcciones IP locales y puertos de comunicación.

**IP remota**: dirección IP y número de puerto de un ordenador remoto determinado.

**Protocolo**: protocolo de transferencia utilizado.

**Velocidad de carga/velocidad de descarga**: la velocidad actual de los datos salientes y entrantes.

**Enviados/recibidos**: cantidad de datos intercambiados dentro de la conexión.

**Mostrar detalles**: seleccione esta opción para mostrar información detallada sobre la conexión seleccionada.

Haga clic con el botón derecho del ratón en una conexión para ver más opciones, como:

**Resolver nombres de host**: si es posible, todas las direcciones de red se mostrarán en formato DNS, y no en el

formato numérico de dirección IP.

**Mostrar solo las conexiones TCP**: la lista incluye únicamente las conexiones que pertenecen al protocolo TCP.

**Mostrar conexiones en escucha**: seleccione esta opción para mostrar únicamente las conexiones en las que no haya ninguna comunicación establecida actualmente, pero en las que el sistema haya abierto un puerto y esté esperando una conexión.

**Mostrar las conexiones del ordenador**: seleccione esta opción únicamente para mostrar conexiones en las que la ubicación remota sea un sistema local, lo que se denominan conexiones de localhost.

**Velocidad de actualización**: selecciona la frecuencia de actualización de las conexiones activas.

**Actualizar ahora**: vuelve a cargar la ventana **Conexiones de red**.

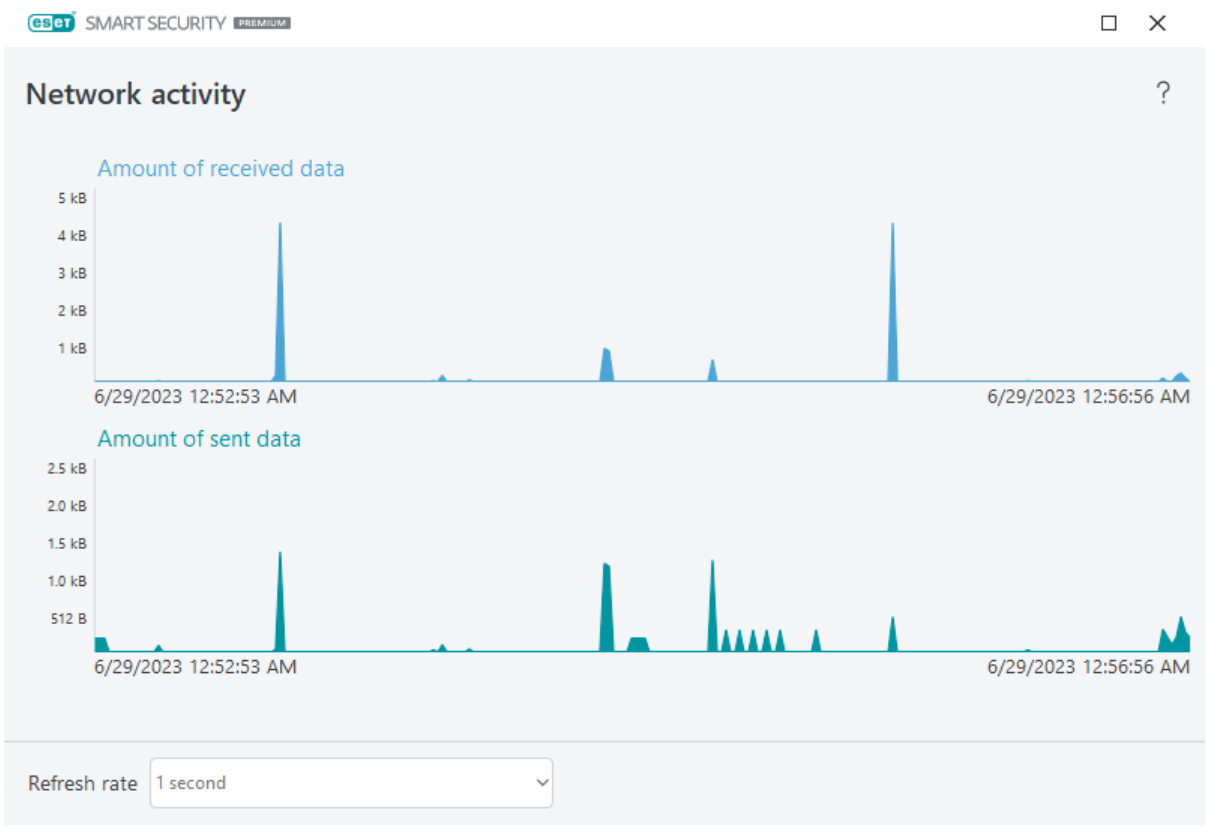
Las opciones siguientes están disponibles al hacer clic en una aplicación o proceso, no en una conexión activa:

**Denegar temporalmente la comunicación para el proceso**: rechaza las conexiones actuales de una aplicación determinada. Si se establece una nueva conexión, el cortafuegos utiliza una regla predefinida. La descripción de la configuración puede encontrarse en la sección Reglas de cortafuegos.

**Permitir temporalmente la comunicación para el proceso**: permite las conexiones actuales de una aplicación determinada. Si se establece una nueva conexión, el cortafuegos utiliza una regla predefinida. La descripción de la configuración puede encontrarse en la sección Reglas de cortafuegos.

# Actividad de red

Para ver la **actividad de red** actual en un gráfico, haga clic en **Herramientas** > **Conexiones de red** y seleccione el icono de gráfico . En la parte inferior del gráfico hay una línea cronológica que registra la actividad de la red en tiempo real durante el intervalo de tiempo seleccionado. Si desea cambiar el intervalo de tiempo, seleccione el valor correspondiente en el menú desplegable **Índice de actualización**.




Están disponibles las opciones siguientes:

- **Pasar 1 segundo**: el gráfico se actualiza cada segundo y la línea cronológica abarca los últimos 4 minutos.
- **Pasar 1 minuto (últimas 24 horas)**: el gráfico se actualiza cada minuto y la línea cronológica abarca las últimas 24 horas.
- **Pasar 1 hora (último mes)**: el gráfico se actualiza cada hora y la línea cronológica abarca el último mes.

El eje vertical del gráfico representa la cantidad de datos recibidos o enviados. Coloque el ratón sobre el gráfico para ver la cantidad exacta de datos recibidos o enviados a una hora concreta.

# ESET SysInspector

ESET SysInspector es una aplicación que inspecciona a fondo el ordenador, recopila información detallada sobre los componentes del sistema (como los controladores y aplicaciones instalados, las conexiones de red o las entradas importantes del registro) y evalúa el nivel de riesgo de cada componente.

Esta información puede ayudar a determinar la causa de un comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de código malicioso. Para aprender a usar ESET SysInspector, consulte la Ayuda en línea de ESET SysInspector.

En la ventana de ESET SysInspector se muestra la siguiente información sobre los registros:

- **Fecha y hora**: fecha y hora de creación del registro.
- **Comentario**: breve comentario.
- **Usuario**: nombre del usuario que creó el registro.

- **Estado**: estado de la creación del registro.

Están disponibles las siguientes acciones:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector. También puede hacer clic con el botón derecho del ratón sobre un archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.

- **Crear**: crea un registro nuevo. Espere a que se genere ESET SysInspector (estado **Creado**) antes de intentar acceder al registro. El registro se guarda en C:\ProgramData\ESET\ESET Security\SysInspector.

- **Eliminar**: elimina de la lista los archivos de registro seleccionados.

El menú contextual ofrece las siguientes opciones al seleccionar uno o más archivos de registro:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).

- **Crear**: crea un registro nuevo. Espere a que se genere ESET SysInspector (estado **Creado**) antes de intentar acceder al registro.

- **Eliminar**: elimina de la lista los archivos de registro seleccionados.

- **Eliminar todos**: elimina todos los registros.

- **Exportar**: exporta el registro a un archivo .esil o .json.

# Tareas programadas

El planificador de tareas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas.

Tareas programadas está disponible en la ventana principal de ESET Small Business Security; para acceder, haga clic en **Herramientas** > **Tareas programadas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

El Planificador de tareas sirve para programar las siguientes tareas: módulos de actualización, tarea de análisis, verificación de archivos en el inicio del sistema y mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana Planificador de tareas (haga clic en **Agregar tarea** o **Eliminar** en la parte inferior).

Puede restaurar los valores predeterminados de la lista de tareas programadas y eliminar todos los cambios haciendo clic en **Predeterminado**. Haga clic con el botón derecho en cualquier parte de la ventana Planificador de tareas para realizar las siguientes acciones: mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente. Utilice las casillas de verificación disponibles al comienzo de cada entrada para activar o desactivar las tareas.

De forma predeterminada, en el **Planificador de tareas** se muestran las siguientes tareas programadas:

- **Mantenimiento de registros**

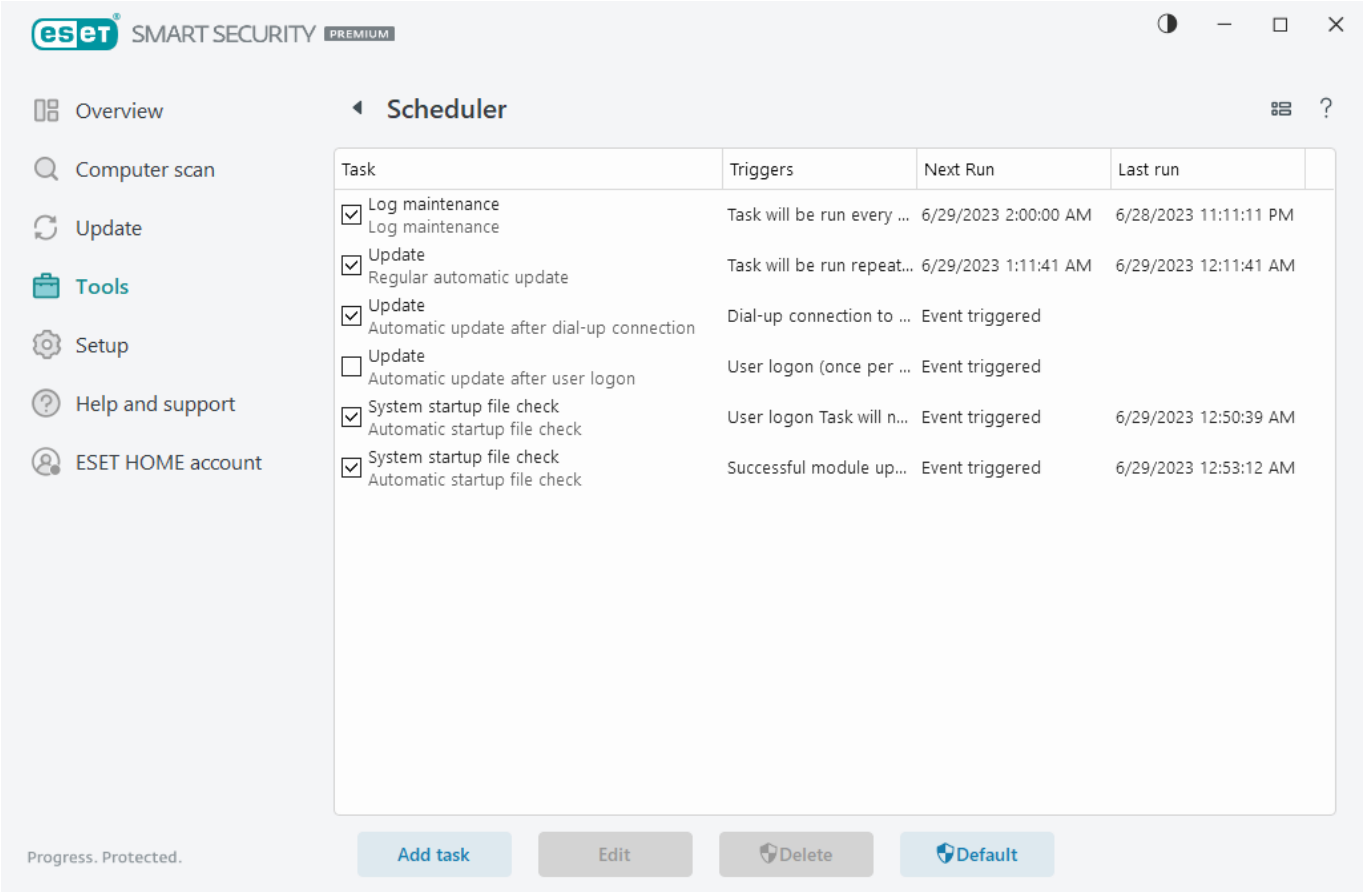
- **Actualización automática de rutina**

- **Actualización automática después del registro del usuario**

• **Verificación automática de archivos en el inicio** (tras inicio de sesión del usuario)

• **Verificación de la ejecución de archivos en el inicio** (después de actualizar correctamente el motor de detección)

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón derecho en la tarea y, a continuación, haga clic en **Modificar** o seleccione la tarea que desea modificar y haga clic en **Modificar**.




## Agregar una nueva tarea

1. Haga clic en **Agregar tarea**, en la parte inferior de la ventana.

2. Introduzca un nombre para la tarea.

3. Seleccione la tarea deseada en el menú desplegable:

• **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.

• **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.

• **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.

• **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones)

y evalúa el nivel de riesgo de cada componente.

- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

4. Active el interruptor situado junto a **Activado** para activar la tarea (puede hacerlo más adelante marcando o desmarcando la casilla de verificación en la lista de tareas programadas), haga clic en **Siguiente** y seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará en la fecha y a la hora predefinidas.
- **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado.
- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
- **Semanalmente**: la tarea se ejecutará el día y a la hora seleccionados.
- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

5. Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se ejecutará de nuevo:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si el tiempo desde la última ejecución supera (horas)**: representa el tiempo transcurrido desde la primera ejecución omitida de la tarea. Si se supera este tiempo, la tarea se ejecutará inmediatamente. Establezca el tiempo con el selector que aparece a continuación.

Para revisar la tarea programada, haga clic con el botón derecho en la tarea y, a continuación, haga clic en **Mostrar detalles de la tarea**.

# Opciones de análisis programado

En esta ventana puede especificar opciones avanzadas para una tarea de análisis programado del ordenador.

Para ejecutar un análisis sin desinfección, haga clic en **Configuración avanzada** y seleccione **Analizar sin desinfectar**. El historial del análisis se guarda en el registro del análisis.

Cuando se selecciona **Ignorar exclusiones**, se analizan sin excepciones los archivos con extensiones excluidas anteriormente del análisis.

En el menú desplegable **Acción tras el análisis** puede establecer la acción que desea efectuar automáticamente cuando concluya el análisis:

- **Sin acciones**: cuando el análisis concluya no se realizará ninguna acción.
- **Apagar**: el ordenador se apaga cuando finaliza el análisis.

- **Reiniciar si es necesario**: el ordenador se reinicia solo si es necesario para completar la desinfección de las amenazas detectadas.

- **Reiniciar**: cierra todos los programas abiertos y reinicia el ordenador cuando concluye el análisis.

- **Forzar reinicio si es necesario**: el ordenador fuerza el reinicio solo si es necesario para completar la desinfección de las amenazas detectadas.

- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el ordenador cuando concluye el análisis.

- **Suspender**: guarda la sesión y establece el ordenador en un estado de bajo consumo para que pueda retomar su trabajo rápidamente.

- **Hibernar**: recopila todos los programas y archivos que se encuentran en ejecución en la RAM y los guarda en un archivo especial de su disco duro. El ordenador se apaga, pero la próxima vez que lo encienda presentará el estado anterior al apagado.

> Las acciones **Suspender** o **Hibernar** estarán disponibles según la configuración de las opciones de encendido y suspensión del sistema operativo de su ordenador o las prestaciones correspondientes. Debe tener en cuenta que cuando el ordenador está en suspensión sigue en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad si funciona con la alimentación de la batería. Si desea ahorrar carga de la batería, por ejemplo al salir de la oficina, le recomendamos utilizar la opción Hibernar.

La acción seleccionada se iniciará cuando finalicen todos los análisis que se están ejecutando. Cuando se seleccione **Apagar** o **Reiniciar**, se mostrará un cuadro de diálogo de confirmación de apagado con una cuenta atrás de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

Seleccione **El análisis no se puede cancelar** para impedir a los usuarios sin privilegios que detengan las acciones realizadas tras el análisis.

Seleccione la opción **El usuario puede poner en pausa el análisis durante (min)** si desea permitir que un usuario limitado pause el análisis del ordenador durante un periodo de tiempo especificado.

Consulte también Progreso del análisis.

# Resumen general de tareas programadas

En este cuadro de diálogo se muestra información detallada sobre la tarea programada seleccionada al hacer doble clic en una tarea personalizada o al hacer clic con el botón derecho del ratón en una tarea personalizada del planificador de tareas y, a continuación, hacer clic en **Mostrar detalles de la tarea**.

# Detalles de la tarea

Escriba el **nombre de la tarea**, seleccione un **tipo de tarea** y, a continuación, haga clic en **Siguiente**:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.

- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su

eficacia.

- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.

- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.

- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.

- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

# Tiempo de las tareas

La tarea se repetirá con el intervalo de tiempo especificado. Seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará solo una vez en la fecha y a la hora predefinidas.

- **Reiteradamente**: la tarea se ejecutará en el intervalo especificado (en horas).

- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.

- **Semanalmente**: la tarea se ejecutará una o varias veces por semana, en los días y a la hora seleccionados.

- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

**No ejecutar la tarea si está funcionando con batería**: la tarea no se iniciará si el ordenador está funcionando con batería en el momento en que está programado el inicio de la tarea. Esto también se aplica a los ordenadores que funcionan con SAI (sistema de alimentación ininterrumpida).

# Sincronización de la tarea: una vez

**Ejecución de la tarea**: la tarea especificada solo se ejecutará una vez a la fecha y hora especificadas.

# Sincronización de la tarea: diariamente

La tarea se ejecutará todos los días a la hora especificada.

# Sincronización de la tarea: semanalmente

La tarea se ejecutará todas las semanas en los días y horas seleccionados.

# Sincronización de la tarea: cuando se cumpla la condición

La tarea se desencadenará cuando se produzca uno de los siguientes sucesos:

- **Cada vez que se inicie el ordenador.**
- **La primera vez que se inicie el ordenador en el día**
- **Conexión a Internet/VPN por módem**
- **Actualización de módulo correcta**
- **Actualización de producto correcta**
- **Registro del usuario**
- **Detección de amenazas**

Cuando se programa una tarea desencadenada por un suceso, se puede especificar el intervalo mínimo entre dos finalizaciones de la tarea. Por ejemplo, si inicia sesión en su ordenador varias veces al día, seleccione 24 horas para realizar la tarea solo en el primer inicio de sesión del día y, después, al día siguiente.

# Tarea omitida

Una tarea se puede omitir si el ordenador está apagado o funciona con batería. Seleccione cuándo desea que se ejecute la tarea omitida y haga clic en **Siguiente**:

- **En la siguiente hora programada**: la tarea se ejecutará si el ordenador está encendido en la siguiente hora programada.
- **Lo antes posible**: la tarea se ejecutará cuando el ordenador esté encendido.
- **Inmediatamente, si el tiempo desde la última ejecución programada supera (horas)**: representa el tiempo transcurrido desde la primera ejecución omitida de la tarea. Si se supera este tiempo, la tarea se ejecutará inmediatamente.

### Inmediatamente, si el tiempo desde la última ejecución programada supera (horas) –ejemplos

Hay una tarea de ejemplo configurada para que se ejecute de forma reiterada en cada hora. La opción **Inmediatamente, si el tiempo desde la última ejecución programada supera (horas)** está seleccionada y el tiempo superado está establecido en dos horas. La tarea se ejecuta a las 13:00 y, cuando finaliza, el ordenador se queda en suspensión:

- El ordenador se activa a las 15:30. La primera ejecución omitida de la tarea fue a las 14:00. Solo han transcurrido 1,5 horas desde las 14:00, por lo que la tarea se ejecutará a las 16:00.
- El ordenador se activa a las 16:30. La primera ejecución omitida de la tarea fue a las 14:00. Han transcurrido dos horas y media desde las 14:00, por lo que la tarea se ejecutará inmediatamente.

# Detalles de la tarea: actualización

Si desea actualizar el programa desde dos servidores de actualización, es necesario crear dos perfiles de actualización diferentes. Así, si el primer servidor no descarga los archivos de actualización, el programa cambia al otro automáticamente.

Esta función es útil para portátiles, por ejemplo, ya que normalmente se actualizan desde un servidor de actualización LAN local, aunque sus propietarios suelen conectarse a Internet utilizando otras redes. Así pues, en caso de que el primer perfil falle, el segundo descargará automáticamente los archivos de actualización de los servidores de actualización de ESET.

# Detalles de la tarea: ejecutar aplicación

Esta tarea programa la ejecución de una aplicación externa.

**Archivo ejecutable**: seleccione un archivo ejecutable en el árbol de directorios y haga clic en la opción **...**, o introduzca la ruta manualmente.

**Carpeta de trabajo**: defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **archivo ejecutable** seleccionado se crearán en este directorio.

**Parámetros**: parámetros de la línea de comandos de la aplicación (opcional).

Haga clic en **Finalizar** para aplicar la tarea.

# Limpieza del sistema

Limpieza del sistema es una herramienta que le ayuda a restaurar el ordenador a un estado utilizable tras la desinfección de la amenaza. El código malicioso puede desactivar utilidades del sistema como el Editor del registro, el Administrador de tareas o las Actualizaciones de Windows. La desinfección del sistema restablece los ajustes y los valores predeterminados de cada sistema con un clic.

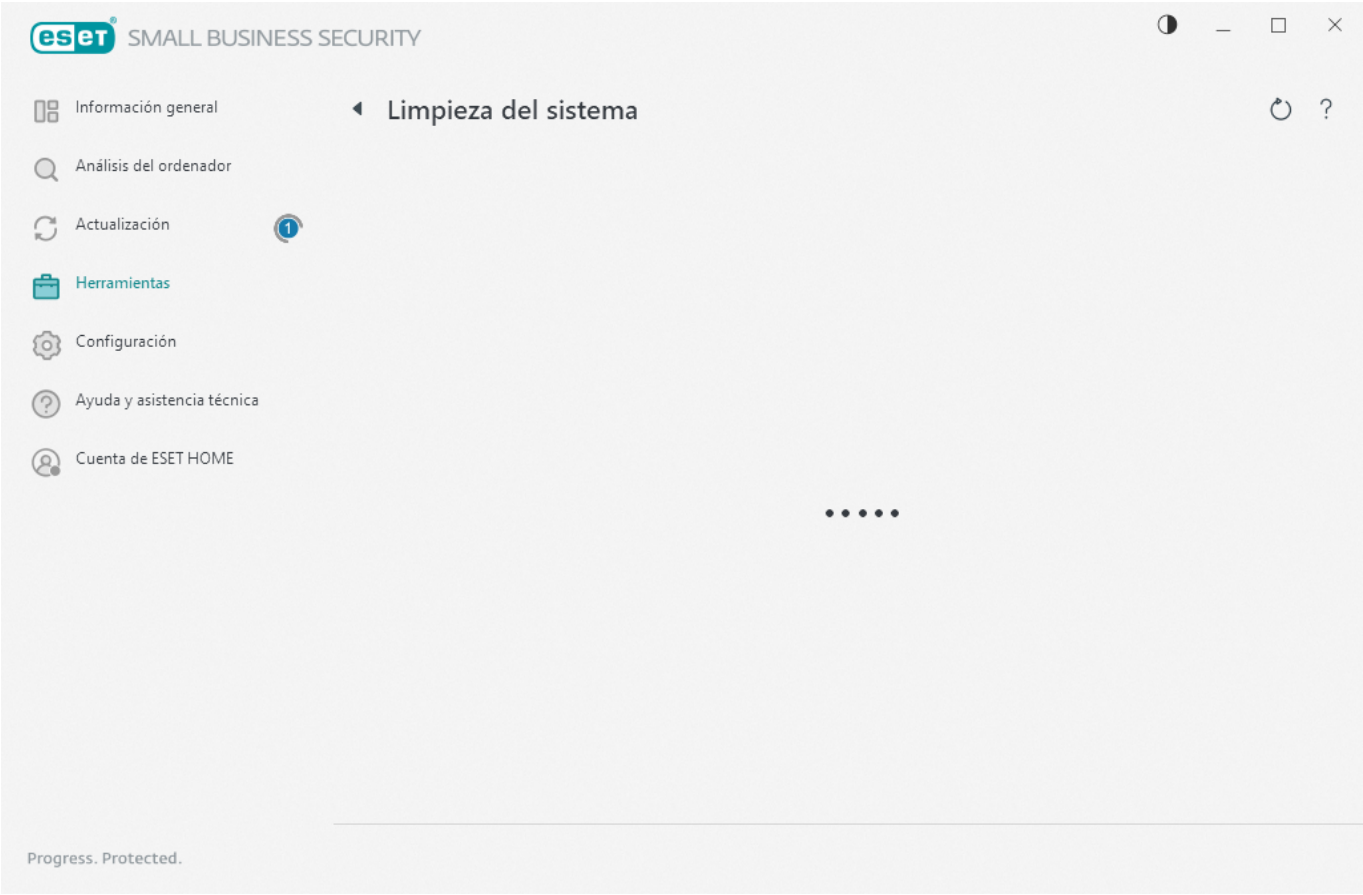
La limpieza del sistema comunica problemas de cinco categorías de ajustes:

- **Configuración de seguridad**: cambios de ajustes que pueden aumentar la vulnerabilidad de su ordenador, como Windows Update.
- **Ajustes del sistema**: cambios de los ajustes del sistema que pueden modificar el comportamiento de su ordenador, como asociaciones de archivos.
- **Aspecto del sistema**: ajustes que afectan a la apariencia del sistema, como el fondo de pantalla.
- **Funciones desactivadas**: funciones y aplicaciones importantes que podrían estar desactivadas.
- **Restauración del sistema Windows**: ajustes de la función Restauración del sistema Windows, que le permite devolver el sistema a un estado anterior.

La limpieza del sistema puede solicitarse en las siguientes situaciones:

- Cuando se detecta una amenaza.
- Cuando un usuario hace clic en **Restablecer**.

Puede revisar los cambios y restablecer la configuración si procede.




Solo un usuario con derechos de administrador puede realizar acciones en la Limpieza del sistema.

# Inspector de red

Inspector de red puede ayudar a identificar vulnerabilidades en su red de confianza (doméstica o de oficina; ejemplo, puertos abiertos o una contraseña débil de router). También ofrece una lista de los dispositivos conectados, categorizados por tipo de dispositivo (por ejemplo, impresora, router, dispositivo móvil, etc.) para mostrarle lo que está conectado a su red (por ejemplo, videoconsola, IoT u otros dispositivos domésticos inteligentes).

El Inspector de red le ayuda a identificar las vulnerabilidades de un router y aumenta el nivel de protección cuando se establece conexión con una red.

Inspector de red no reconfigura el router por usted. Debe hacer los cambios usted utilizando la interfaz especializada del router. Los routers domésticos pueden ser altamente vulnerables al malware que se utiliza para lanzar ataques de denegación de servicio distribuidos (DDoS). Si el usuario no ha cambiado la contraseña predeterminada del router, los hackers podrán adivinarla fácilmente y, a continuación, iniciar sesión en el router y reconfigurarlo o poner su red en peligro.

Recomendamos encarecidamente crear una contraseña segura lo suficientemente larga y que incluya números, símbolos y letras en mayúscula y minúscula. Para que la contraseña resulte más difícil de adivinar, utilice una mezcla de distintos tipos de caracteres.

Si la red a la que está conectado está configurada como de confianza, puede marcar la red como "Mi red". Haga clic en **Marcar como "Mi red"** para agregar una etiqueta Mi red a la red. Esta etiqueta se mostrará junto a la red en todas las secciones de ESET Small Business Security para mejorar la identificación y la visión general de seguridad. Haga clic en **Desmarcar como "Mi red"** para quitar la etiqueta.

Todos los dispositivos conectados a su red se muestran en una vista de lista con información básica. Haga clic en el dispositivo específico para editarlo o ver información detallada.

En la vista de lista, el menú desplegable **Redes** le permite filtrar dispositivos en función de los siguientes criterios:

- Dispositivos conectados a una red concreta
- Dispositivos conectados a **Todas las redes**
- Dispositivos sin clasificar

Para mostrar todos los dispositivos conectados a la red en vista de sonar, haga clic en el icono de sonar . Coloque el cursor sobre un icono de dispositivo para ver información básica, como el nombre de la red y la fecha de última conexión.

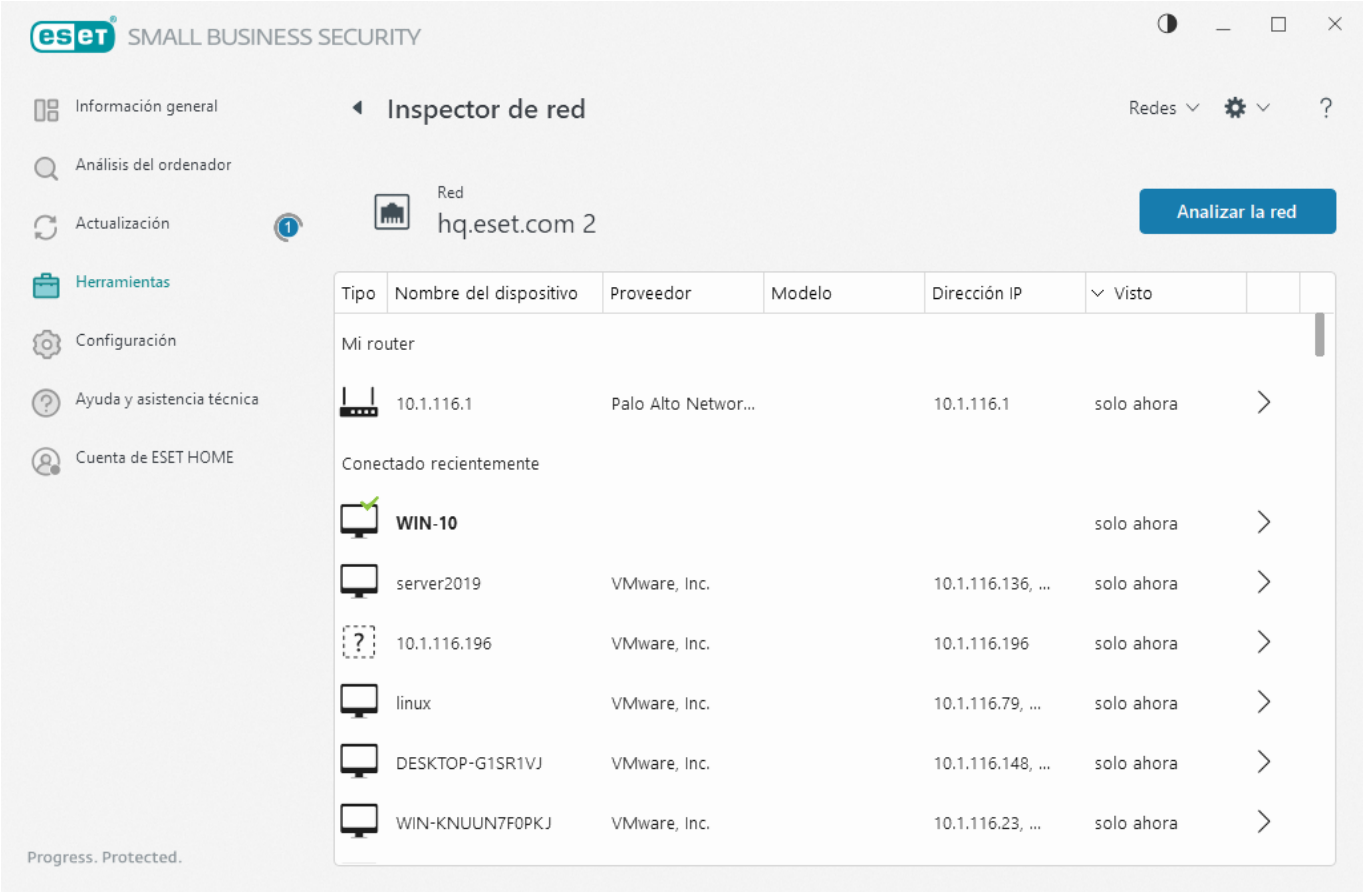
Haga clic en el icono de dispositivo para editarlo o ver información detallada. Los dispositivos conectados recientemente se muestran más cerca del router para que pueda detectarlos fácilmente.

Haga clic en **Analizar la red** para realizar manualmente un análisis de la red a la que está conectado. **Analizar la red** solo está disponible para una red de confianza. Consulte Perfiles de conexión de la red para revisar o editar la configuración de red.

Tiene las siguientes opciones de análisis:

- Analizarlo todo
- Analizar solo el router
- Analizar solo los dispositivos

Realice análisis de red solo en redes de confianza. Si lo hace en redes no de confianza, debe tener en cuenta los posibles riesgos.




Una vez finalizado el análisis, se mostrará una notificación con un vínculo a información básica sobre el dispositivo; también puede hacer doble clic en el dispositivo sospechoso en una vista de lista o sonar. Haga clic en **Solucionar problemas** para ver las comunicaciones recientemente bloqueadas. Más información sobre la solución de problemas del cortafuegos.

El módulo Inspector de red muestra dos tipos de notificaciones:

- **Nuevo dispositivo conectado a la red**: se muestra si un dispositivo que anteriormente no se ha visto se conecta a la red mientras el usuario está conectado.
- **Se han encontrado dispositivos de red nuevos**: se muestra si se vuelve a conectar a la red de confianza y hay un dispositivo que no se había detectado anteriormente.

Ambos tipos de notificación le informan si un dispositivo no autorizado intenta conectarse a su red. Haga clic en **ver dispositivo** para ver los detalles del dispositivo.

## ¿Qué significan los iconos de los dispositivos en Inspector de red?

| | |
|---|---|
| | El icono de estrella amarilla indica los dispositivos que son nuevos en la red o que ESET ha detectado por primera vez. |
| | El icono de precaución amarillo indica que su router puede contener vulnerabilidades. Haga clic en el icono de su producto para obtener información detallada sobre el problema. |
| | El icono rojo de advertencia indica a los dispositivos que su router contiene vulnerabilidades y pueden infectarse. Haga clic en el icono de su producto para obtener información detallada sobre el problema. |
| | El icono azul puede aparecer cuando el producto de ESET contiene información adicional para su router pero no requiere atención inmediata, ya que no hay riesgos de seguridad. Haga clic en el icono de su producto para obtener información detallada. |

# Dispositivo de red en Inspector de red

Aquí puede encontrar información detallada sobre el dispositivo, como por ejemplo:

- Nombre del dispositivo
- Tipo de dispositivo
- Visto por última vez
- Nombre de red
- Dirección IP
- Dirección MAC
- Sistema operativo

El icono de lápiz indica que puede modificar el nombre o tipo del dispositivo.

**Quitar del historial**: elimina el dispositivo de la lista de dispositivos. Esta opción solo está disponible para los dispositivos que no están conectados a su red en ese momento.

Para cada tipo de dispositivo, están disponibles las siguientes acciones:

Router

**Configuración del router**: acceda a la configuración del router desde la interfaz web o la aplicación móvil o haga clic en **Abrir la interfaz del router**. Si tiene un router proporcionado por su proveedor de servicios de Internet, puede ser necesario que se ponga en contacto con los recursos de soporte del proveedor de servicios de Internet o con el fabricante del router para resolver los problemas de seguridad detectados. Siga siempre las precauciones de seguridad indicadas en la guía del usuario de su router.
**Protección** – Para proteger su router y su red de ataques contra la seguridad informática, siga estas recomendaciones básicas.

Dispositivo de red

**Identificación del dispositivo**: en caso de que tenga dudas sobre el dispositivo conectado a su red, compruebe el nombre del distribuidor o fabricante bajo el nombre del dispositivo. Esto puede ayudarle a identificar de qué tipo de dispositivo se trata. Puede cambiar el nombre del dispositivo para poder consultarlo en el futuro.
**Desconexión del dispositivo**: en caso de que tenga dudas sobre si un dispositivo conectado es seguro para su red o sus dispositivos, administre el acceso a la red de este dispositivo en la configuración de su router o cambie la contraseña de su red.
**Protección**: para proteger su dispositivo de ataques y software malicioso, instale una solución de seguridad informática en el dispositivo y mantenga siempre actualizados el sistema operativo y el software instalado. Para garantizar su protección, no se conecte a redes Wi-Fi desprotegidas.

Este dispositivo

Este dispositivo representa a su ordenador en la red.
**Adaptadores de red**: muestra la información de sus adaptadores de red.

# Notificaciones | Inspector de red

A continuación se muestran diversas notificaciones que pueden aparecer cuando ESET Small Business Security detecta algún problema de vulnerabilidad en el router. Cada notificación contiene una descripción breve, y ofrece soluciones o pasos que se deben seguir para minimizar el riesgo de vulnerabilidad del router. Si no está familiarizado con realizar cambios en el router, le recomendamos que se ponga en contacto con el fabricante del router o el proveedor de servicios de Internet.

**Se ha encontrado una posible vulnerabilidad**
Su router puede contener vulnerabilidades conocidas que pueden hacer que resulte fácil de atacar y acceder. Actualice el firmware de su router.

**Vulnerabilidad encontrada**
Su router contiene vulnerabilidades conocidas que hacen que resulte fácil de atacar y acceder. Actualice el firmware de su router.

**Amenaza detectada**
Su router está infectado por software malicioso. Reinicie su router y repita el análisis.

**Contraseña de router débil**
La contraseña de su router es débil y otra persona podría adivinarla. Cambie la contraseña de su router.

**Redirección de red maliciosa**
Parece que su tráfico de Internet está redirigido a sitios web malintencionados. Esto puede significar que su router está en situación de riesgo. Cambie el ajuste de servidor DNS de su router.

**Servicios de red abiertos**
En su router hay en ejecución algunos servicios de red que otras personas pueden utilizar. Esto puede deberse a una configuración deficiente o a un router en situación de riesgo. Revise la configuración de su router.

**Servicios de red confidenciales abiertos**
En su router hay en ejecución algunos servicios de red confidenciales que otras personas pueden utilizar. Esto puede deberse a una configuración deficiente o a un router en situación de riesgo. Revise la configuración de su router.

**Firmware obsoleto**
El firmware de su router está obsoleto y puede contener vulnerabilidades. Actualice el firmware de su router.

**Ajuste de router malicioso**
El servidor DNS que utiliza es malintencionado y puede enviarle a sitios web peligrosos. Esto puede significar que su router está en situación de riesgo. Cambie el ajuste de servidor DNS de su router.

**Servicios de red**
En su router hay en ejecución servicios de red comunes. Son necesarios para la red y probablemente sean seguros. Revise la configuración de su router.

# Cuarentena

La función principal de la cuarentena es almacenar de forma segura objetos que se clasifican como peligrosos (como malware, archivos infectados o aplicaciones potencialmente indeseables).

Puede acceder a la cuarentena en la ventana principal de ESET Small Business Security. Para ello, haga clic en **Herramientas** > **Cuarentena**.

Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra:

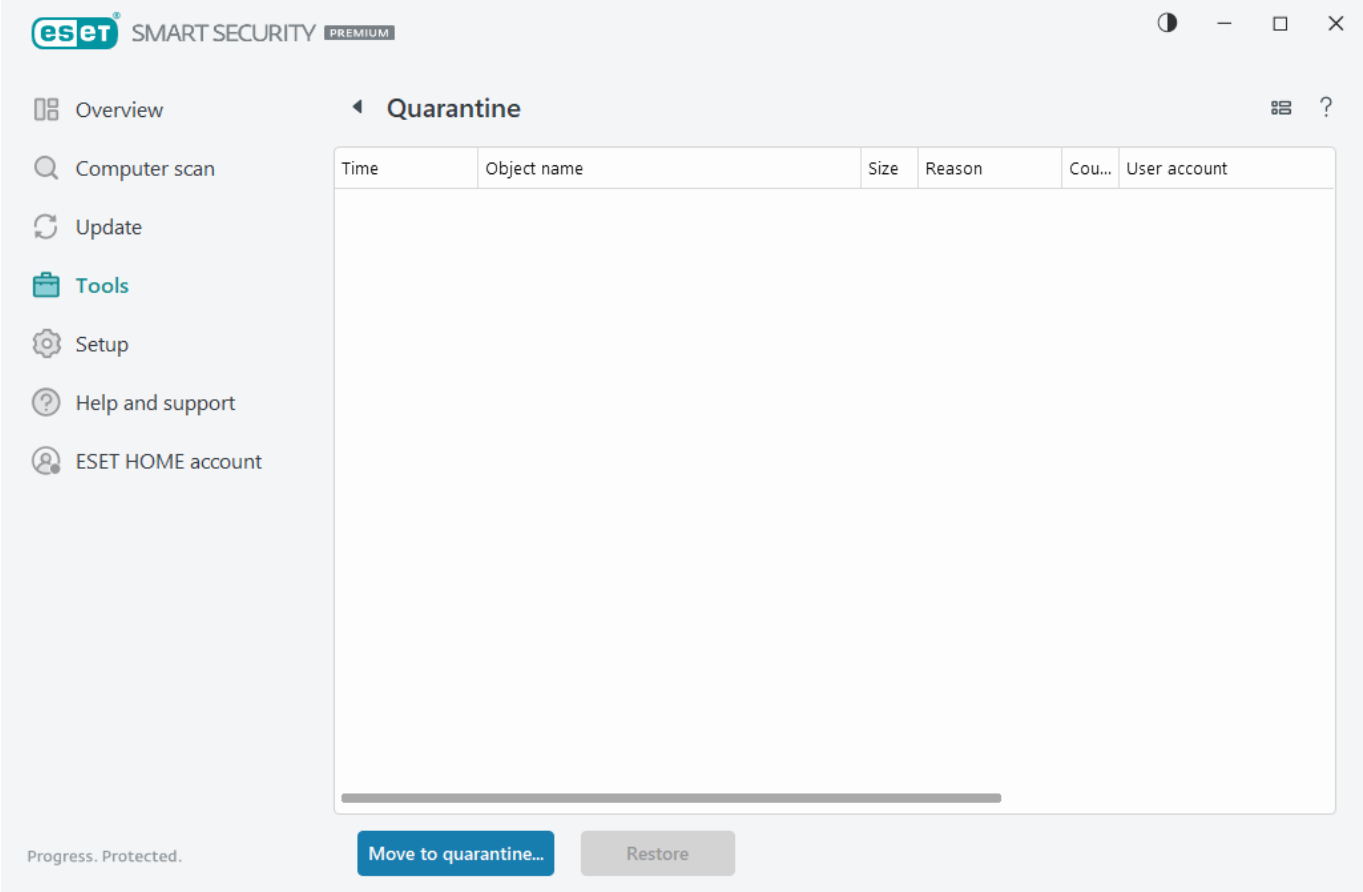
• La fecha y la hora de la cuarentena.

• La ruta de acceso a la ubicación original del archivo.

• Su tamaño en bytes.

• Motivo (por ejemplo, objeto agregado por el usuario).

• Número de detecciones (por ejemplo, detecciones duplicadas de un mismo archivo o si se trata de un archivo comprimido que contiene varias infiltraciones).




## Poner archivos en cuarentena

ESET Small Business Security pone en cuarentena automáticamente los archivos eliminados (si no ha cancelado esta opción en la ventana de alertas).

Otros archivos se deben poner en cuarentena si:

a.No se pueden desinfectar.

b.No es seguro ni aconsejable eliminarlos.

c.ESET Small Business Security los detecta incorrectamente como infectados.

d.El comportamiento de un archivo es sospechoso, pero Protecciones no lo detecta.

Para poner en cuarentena un archivo, tiene varias opciones:

a.Utilice la función de arrastrar y colocar para poner en cuarentena un archivo manualmente al hacer clic

en el archivo, desplazar el cursor del ratón hasta la zona marcada mientras se mantiene pulsado el botón del ratón, para después soltarlo. Después, la aplicación pasa al primer plano.

b.Haga clic con el botón derecho del ratón en el archivo > haga clic en **Opciones avanzadas** > **Archivo de cuarentena**.

c.Haga clic en **Mover a cuarentena** desde la ventana **Cuarentena**.

d.El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

## Restauración de archivos de cuarentena

Los archivos en cuarentena también pueden restaurarse en su ubicación original:

- Utilice la función **Restaurar** para tal fin, disponible desde el menú contextual si hace clic con el botón derecho en un archivo determinado en cuarentena.

- Si un archivo se marca como aplicación potencialmente indeseable, la opción **Restaurar y excluir** se activa. Consulte también Exclusiones.

- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar archivos en una ubicación distinta de la cual se eliminaron.

- La función de restauración no está disponible en algunos casos, por ejemplo, para los archivos que se encuentran en un recurso compartido de red de solo lectura.

## Eliminación de archivos de cuarentena

Haga clic con el botón derecho del ratón en el elemento que desee y seleccione **Eliminar de la cuarentena**, o seleccione el elemento que desee eliminar y pulse **Suprimir** en el teclado. Si desea seleccionar y eliminar todos los elementos de la Cuarentena, puede pulsar **Ctrl + A** y luego **Delete** en el teclado. Los elementos eliminados se eliminarán de forma permanente de su dispositivo y de la cuarentena.

## Envío de un archivo de cuarentena

Si ha puesto en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha determinado incorrectamente que un archivo está infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, se ha puesto en cuarentena, envíe la muestra al laboratorio de investigación de ESET para su análisis. Para enviar un archivo, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

## Descripción de la detección

Haga clic con el botón derecho del ratón en un elemento y, a continuación, haga clic en **Descripción de la detección** para abrir la Enciclopedia de amenazas de ESET, que contiene información detallada sobre los peligros y los síntomas de la infiltración registrada.

Instrucciones con ilustraciones

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- Restaurar un archivo en cuarentena en ESET Small Business Security
- Eliminar un archivo en cuarentena en ESET Small Business Security
- Mi producto de ESET me ha avisado de una detección, ¿qué debo hacer?

## Error al poner en cuarentena

Los motivos por los que archivos concretos no pueden moverse a la cuarentena son los siguientes:

- **No tiene permisos de lectura**: significa que no puede ver el contenido de un archivo.
- **No tiene permisos de escritura**: significa que no puede modificar el contenido del archivo, es decir, agregar nuevo contenido o eliminar el contenido existente.
- **El archivo que está intentando poner en cuarentena es demasiado grande,**: tiene que reducir el tamaño del archivo.

Cuando reciba el mensaje de error "Error al poner en cuarentena", haga clic en **Más información**. Aparece la ventana de lista de errores de cuarentena y se mostrarán el nombre del archivo y el motivo por el que no se puede poner en cuarentena el archivo.

# Seleccionar muestra para el análisis

Si encuentra un archivo sospechoso en su ordenador o un sitio sospechoso en Internet, puede enviarlos al laboratorio de investigación de ESET para que los analicen (puede que no esté disponible en función de su configuración de ESET LiveGrid®).

Antes de enviar muestras a ESET

No envíe muestras que no cumplan al menos uno de los siguientes criterios:

- Su producto de ESET no detecta la muestra.
- La muestra se detecta como una amenaza, pero no lo es.
- No aceptamos archivos personales (que le gustaría que ESET analizara para buscar malware) como muestras (el laboratorio de investigación de ESET no realiza análisis bajo demanda para sus usuarios).
- Utilice un asunto descriptivo y adjunte toda la información posible sobre el archivo (por ejemplo, una captura de pantalla o el sitio web del que lo descargó).

Puede enviar una muestra (un archivo o un sitio web) para que ESET la analice a través de uno de los siguientes métodos:

1. Utilice el formulario de envío de muestras de su producto. Se encuentra en **Herramientas** > **Enviar muestra para su análisis**. El tamaño máximo de una muestra enviada es de 256 MB.

2. También puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima los archivos con WinRAR/WinZIP, proteja el archivo comprimido con la contraseña "infected" y envíelo a samples@eset.com.

3. Si desea informar sobre spam o falsos positivos de spam, consulte el artículo de la base de conocimiento de ESET.

En el formulario **Seleccionar muestra para el análisis**, seleccione en el menú desplegable **Motivo de envío de la muestra** la descripción que mejor se ajuste al fin de su mensaje:

- Archivo sospechoso
- Sitio sospechoso (sitio web que está infectado por código malicioso)
- Sitio de falso positivo
- Archivo de falso positivo (archivo que se detecta como amenaza pero no está infectado)
- Otros

**Archivo/Sitio**: la ruta del archivo o sitio web que quiere enviar.

**Correo electrónico de contacto**: esta dirección de correo electrónico de contacto se envía a ESET junto con los archivos sospechosos y se puede utilizar para contactar con usted en caso de que sea necesaria más información para poder realizar el análisis. Introducir una dirección de correo electrónico de contacto es opcional. Seleccione **Enviar de forma anónima** para dejar el campo vacío.

> **Puede que no reciba ninguna respuesta de ESET.**
> No obtendrá ninguna respuesta de ESET a menos que sea necesario que envíe información adicional. Cada día, nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.
> Si la muestra resulta ser una aplicación o un sitio web maliciosos, su detección se agregará a una actualización futura de ESET.

# Seleccionar muestra para el análisis: archivo sospechoso

**Signos y síntomas observados de la infección por código malicioso**: describa el comportamiento del archivo sospechoso que ha observado en el ordenador.

**Origen del archivo (dirección URL o proveedor)**: escriba el origen (fuente) del archivo y cómo llego a él.

**Notas e información adicional**: aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

> El primer parámetro (**Signos y síntomas observados de la infección por código malicioso**) es necesario; la información adicional que proporcione será de gran utilidad para nuestros laboratorios en los procesos de identificación y procesamiento de muestras.

# Seleccionar muestra para el análisis: sitio sospechoso

Seleccione una de las opciones siguientes en el menú desplegable **Problema del sitio**:

- **Infectado**: sitio web que contiene virus u otro código malicioso distribuido por diversos métodos.
- **Phishing** – su objetivo es acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, PIN, etc. Puede obtener más información sobre este tipo de ataque en el glosario.
- **Fraude**: sitio web fraudulento o con información falsa, destinado sobre todo a obtener un beneficio

rápido.

- Seleccione **Otros** si las opciones anteriores no hacen referencia al sitio que va a enviar.

**Notas e información adicional**: puede escribir más información o una descripción que ayude a analizar el sitio web sospechoso.

# Seleccionar muestra para el análisis: archivo de falso positivo

Le rogamos que nos envíe los archivos que se detectan como amenazas pero no están infectados, para mejorar nuestro motor de antivirus y antiespía y ayudar a proteger a otras personas. Los falsos positivos (FP) se generan cuando el patrón de un archivo coincide con un mismo patrón disponible en un motor de detección.

**Nombre y versión de la aplicación**: título y versión del programa (por ejemplo, número, alias o nombre en código).

**Origen del archivo (dirección URL o proveedor)**: escriba el origen (fuente) del archivo y cómo llego a él.

**Objetivo de la aplicación**: descripción general de la aplicación, tipo de aplicación (por ejemplo, navegador, reproductor multimedia, etc.) y su funcionalidad.

**Notas e información adicional**: aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

> Los tres primeros parámetros son necesarios para identificar las aplicaciones legítimas y distinguirlas del código malicioso. La información adicional que proporcione será de gran ayuda para los procesos de identificación y procesamiento de muestras en nuestros laboratorios.

# Seleccionar muestra para el análisis: sitio de falso positivo

Le solicitamos que nos envíe los sitios que se detectan como amenazas, fraudes o phishing, pero no lo son. Los falsos positivos (FP) se generan cuando el patrón de un archivo coincide con un mismo patrón disponible en un motor de detección. Proporcione este sitio web para mejorar nuestro motor de antivirus y anti-phishing y ayudar a proteger a otras personas.

**Notas e información adicional**: aquí puede especificar más información o una descripción que ayude a procesar el sitio web sospechoso.

# Seleccionar muestra para el análisis: otros

Utilice este formulario si el archivo no se puede categorizar como un **Archivo sospechoso** o un **Falso positivo**.

**Motivo de envío del archivo**: introduzca una descripción detallada y el motivo por el que envía el archivo.

# Configuración

Puede ver grupos de funciones de protección disponibles en la ventana principal del programa > **Configuración**.


El menú **Configuración** se divide en las siguientes secciones:

Protección del ordenador

Protección de Internet

Protección de la red

Herramientas de seguridad

En la parte inferior de la ventana de configuración encontrará opciones adicionales disponibles. Haga clic en Configuración avanzada para configurar más parámetros detallados de cada módulo. Para cargar los parámetros de configuración con un archivo de configuración .xml, o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción Importar/exportar configuración.

# Protección del ordenador

Haga clic en **Protección del ordenador** en la ventana principal del programa > **Configuración** para ver una descripción general de todos los módulos de protección:

- Protección del sistema de archivos en tiempo real: se analizan todos los archivos en busca de código malicioso cuando se abren, crean o ejecutan.

- ESET LiveGuard: agrega una capa de protección basada en la nube diseñada específicamente para mitigar las amenazas desconocidas.

  - **Protección proactiva**: bloquea la ejecución de nuevos archivos hasta que se recibe el resultado del análisis de ESET LiveGuard. Si desea desbloquear el archivo que se está analizando, haga clic con el botón derecho en el archivo y haga clic en **Desbloquear archivo analizado por ESET LiveGuard**.

- Control de dispositivos: este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como seleccionar el modo de acceso y uso de un usuario en un dispositivo dado (CD/DVD/USB...).

- HIPS: el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.

- Modo de presentación: habilita o deshabilita el modo de presentación. Cuando se active el modo de presentación, recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal se volverá naranja.

- Protección de la cámara web: controla los procesos y las aplicaciones que acceden a la cámara web.

Para pausar o desactivar módulos de protección específicos, haga clic en el icono .

⚠ Desactivar los módulos de protección puede disminuir el nivel de protección del ordenador.

Haga clic en el icono del engranaje ubicado junto a un módulo de protección para acceder a la configuración avanzada de ese módulo.

Para la **protección del sistema de archivos en tiempo real**, haga clic en el icono del engranaje y elija una de las siguientes opciones:

- **Configurar**: abre la configuración avanzada de la Protección del sistema de archivos en tiempo real.

- **Editar exclusiones**: abre la ventana de configuración de exclusiones para que pueda excluir archivos y carpetas del análisis.

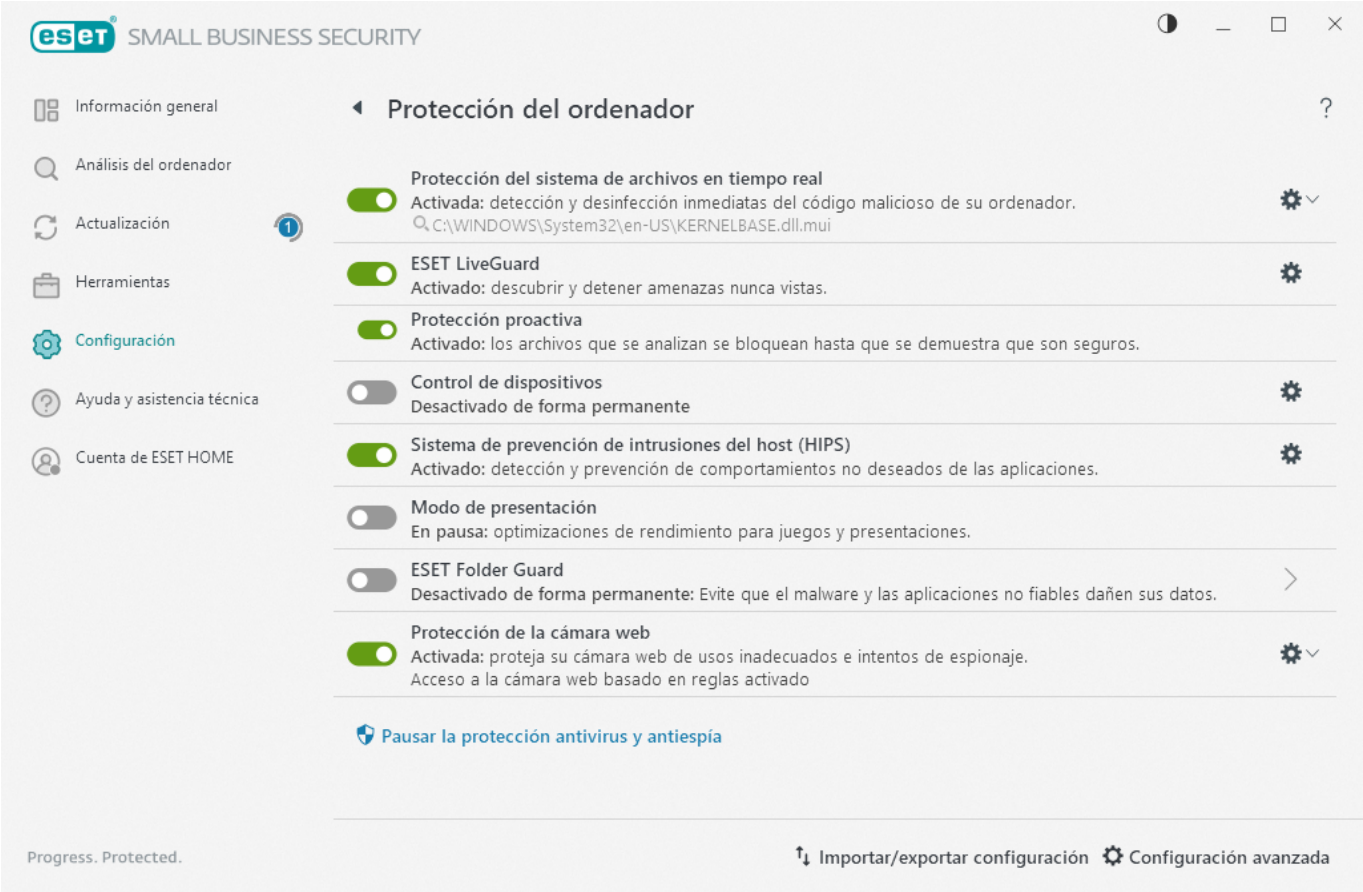
Para la **protección de la cámara web**, haga clic en el icono del engranaje y elija una de las siguientes opciones:

- **Configurar**: abre la configuración avanzada de la Protección de la cámara web.

- **Bloquear todos los accesos hasta reiniciar**: bloquea todos los accesos a la cámara web hasta que se reinicia el ordenador.

- **Bloquear todos los accesos permanentemente**: bloquea todos los accesos a la cámara web hasta que se desactiva este ajuste.

- **Detener el bloqueo de todos los accesos**: desactiva la posibilidad de bloquear el acceso a la cámara web. Esta opción solo está disponible cuando está bloqueado el acceso a la cámara web.




**Pausar la protección antivirus y antiespía**: desactiva todos los módulos de protección antivirus y antiespía. Cuando desactiva la protección, se abre una ventana para determinar durante cuánto tiempo se desactivará la protección usando el menú desplegable **Intervalo de tiempo**. Utilice esta opción solo si es un usuario experimentado o si se lo indica el soporte técnico de ESET.

# Detección de una amenaza

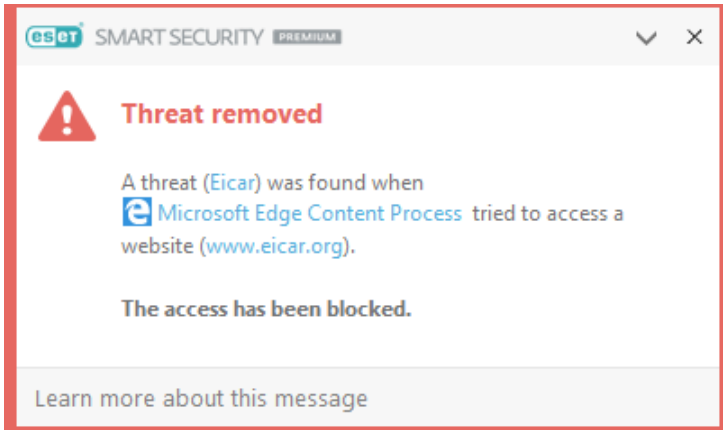
Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, etc.).

## Comportamiento estándar

ESET Small Business Security detecta infiltraciones mediante:

- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección de clientes de correo electrónico
- Análisis del ordenador a petición

Cada uno de estos componentes utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Se muestra una ventana de notificación en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para obtener más información sobre los objetos detectados o desinfectados, consulte Archivos de registro. Para obtener más información sobre los niveles de desinfección y el comportamiento, consulte Niveles de desinfección.




## Análisis del ordenador en busca de archivos infectados

Si el ordenador muestra señales de infección por código malicioso — por ejemplo, se ralentiza, se bloquea con frecuencia, etc., le recomendamos que haga lo siguiente:

1.Abra ESET Small Business Security y haga clic en **Análisis del ordenador**.

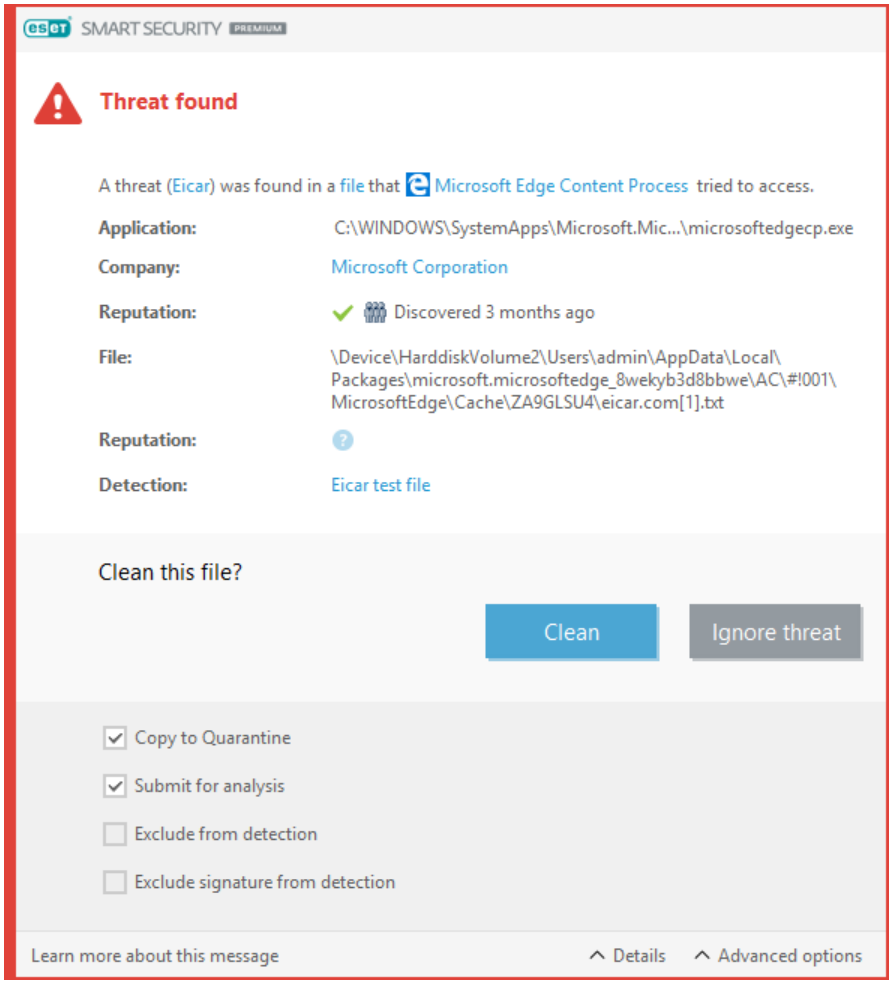
2.Haga clic en **Análisis del ordenador** (para obtener más información, consulte Análisis del ordenador).

3.Tras el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

Si desea analizar una parte específica del disco, haga clic en **Análisis personalizado** y seleccione los objetos que desea incluir en el análisis de virus.

## Desinfección y eliminación

Si no hay que realizar ninguna acción predefinida para la protección del sistema de archivos en tiempo real, la ventana de alerta le pedirá que seleccione una opción. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados quedarían intactos. La única excepción es cuando está seguro de que el archivo es inofensivo y se ha detectado por error.




Proceda a desinfectar si un virus ha adjuntado código malicioso a un archivo. Si es así, primero intente desinfectar el archivo infectado para restaurarlo. Si el archivo es completamente código malicioso, se eliminará.

Si un proceso del sistema bloquea o está utilizando un archivo infectado, por lo general solo se eliminará cuando se haya publicado (normalmente, tras reiniciar el sistema).

## Restauración de archivos de cuarentena

Puede acceder a la cuarentena en la ventana principal de ESET Small Business Security. Para ello, haga clic en **Herramientas** > **Cuarentena**.

Los archivos en cuarentena también pueden restaurarse en su ubicación original:

- Utilice la función **Restaurar** para tal fin, disponible desde el menú contextual si hace clic con el botón derecho en un archivo determinado en cuarentena.

- Si un archivo se marca como aplicación potencialmente indeseable, la opción **Restaurar y excluir** se activa. Consulte también Exclusiones.

- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar archivos en una ubicación distinta de la cual se eliminaron.

- La función de restauración no está disponible en algunos casos, por ejemplo, para los archivos que se encuentran en un recurso compartido de red de solo lectura.

## Múltiples amenazas

Si durante un análisis del ordenador no se desinfectaron algunos archivos infectados (o el Nivel de desinfección se estableció en **Sin desinfección**), aparecerá una ventana de alerta solicitándole que seleccione las acciones que desea llevar a cabo en esos archivos. Seleccione las acciones para los archivos (las acciones se establecen individualmente para cada archivo de la lista) y, a continuación, haga clic en **Finalizar**.

## Eliminación de amenazas en archivos comprimidos

En el modo de desinfección predeterminado, solo se eliminará todo el archivo comprimido si todos los archivos que contiene están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos no infectados e inofensivos. Tenga cuidado al realizar un análisis de desinfección estricta. Cuando esté activada la desinfección estricta, un archivo se eliminará si contiene al menos un archivo infectado, sin tener en cuenta el estado de los otros archivos.

# ESET Folder Guard

ESET Folder Guard mejora la seguridad de archivos y datos. Evita que el malware y las aplicaciones que no son de confianza accedan a las carpetas protegidas. Se pueden realizar las siguientes acciones:

- Agregar nueva carpeta
- Eliminar carpeta
- Administrar reglas de aplicaciones

## Agregar nueva carpeta

Puede agregar una nueva carpeta a las carpetas protegidas a través del menú contextual o directamente desde su producto ESET según sus preferencias.

Agregue solo carpetas (no archivos) a la lista de carpetas protegidas.

### Agregar una carpeta a las carpetas protegidas a través del menú contextual

1. Seleccione una o varias carpetas en su dispositivo Windows.
2. Haga clic con el botón derecho y seleccione **Opciones avanzadas** (para Windows 10) o **ESET Small Business Security** (para Windows 11) > **Proteger con ESET Folder Guard**.

Recibirá una notificación de confirmación después de agregar las carpetas a ESET Folder Guard. En la notificación, haga clic en **Ver carpeta** para que se muestren como elementos resaltados las carpetas recién agregadas con las rutas de la carpeta en la pantalla de ESET Folder Guard.

### Agregue una carpeta a las carpetas protegidas a través del producto ESET

1. Abra la ventana principal del programa > **Configuración** > **Protección del ordenador** > **ESET Folder Guard**.
2. Haga clic en el icono de interruptor junto a **ESET Folder Guard** para activar la función.

3. Haga clic en el elemento de ESET Folder Guard para abrir la pantalla de ESET Folder Guard.

4. Haga clic en el botón **Agregar nueva carpeta**.

5. Elija la carpeta específica de la estructura de árbol y haga clic en **Agregar carpeta**.

Las unidades completas, las unidades extraíbles y las carpetas específicas (C:\Windows\SysWOW64, C:\Windows\System32, C:\Archivos de programa (x86), C:\Archivos de programa) no son adecuadas para la protección de ESET Folder Guard.

## Eliminar carpeta

Para eliminar la carpeta de la lista de carpetas protegidas, siga estas instrucciones:

1. Abra la ventana principal del programa > **Configuración** > **Protección del ordenador** > **ESET Folder Guard**.

2. Haga clic en el elemento de ESET Folder Guard para abrir la pantalla de ESET Folder Guard.

3. Seleccione la carpeta y haga clic en el botón **Eliminar carpeta**.

4. Para confirmar la pérdida de protección de la carpeta seleccionada, haga clic en **Eliminar**.

Desactivar la protección de las carpetas seleccionadas las volverá vulnerables a posibles amenazas y al acceso de aplicaciones que no son de confianza.

## Impacto de desactivar el HIPS en la función de ESET Folder Guard

ESET Folder Guard no está operativo

La alerta de seguridad aparece en la sección Información general cuando el Sistema de prevención de intrusiones del host (HIPS) está desactivado. La protección de carpetas contra accesos no autorizados no funciona. Desactivar el HIPS puede hacer que su dispositivo sea vulnerable a varios tipos de amenazas. En esta alerta de seguridad, haga clic en **Activar HIPS** para garantizar su protección. Es necesario un reinicio del ordenador para que los cambios tengan efecto. Una vez que HIPS esté activado, puede habilitar la función de ESET Folder Guard.

# Permisos de la aplicación

La pantalla de permisos de la aplicación contiene una lista de aplicaciones individuales con las reglas establecidas para controlar su interacción con las carpetas protegidas por la función ESET Folder Guard. Las aplicaciones verificadas por ESET como seguras pueden acceder sin ningún paso adicional a las carpetas que usted protege. Si una aplicación ya se considera de confianza, se le permite el acceso automáticamente.

## Agregar una aplicación

1. Abra la ventana principal del programa > **Configuración** > **Protección del ordenador** > **ESET Folder Guard**.

2. Haga clic en **Gestionar permisos de la aplicación** en la parte inferior de la pantalla. Se abrirá la pantalla de permisos de la aplicación.

3. Haga clic en **Agregar**.

4. Establezca el permiso de acceso que se menciona a continuación y haga clic en **Aceptar**.

## Gestionar permisos de la aplicación

Puede definir los siguientes permisos de acceso para las aplicaciones especificadas:

- **Permitir acceso**: permite el acceso de una aplicación específica a la carpeta protegida.
- **Bloquear acceso**: bloquea el acceso de una aplicación específica a la carpeta protegida.
- **Preguntar cada vez**: el producto de ESET pide permiso cada vez para permitir o bloquear el acceso de la aplicación a la carpeta protegida.

Puede cambiar una regla existente para la aplicación en cualquier momento si elige otra opción en el menú desplegable y la confirma con el botón **Aceptar** en la parte inferior de la pantalla Permisos de la aplicación.

Si establece los permisos en **Permitir acceso** y **Bloquear acceso**, también tiene la opción de recibir una notificación cuando la aplicación que no es de confianza intente modificar archivos en la carpeta protegida. Marque la casilla **Notificar intento de acceso** para que la aplicación reciba una notificación.

Los permisos de acceso a la aplicación también se pueden establecer desde la ventana de alerta que se muestra a continuación cuando la aplicación que no es de confianza intenta acceder a una carpeta protegida. Los permisos creados desde la ventana de alerta se consideran equivalentes a los permisos creados manualmente. Puede acceder a los ajustes de los parámetros de permisos más detallados haciendo clic en **Opciones avanzadas**.

## Eliminar una aplicación

Para eliminar las aplicaciones específicas de la lista, siga las instrucciones a continuación:

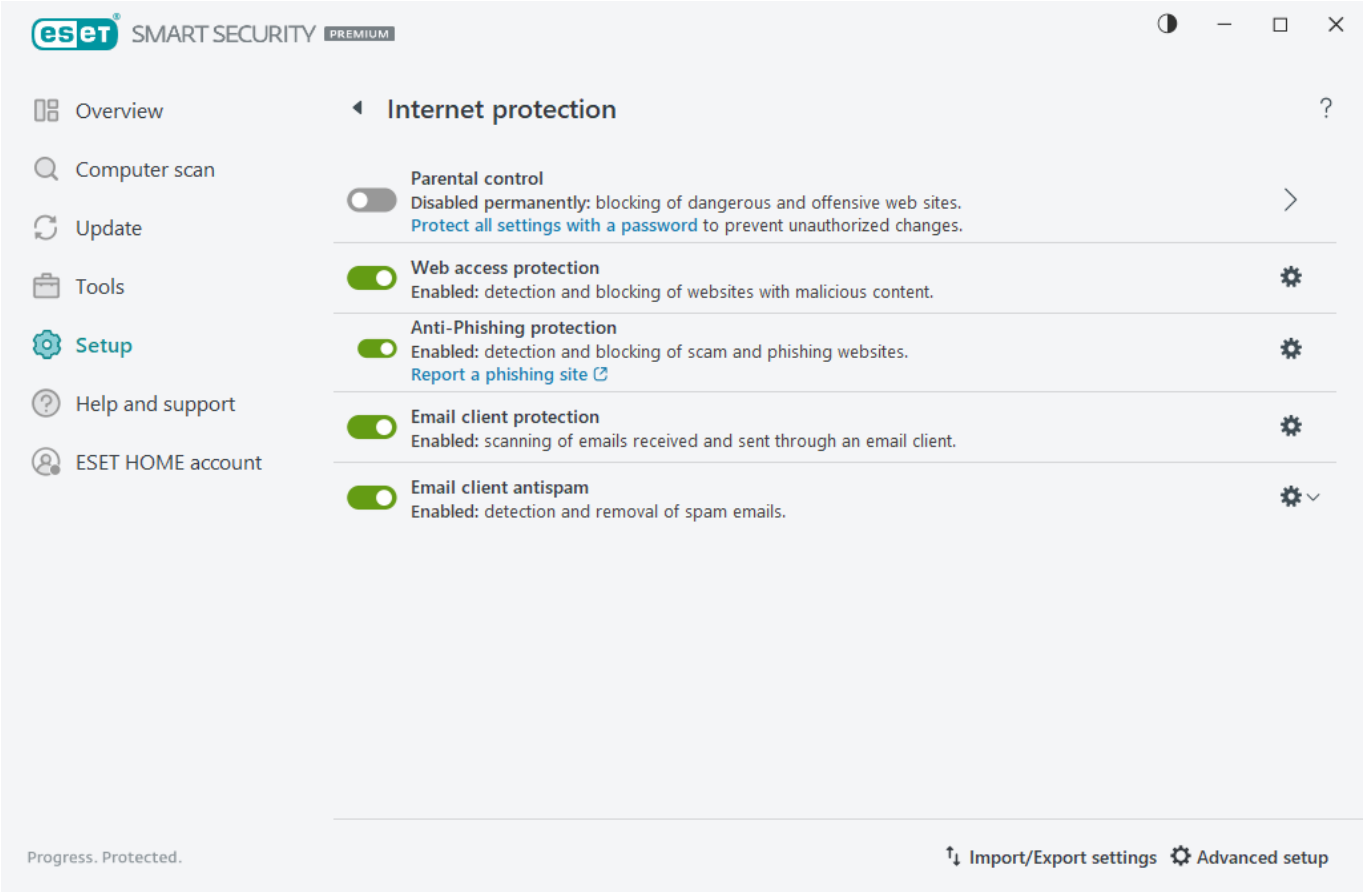
1. Abra la ventana principal del programa > **Configuración** > **Protección del ordenador** > **ESET Folder Guard**.
2. Haga clic en **Gestionar permisos de la aplicación** en la parte inferior de la pantalla. Se abrirá la pantalla de permisos de la aplicación.
3. Seleccione las aplicaciones específicas > **Eliminar**.
4. Haga clic en **Aceptar** para confirmar.

# Protección de Internet

La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. Abra la ventana principal del programa > **Configuración** > **Protección de Internet** para configurar las funciones de ESET Small Business Security que aumentan la protección de Internet.

Para pausar o desactivar módulos de protección específicos, haga clic en el icono  .

⚠ Desactivar los módulos de protección puede disminuir el nivel de protección del ordenador.




Haga clic en el icono del engranaje ubicado junto a un módulo de protección para acceder a la configuración avanzada de ese módulo.

Protección de acceso a la web analiza la comunicación HTTP/HTTPS en busca de malware y phishing. Protección de acceso a la web solo debe desactivarse para solucionar problemas.

Protección antiphishing le permite bloquear páginas web conocidas por distribuir contenido de phishing. Le recomendamos encarecidamente que deje Anti-Phishing activado.

**Informar sobre una página de phishing**: envía un informe sobre un sitio web malicioso o de phishing a ESET para su análisis.

Antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:
- El sitio web no se detecta en absoluto.
- El sitio web se detecta como una amenaza, pero no lo es. En este caso, puede Informar de página bloqueada incorrectamente.

La opción Protección del cliente de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S). Con el programa de complemento para su cliente de correo electrónico, ESET Small Business Security ofrece control de todas las comunicaciones realizadas desde el cliente de correo electrónico.

Antispam del cliente de correo electrónico filtra los mensajes de correo electrónico no solicitados.

Para el **Antispam del cliente de correo electrónico**, haga clic en el icono del engranaje y elija una de las siguientes opciones:

- **Configurar**: abre la ventana de configuración avanzada para Antispam del cliente de correo electrónico.

• **Lista de direcciones del usuario**: abre un cuadro de diálogo donde puede agregar, modificar o eliminar direcciones para definir las reglas antispam. Las reglas de esta lista se aplicarán al usuario actual.

• **Lista de direcciones global**: abre un cuadro de diálogo donde puede agregar, modificar o eliminar direcciones para definir las reglas antispam. Las reglas de esta lista se aplicarán a todos los usuarios.

# Protección Anti-Phishing

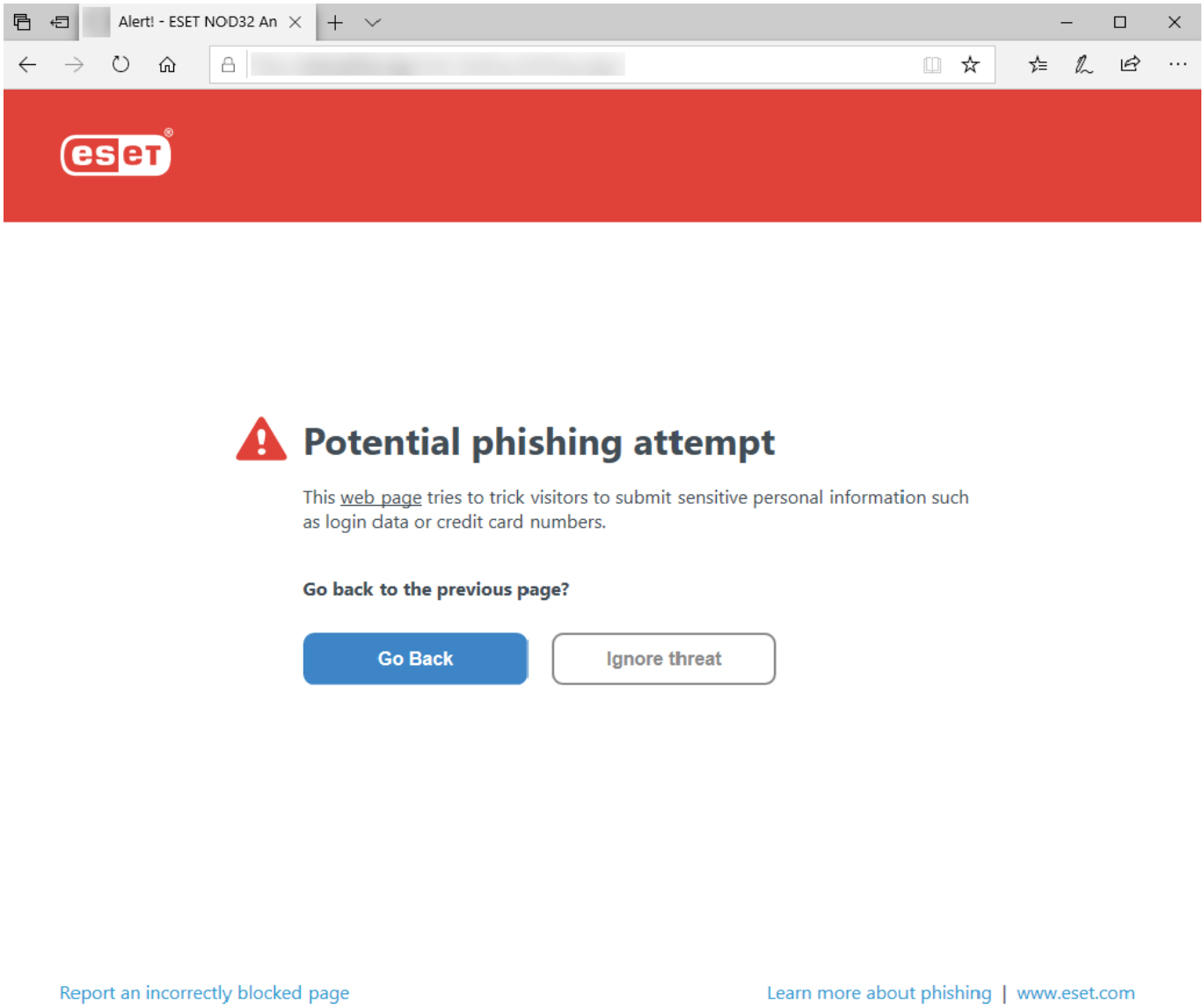
El phishing es una actividad delictiva en la que se aplica ingeniería social, es decir, se manipula al usuario para obtener información confidencial. El phishing se utiliza para acceder a datos confidenciales, como números de cuentas bancarias, PIN, etc. Para obtener más información, consulte el glosario. ESET Small Business Security incluye protección anti-phishing, que bloquea las páginas web conocidas por distribuir este tipo de contenido.

La protección antiphishing está activada de forma predeterminada. Esta opción se puede configurar en Configuración avanzada > **Protecciones** > **Protección de acceso a la web**.

Visite nuestro artículo de la base de conocimiento para obtener más información sobre la protección Anti-Phishing de ESET Small Business Security.

## Acceso a un sitio web de phishing

Al acceder a un sitio web de phishing reconocido, su navegador web mostrará el siguiente cuadro de diálogo. Si aun así quiere acceder al sitio web, haga clic en **Ignorar amenaza** (no recomendado).




Los posibles sitios de phishing que se han incluido en la lista blanca expirarán de forma predeterminada después de unas horas. Para permitir un sitio web permanentemente, use la herramienta Gestión de direcciones URL. En Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Gestión de direcciones URL** > **Lista de direcciones** > **Modificar** agregue a la lista el sitio web que desee modificar.

## Informar sobre una página de phishing

El vínculo **Informar de una página bloqueada incorrectamente** le permite informar de un sitio web que se detecta incorrectamente como una amenaza.

También puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el sitio web (por ejemplo, el sitio web que le refirió a este, cómo tuvo constancia de su existencia, etc.).

# Protección de la red

Abra la ventana principal del programa **Configuración** > **Protección de la red** > para configurar las opciones básicas de protección de red o solucionar problemas de comunicación de red.

Para pausar o desactivar módulos de protección específicos, haga clic en el icono .

⚠ Desactivar los módulos de protección puede disminuir el nivel de protección del ordenador.


Haga clic en el icono del engranaje ubicado junto a un módulo de protección para acceder a la configuración avanzada de ese módulo.

**Cortafuegos**: filtra toda la comunicación de red según la configuración de ESET Small Business Security.

**Configurar**: abre la Configuración avanzada de cortafuegos, donde puede definir el modo en que el cortafuegos gestionará la comunicación de red.

**Pausar cortafuegos (permitir todo el tráfico)**: todas las opciones de filtrado del cortafuegos se desactivan y se permiten todas las conexiones entrantes y salientes. Haga clic en **Activar el cortafuegos** para activar el cortafuegos de nuevo cuando el Filtrado del tráfico de red se encuentre en este modo.

**Bloquear todo el tráfico**: el cortafuegos bloqueará todas las comunicaciones entrantes y salientes. Utilice esta opción únicamente si considera que existen riesgos de seguridad importantes que requieran la desconexión del sistema de la red. Cuando la opción Filtrado del tráfico de red esté definida en el modo **Bloquear todo el tráfico**, haga clic en **Detener el bloqueo de todo el tráfico** para restablecer el funcionamiento normal del cortafuegos.

**Modo automático** (cuando está activado otro modo de filtrado): haga clic aquí para cambiar el modo de filtrado a automático (con reglas definidas por el usuario).

**Modo interactivo** (cuando está activado otro modo de filtrado): haga clic aquí para cambiar el modo de filtrado a interactivo.

Protección contra los ataques de red (IDS): analiza el contenido del tráfico de red y protege frente a ataques de

red. El tráfico considerado perjudicial se bloqueará. ESET Small Business Security le informará cuando se conecte a una red inalámbrica sin protección o a una red con una protección débil.

**Protección contra botnets**: detecta código malicioso en el sistema de forma rápida y precisa.

Conexiones de red: muestra las redes a las que están conectados los adaptadores de red con información detallada.

**Resolver la comunicación bloqueada**: le ayuda a solucionar los problemas de conectividad provocados por el cortafuegos de ESET. Encontrará más información detallada en Asistente de solución de problemas.

**Resolver direcciones IP bloqueadas temporalmente**: ver una lista de direcciones IP que se han detectado como fuente de los ataques y se han agregado a la lista negra para bloquear la conexión durante un período de tiempo concreto.

**Mostrar registros**: abre el archivo de registro de Protección de la red.

# Conexiones de red

Muestra las redes a las que están conectados los adaptadores de red. Para ver las conexiones de red, abra la ventana principal del programa > **Configuración** > **Protección de la red** > **Conexiones de red**.

Haga doble clic en una conexión de la lista para mostrar sus detalles y los detalles del adaptador de red.

Coloque el cursor del ratón sobre una conexión de red específica y haga clic en el icono de menú ⋮ de la columna **De confianza** para elegir una de las siguientes opciones:

- **Editar**: abre la ventana Configurar protección de la red, donde puede asignar un perfil de protección de la red a una red específica.
- **Olvidar**: restablece la configuración de la conexión de red a los valores predeterminados.
- **Analizar la red con Inspector de red**: abre el Inspector de red para ejecutar un análisis de red
- **Marcar como "Mi red"**: agrega una etiqueta "Mi red" a la red. Esta etiqueta se mostrará junto a la red en todas las secciones de ESET Small Business Security para mejorar la identificación y la visión general de seguridad.
- **Desmarcar como "Mi red"**: quita la etiqueta "Mi red"; esta opción solo disponible si la red ya está etiquetada.

# Detalles de la conexión de red

Haga doble clic en una conexión de la lista de Conexiones de red para mostrar los detalles junto con los detalles del adaptador de red. La conexión de red y los detalles del adaptador pueden ayudarle a identificar la red que está intentando configurar en Protección de acceso a la red.

Detalles de la conexión de red:

- Estado de la conexión de red

- Fecha y hora de la primera detección de la red
- Última hora a la que la red estuvo activa
- Tiempo total de conexión a esta red
- Perfil de conexión de la red
- Perfil de conexión de red definido en Windows
- Configuración de protección de la red (si la red es de confianza)

Detalles del adaptador de red:

- Tipo de conexión (cableada, virtual, etc.)
- Nombre del adaptador de red
- Descripción del adaptador
- Dirección IP con dirección MAC
- La dirección IPv4 e IPv6 de la red con subred
- Sufijo de DNS
- IP del servidor DNS
- IP del servidor DHCP
- IP y dirección MAC de la puerta de enlace predeterminada
- Dirección MAC del adaptador

# Resolución de problemas de acceso a la red

El asistente de solución de problemas le ayuda a solucionar los problemas de conectividad provocados por el cortafuegos. **Resolución de problemas de acceso a la red** está disponible en la ventana principal del programa > **Configuración** > **Protección de la red** > **Resolver la comunicación bloqueada**.

Seleccione si desea mostrar la comunicación bloqueada para **Aplicaciones locales** o la comunicación bloqueada desde **Dispositivos remotos**.

En el menú desplegable, seleccione un período de tiempo durante el que se haya bloqueado la comunicación. Una lista de comunicaciones bloqueadas recientemente ofrece una descripción general sobre el tipo de aplicación o dispositivo, la reputación y el número total de aplicaciones y dispositivos bloqueados durante ese período de tiempo. Para obtener más información sobre la comunicación bloqueada, haga clic en **Detalles**. El siguiente paso es desbloquear la aplicación o dispositivo en el que experimente problemas de conectividad.

Tras hacer clic en **Desbloquear**, se permitirá la comunicación bloqueada anteriormente. Si sigue experimentando problemas con una aplicación o el dispositivo no funciona según lo esperado, haga clic en **crear otra regla** para permitir todas las comunicaciones bloqueadas anteriormente para ese dispositivo. Reinicie el ordenador si el

problema persiste.

Haga clic en **Abrir reglas de cortafuegos** para ver las reglas creadas por el asistente. También puede ver las reglas creadas por el asistente en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Cortafuegos** > **Reglas** > **Editar**.

Si no se puede crear la regla, recibirá un mensaje de error. Haga clic en **Volver a intentarlo** y repita el proceso para desbloquear la comunicación o cree otra regla desde la lista de comunicaciones bloqueadas.

# Lista negra de direcciones IP temporales

Para ver las direcciones IP detectadas como fuentes de ataques y agregadas a la lista negra para bloquear la conexión durante un periodo de tiempo concreto, abra la ventana principal del programa > **Configuración** > **Protección de la red** > **Lista negra temporal de direcciones IP**. Las direcciones IP bloqueadas temporalmente se bloquean durante 1 hora.

## Columnas

**Dirección IP**: muestra una dirección IP que se ha bloqueado.

**Motivo del bloqueo**: muestra el tipo de ataque que se ha evitado desde la dirección (por ejemplo, ataque de exploración de puerto TCP).

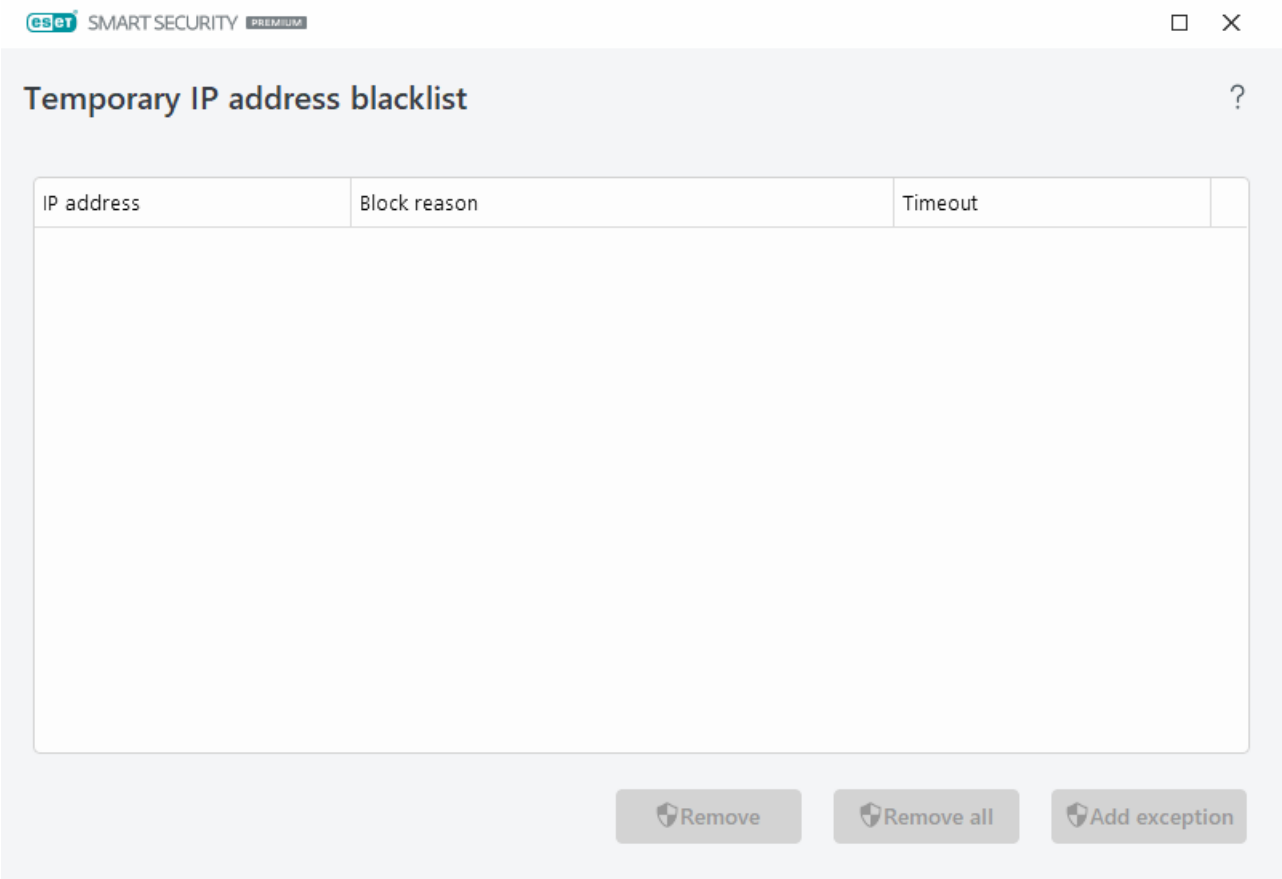
**Tiempo de espera**: muestra la fecha y la hora a la que la dirección se eliminará de la lista negra.

## Elementos de control

**Quitar**: haga clic en esta opción para eliminar una dirección de la lista negra antes de que expire.

**Quitar todo**: haga clic en esta opción para eliminar todas las direcciones de la lista negra de inmediato.

**Agregar excepción**: haga clic en esta opción para agregar una excepción del cortafuegos en el filtrado de IDS.




# Registros de protección de la red

La protección de la red de ESET Small Business Security guarda todos los sucesos importantes en un archivo de registro. Para ver el archivo de registro, abra la ventana principal del programa > **Configuración** > **Protección de la red** > **Mostrar registros**.

Los archivos de registro sirven para la detección de errores e intrusiones en el sistema. Los registros de protección de la red contienen los datos siguientes:

- Fecha y hora del suceso.
- Nombre del suceso
- Fuente
- Dirección de la red de destino
- Protocolo de comunicación de red
- Regla aplicada o nombre del gusano (si se identifica)
- Ruta de acceso y nombre de la aplicación
- Hash
- Usuario
- Firmante de la aplicación (editor)

- Nombre del paquete
- Nombre del servicio

Un análisis exhaustivo de estos datos puede ayudarle a detectar los intentos de poner en peligro la seguridad del sistema. Existen otros muchos factores que indican posibles riesgos de seguridad y le permiten minimizar el impacto: conexiones frecuentes desde ubicaciones desconocidas, intentos repetidos de establecer conexiones, comunicación de aplicaciones desconocidas o utilización de números de puertos poco comunes.

> **Explotación de vulnerabilidades de seguridad**
> El mensaje de explotación de vulnerabilidades de seguridad se registra incluso si la vulnerabilidad concreta se ha revisado desde que se ha detectado y bloqueado el intento de explotación en el nivel de red antes de que se produzca la explotación propiamente dicha.

# Solución de problemas con el cortafuegos

Si tiene problemas de conectividad cuando ESET Small Business Security está instalado, tiene a su disposición varias maneras de comprobar si el cortafuegos es la causa del problema. Además, el cortafuegos puede ayudarle a crear reglas o excepciones nuevas para solucionar los problemas de conectividad.

Consulte los temas siguientes para obtener ayuda a la hora de solucionar problemas con el cortafuegos:

- Resolución de problemas de acceso a la red
- Registro y creación de reglas o excepciones del registro
- Creación de excepciones a partir de notificaciones del cortafuegos
- Registro avanzado de la protección de la red
- Resolución de problemas con el análisis de tráfico de red

# Registro y creación de reglas o excepciones del registro

De forma predeterminada, el cortafuegos de ESET no registra todas las conexiones bloqueadas. Si desea ver qué estaba bloqueado por la protección de la red, abra Configuración avanzada > **Herramientas** > **Diagnóstico** > **Registro avanzado** y active **Activar registro avanzado de la protección de red**. Si ve en el registro algo que no desea que el cortafuegos bloquee, puede crear una regla o una regla de IDS haciendo clic con el botón derecho del ratón en dicho elemento y seleccionando **No bloquear sucesos similares en el futuro**. Tenga en cuenta que el registro de todas las conexiones bloqueadas puede contener miles de elementos, por lo que puede resultar complicado encontrar una conexión específica en este registro. Una vez que haya resuelto el problema, puede desactivar el registro.

Para obtener más información sobre el registro, consulte Archivos de registro.

> Utilice el registro para ver el orden en que el Protección de la red bloqueó las conexiones. Además, la creación de reglas a partir del registro le permite crear reglas que hagan exactamente lo que usted desee.

# Crear una regla desde un registro

La nueva versión de ESET Small Business Security le permite crear una regla desde el registro. En el menú principal, haga clic en **Herramientas** > **Archivos de registro**. Seleccione **Protección de la red** en el menú desplegable, haga clic con el botón derecho en la entrada del registro que desee y seleccione **No bloquear sucesos similares en el futuro** en el menú contextual. Se abrirá una ventana de notificación con la nueva regla.

Si desea permitir la creación de reglas nuevas a partir del registro, configure ESET Small Business Security con los ajustes siguientes:

1. Defina el nivel mínimo de detalle al registrar en **Diagnóstico**, en Configuración avanzada > **Herramientas** > **Archivos de registro**.

2. Active **Notificar ataques entrantes contra vulnerabilidades de seguridad** en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red (IDS)** > **Opciones avanzadas** > **Detección de intrusiones**.

# Creación de excepciones a partir de notificaciones del cortafuegos

Cuando el cortafuegos de ESET detecta actividad de red maliciosa, se muestra una ventana de notificación donde se describe el suceso. Esta notificación contiene un enlace con más información sobre el suceso y que le permite configurar una regla para dicho suceso, si desea hacerlo.

Si un dispositivo o una aplicación de red no implementa correctamente los estándares de red, puede desencadenar notificaciones de IDS del cortafuegos repetidas. Puede crear una excepción directamente desde la notificación para impedir que el cortafuegos de ESET detecte este dispositivo o esta aplicación.

Instrucciones con ilustraciones

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- Excluir una dirección IP del IDS en ESET Small Business Security

# Registro avanzado de la protección de la red

El objetivo de esta característica es proporcionar archivos de registro más complejos para el servicio de soporte técnico de ESET. Solo se debe utilizar cuando lo solicite el servicio de soporte técnico de ESET, ya que puede generar un archivo de registro muy grande y ralentizar su ordenador.

1. Vaya a Configuración avanzada > **Herramientas** > **Diagnóstico** > **Registro avanzado** y active **Activar registro avanzado de la protección de red**.

2. Intente repetir los pasos que provocaron el problema.

3. Desactive el registro avanzado de la protección de la red.

4. El archivo de registro PCAP creado por el registro avanzado de protección de la red está en el mismo directorio en el que se generan los volcados de memoria de diagnóstico: *C:\ProgramData\ESET\ESET*

*Security\Diagnostics*

# Resolución de problemas con el análisis de tráfico de red

Si tiene problemas con el navegador o cliente de correo electrónico, lo primero que debe hacer es comprobar si la causa es el análisis del tráfico de red. Para ello, desactive de forma temporal el análisis de tráfico de red en Configuración avanzada > **Análisis** > **Análisis del tráfico de red** (no olvide volver a activarlo cuando haya terminado, de lo contrario el navegador y el cliente de correo electrónico no estarán protegidos). Si el problema desaparece al desactivar el filtrado, consulte esta lista de problemas habituales y soluciones:

## Problemas de comunicación segura o actualización

Si su aplicación se queja porque no se puede actualizar o el canal de comunicación no es seguro:

- Si tiene activado SSL/TLS, desactívelo temporalmente. Si esto soluciona el problema, siga utilizando SSL/TLS y realice el trabajo de actualización excluyendo la comunicación problemática:
  Desactivar SSL/TLS. Vuelva a ejecutar la actualización. Debería aparecer un cuadro de diálogo para informarle sobre el tráfico de red cifrado. Asegúrese de que la aplicación coincide con la que tiene el problema y que el certificado procede del servidor desde el que se está actualizando. A continuación, seleccione la opción Recordar acción para este certificado y haga clic en Omitir. Si no se muestra ningún otro cuadro de diálogo, puede volver a poner el modo de filtrado en automático. El problema debería estar resuelto.

- Si la aplicación en cuestión no es un navegador o un cliente de correo electrónico, puede excluirla totalmente de la Protección de acceso a la web (si hace esto con un navegador o cliente de correo electrónico, quedaría muy expuesto). Todas las aplicaciones cuya comunicación se haya filtrado previamente deberían aparecer en la lista que se le proporcionó al agregar una excepción, por lo que no tendría que añadirlas de forma manual.

## Problemas de acceso a un dispositivo de la red

Si no puede utilizar alguna funcionalidad del dispositivo en la red (como abrir un página web de la cámara web o reproducir vídeo en un reproductor multimedia), agregue sus direcciones IPv4 y IPv6 a la lista de direcciones excluidas.

## Problemas con un sitio web determinado

Puede excluir sitios web específicos de la Protección de acceso a la web mediante la gestión de direcciones URL. Por ejemplo, si no puede acceder a https://www.gmail.com/intl/en/mail/help/about.html, inténtelo agregando *gmail.com* a la lista de direcciones excluidas.

## Error "Algunas de las aplicaciones capaces de importar el certificado raíz aun están en funcionamiento"

Cuando se activa SSL/TLS, ESET Small Business Security se asegura de que las aplicaciones instaladas confíen en su método de filtrado del protocolo SSL importando un certificado a su almacén de certificados. Algunas aplicaciones pueden requerir un reinicio para importar un certificado. Asegúrese de que no se está ejecutando ninguna de ellas (la mejor manera de hacerlo es abrir el Administrador de tareas y comprobar que no haya ninguna entrada

firefox.exe ni opera.exe en la ficha Procesos). A continuación, pulse Reintentar.

### Error de emisor no fiable o firma no válida

Lo más probable es que este error haga referencia al fallo de importación descrito anteriormente. Primero asegúrese de que no se está ejecutando ninguna de las aplicaciones mencionadas. A continuación, desactive SSL/TLS y vuelva a activarlo. El proceso de importación se volverá a ejecutar.

> Consulte el artículo de la base de conocimiento para obtener información sobre cómo administrar el análisis de tráfico de red en productos para oficina pequeña de ESET para Windows.

## Amenaza de red bloqueada

Esta situación puede darse cuando alguna de las aplicaciones del ordenador está intentando transmitir tráfico malicioso a otro dispositivo de la red, aprovechando una vulnerabilidad de seguridad, o incluso si se detecta un intento de análisis de puertos en su sistema.

En la notificación puede ver el tipo de amenaza y la dirección IP del dispositivo relacionado. Haga clic en **Cambiar la gestión de esta amenaza** para mostrar las siguientes opciones:

**Seguir bloqueando**: bloquea la amenaza detectada. Si desea dejar de recibir notificaciones de este tipo de amenaza desde la dirección remota concreta, marque el botón de opción situado junto a **No notificar** antes de hacer clic en **Seguir bloqueando**. De esta forma se creará una regla del Servicio de detección de intrusiones (IDS) con la siguiente configuración: **Bloquear**: predeterminado; **Notificar**: no; **Registrar**: no.

**Permitir**: crea una regla del Servicio de detección de intrusiones (IDS) para permitir la amenaza detectada. Seleccione una de las siguientes opciones antes de hacer clic en **Permitir** para especificar la configuración de la regla:

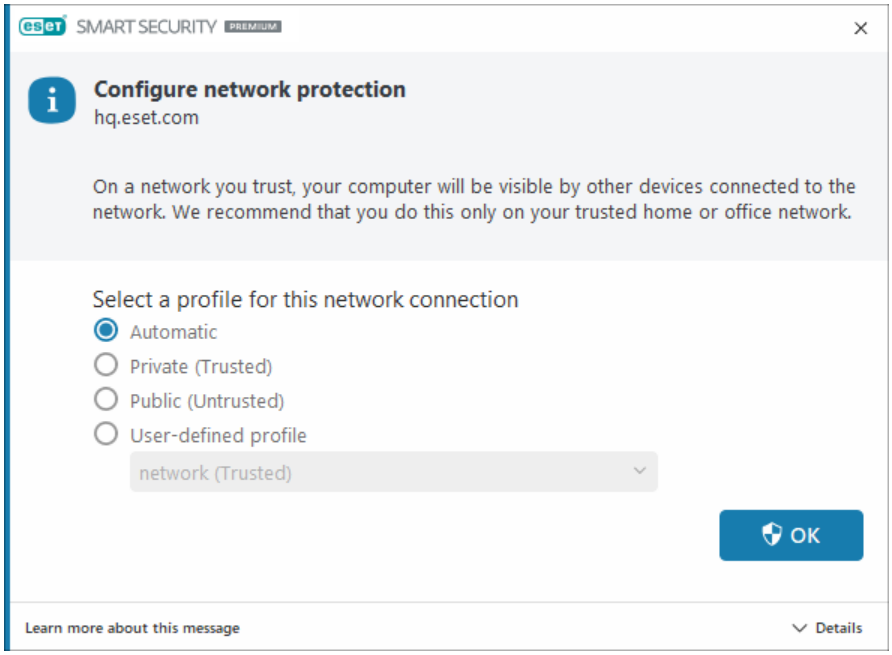
- **Avisar solo cuando se bloquee esta amenaza**—Configuración de la regla: **Bloquear**: no; **Notificar**: no; **Registrar**: no.
- **Avisar siempre que se produzca esta amenaza**—Configuración de la regla: **Bloquear**: no; **Notificar**: predeterminado; **Registrar**: predeterminado.
- **No avisar**—Configuración de la regla: **Bloquear**: no; **Notificar**: no; **Registrar**: no.

> La información que se muestra en esta ventana de notificación puede variar en función del tipo de amenaza detectado.
> Si desea obtener más información sobre amenazas y otros términos relacionados, consulte Tipos de ataques remotos o Tipos de amenazas detectadas.
> Para resolver los sucesos de **redes con direcciones IP duplicadas**, consulte el artículo de la base de conocimiento de ESET.

## Nueva red detectada

De forma predeterminada, ESET Small Business Security utiliza la configuración de Windows cuando se detecta una nueva conexión de red. Para mostrar una ventana de diálogo cuando se detecta una nueva red, cambie la Asignación del perfil de protección de la red a **Preguntar**. La configuración de la protección de la red se muestra

siempre que el ordenador se conecta a una red nueva.




Puede seleccionar entre los siguientes Perfiles de conexión de red:

**Automático**: ESET Small Business Security seleccionará el perfil automáticamente, en función de los Activadores configurados para cada perfil.

**Privado**: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible).

Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Pública**: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado.

Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

**Perfil definido por el usuario**: puede seleccionar uno de los perfiles que ha creado en el menú desplegable. Esta opción solo está disponible si ha creado al menos un perfil personalizado.

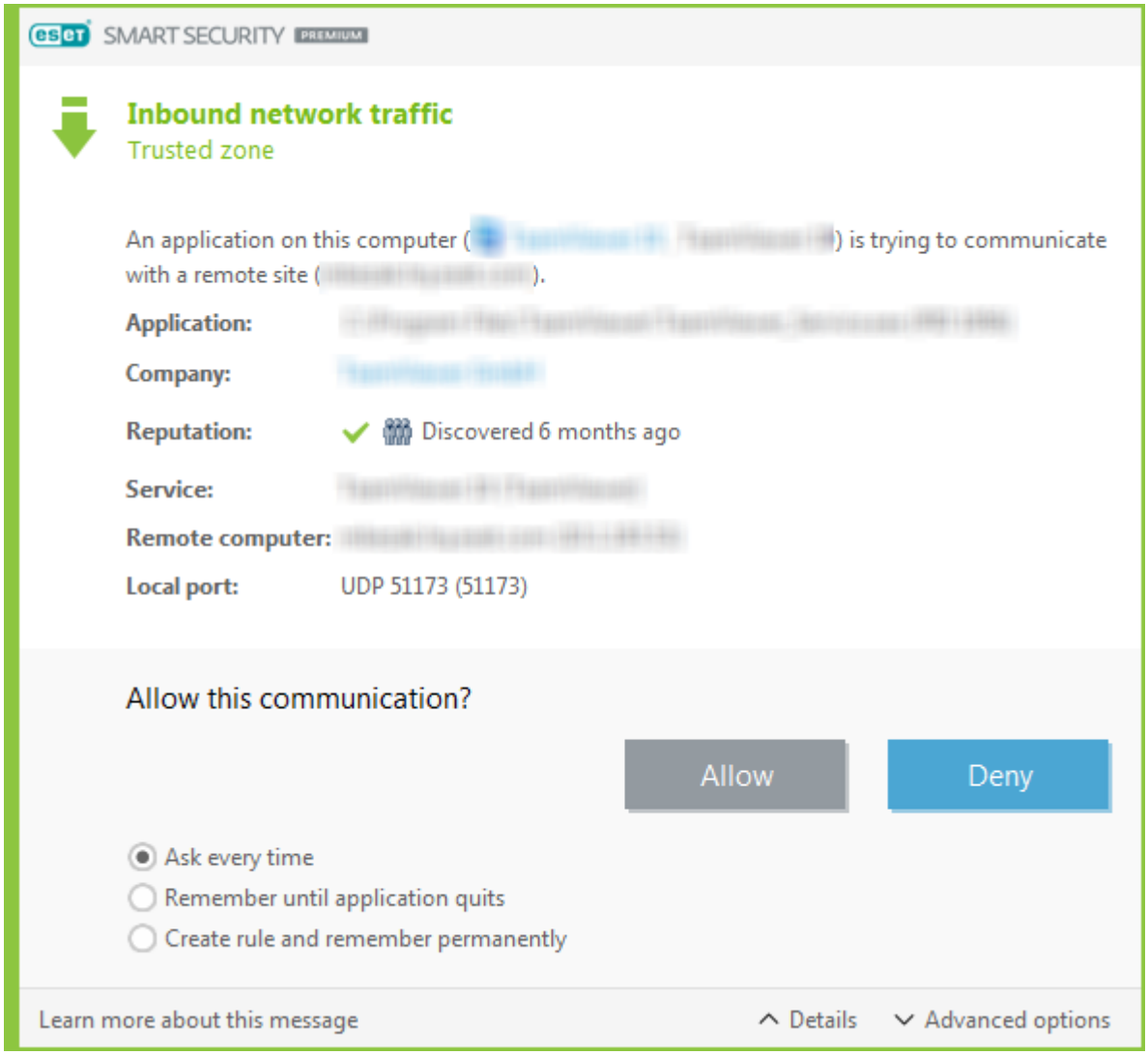
⚠ Una configuración de red incorrecta puede exponer su ordenador a riesgos para la seguridad.

# Establecimiento de una conexión: detección

El cortafuegos detecta cualquier conexión de red nueva. El modo del cortafuegos activo determina las acciones que se deben realizar para la nueva regla. Si el **Modo automático** o el **Modo basado en reglas** están activados, el cortafuegos realizará las acciones predefinidas sin la interacción del usuario.

El **modo interactivo** muestra una ventana informativa que notifica la detección de una nueva conexión de red, con información adicional acerca de dicha conexión. Puede optar por **Permitir** o **Denegar** (bloquear) la conexión. Si permite la misma conexión en el cuadro de diálogo en repetidas ocasiones, es aconsejable que cree una regla nueva para la conexión.

Seleccione **Crear regla y recordarla permanentemente** y guarde la acción como una regla nueva para el cortafuegos. Si el cortafuegos reconoce la misma conexión en el futuro, aplicará la regla existente sin necesidad de que intervenga el usuario.




Al crear reglas nuevas, permita únicamente conexiones que sepa que son seguras. Si permite todas las conexiones, el cortafuegos no podrá cumplir su finalidad. A continuación, se indican una serie de parámetros importantes para las conexiones:

**Aplicación**: ubicación del archivo ejecutable e ID del proceso. No permita conexiones de aplicaciones y procesos desconocidos.

**Firmante**: nombre del editor de la aplicación. Haga clic en el texto para mostrar un certificado de seguridad para la empresa.

**Reputación**: nivel de riesgo de la conexión. A las conexiones se les asigna un nivel de riesgo: Aceptable (verde), Desconocido (naranja) o Riesgo (rojo) mediante una serie de reglas heurísticas que examinan las características de cada conexión, el número de usuarios y la hora de detección. La tecnología ESET LiveGrid® se encarga de recopilar esta información.

**Servicio**: nombre del servicio, si la aplicación es un servicio de Windows.

**Ordenador remoto**: dirección del dispositivo remoto. Permitir únicamente conexiones a direcciones conocidas y de confianza.

**Puerto remoto**: puerto de comunicación. En circunstancias normales, se debe permitir la comunicación en puertos comunes (los números de puerto 80, 443 para el tráfico de Internet, por ejemplo).

Las amenazas informáticas suelen utilizar Internet y conexiones ocultas que les ayudan a infectar sistemas remotos. Si las reglas se configuran correctamente, un cortafuegos puede convertirse en una herramienta muy útil para la protección frente a distintos ataques de código malicioso.

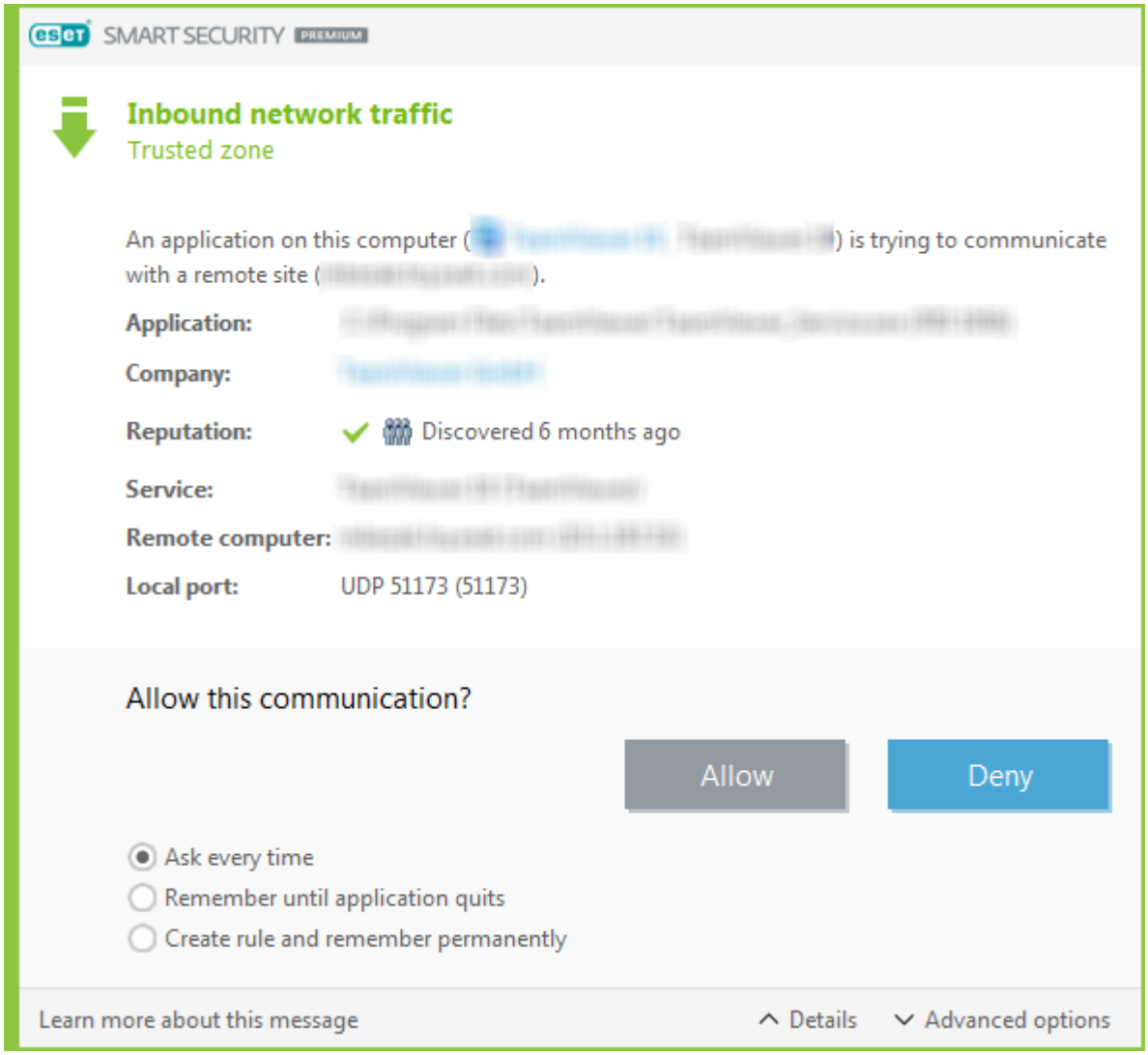
# Cambiar aplicación

El cortafuegos ha detectado una modificación en una aplicación que se utiliza para establecer conexiones salientes desde su ordenador. Es posible que la aplicación se haya actualizado con una nueva versión.

Por otra parte, una modificación puede ser provocada por una aplicación maliciosa. Si no tiene conocimiento de ninguna modificación legítima, recomendamos que rechace la conexión y analice su ordenador con la base de firmas de virus más reciente.

# Comunicación entrante de confianza

Ejemplo de una conexión entrante dentro de la zona de confianza:
Un ordenador remoto intenta establecer comunicación desde la zona de confianza con una aplicación local que se ejecuta en su ordenador.




**Aplicación**: aplicación contactada por un dispositivo remoto.

**Ruta de acceso de la aplicación**: ubicación de la aplicación.

**Aplicación de Microsoft Store**: nombre de la aplicación en Microsoft Store.

**Firmante**: nombre del editor de la aplicación. Haga clic en el texto para mostrar un certificado de seguridad para la empresa.

**Reputación**: la reputación de la aplicación se obtiene mediante la tecnología ESET LiveGrid®.

**Servicio**: nombre del servicio que se está ejecutando actualmente en el ordenador.

**Ordenador remoto**: ordenador remoto que intenta establecer comunicación con la aplicación de su ordenador.

**Puerto remoto**: puerto utilizado para la comunicación.

**Preguntar siempre**: si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla.

**Recordar hasta el cierre de la aplicación**: ESET Small Business Security recordará la acción elegida hasta que vuelva a reiniciar el ordenador.

**Crear regla y recordarla permanentemente**: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Small Business Security recordará la acción y la utilizará si el ordenador remoto vuelve a ponerse en contacto con la aplicación.

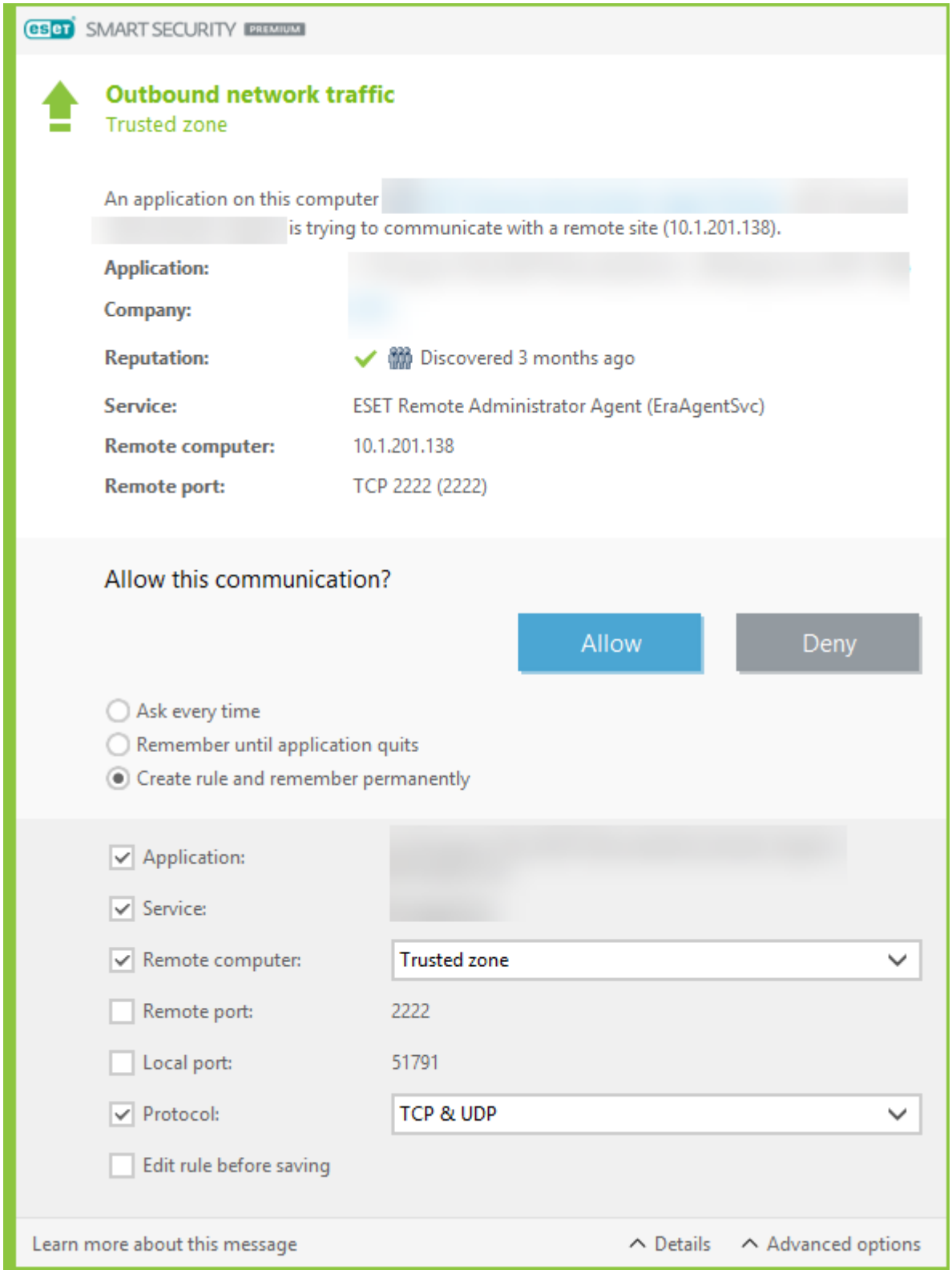
**Permitir**: permite la comunicación entrante.

**Bloquear**: deniega la comunicación entrante.

**Editar regla**: permite personalizar las propiedades de la regla mediante el Editor de reglas del cortafuegos.

# Comunicación saliente de confianza

Ejemplo de una conexión saliente dentro de la zona de confianza:
Una aplicación local intenta establecer una conexión con otro ordenador dentro de la red local, o dentro de una red en la zona de confianza.




**Aplicación**: aplicación contactada por un dispositivo remoto.

**Ruta de acceso de la aplicación**: ubicación de la aplicación.

**Aplicación de Microsoft Store**: nombre de la aplicación en Microsoft Store.

**Firmante**: nombre del editor de la aplicación. Haga clic en el texto para mostrar un certificado de seguridad para la empresa.

**Reputación**: la reputación de la aplicación se obtiene mediante la tecnología ESET LiveGrid®.

**Servicio**: nombre del servicio que se está ejecutando actualmente en el ordenador.

**Ordenador remoto**: ordenador remoto que intenta establecer comunicación con la aplicación de su ordenador.

**Puerto remoto**: puerto utilizado para la comunicación.

**Preguntar siempre**: si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla.

**Recordar hasta el cierre de la aplicación**: ESET Small Business Security recordará la acción elegida hasta que vuelva a reiniciar el ordenador.

**Crear regla y recordarla permanentemente**: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Small Business Security recordará la acción y la utilizará si el ordenador remoto vuelve a ponerse en contacto con la aplicación.

**Permitir**: permite la comunicación entrante.

**Bloquear**: deniega la comunicación entrante.

**Editar regla**: permite personalizar las propiedades de la regla mediante el Editor de reglas del cortafuegos.

# Comunicación entrante

Ejemplo de una conexión de Internet entrante:
Un ordenador remoto intenta comunicarse con una aplicación que se está ejecutando en el ordenador.

**Aplicación**: aplicación contactada por un dispositivo remoto.

**Ruta de acceso de la aplicación**: ubicación de la aplicación.

**Aplicación de Microsoft Store**: nombre de la aplicación en Microsoft Store.

**Firmante**: nombre del editor de la aplicación. Haga clic en el texto para mostrar un certificado de seguridad para la empresa.

**Reputación**: la reputación de la aplicación se obtiene mediante la tecnología ESET LiveGrid®.

**Servicio**: nombre del servicio que se está ejecutando actualmente en el ordenador.

**Ordenador remoto**: ordenador remoto que intenta establecer comunicación con la aplicación de su ordenador.

**Puerto remoto**: puerto utilizado para la comunicación.

**Preguntar siempre**: si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla.

**Recordar hasta el cierre de la aplicación**: ESET Small Business Security recordará la acción elegida hasta que vuelva a reiniciar el ordenador.

**Crear regla y recordarla permanentemente**: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Small Business Security recordará la acción y la utilizará si el ordenador remoto vuelve a

ponerse en contacto con la aplicación.

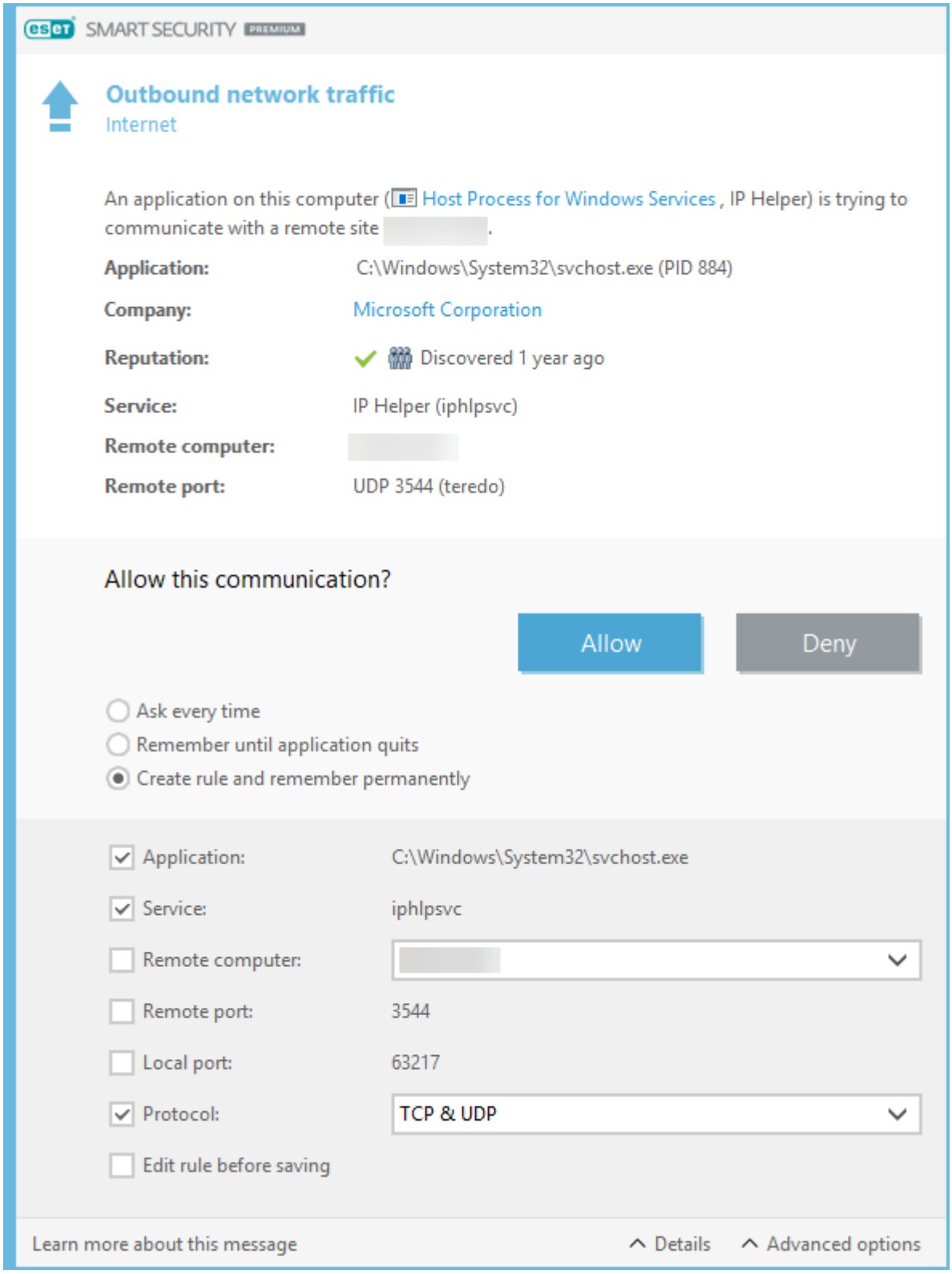
**Permitir**: permite la comunicación entrante.

**Bloquear**: deniega la comunicación entrante.

**Editar regla**: permite personalizar las propiedades de la regla mediante el Editor de reglas del cortafuegos.

# Comunicación saliente

Ejemplo de una conexión a Internet saliente:
Una aplicación local intenta establecer una conexión a Internet.




**Aplicación**: aplicación contactada por un dispositivo remoto.

**Ruta de acceso de la aplicación**: ubicación de la aplicación.

**Aplicación de Microsoft Store**: nombre de la aplicación en Microsoft Store.

**Firmante**: nombre del editor de la aplicación. Haga clic en el texto para mostrar un certificado de seguridad para la empresa.

**Reputación**: la reputación de la aplicación se obtiene mediante la tecnología ESET LiveGrid®.

**Servicio**: nombre del servicio que se está ejecutando actualmente en el ordenador.

**Ordenador remoto**: ordenador remoto que intenta establecer comunicación con la aplicación de su ordenador.

**Puerto remoto**: puerto utilizado para la comunicación.

**Preguntar siempre**: si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla.

**Recordar hasta el cierre de la aplicación**: ESET Small Business Security recordará la acción elegida hasta que vuelva a reiniciar el ordenador.

**Crear regla y recordarla permanentemente**: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Small Business Security recordará la acción y la utilizará si el ordenador remoto vuelve a ponerse en contacto con la aplicación.

**Permitir**: permite la comunicación entrante.

**Bloquear**: deniega la comunicación entrante.

**Editar regla**: permite personalizar las propiedades de la regla mediante el Editor de reglas del cortafuegos.

# Configuración de la visualización de conexiones

Haga clic con el botón derecho del ratón en una conexión para ver más opciones, como:

**Resolver nombres de host**: si es posible, todas las direcciones de red se mostrarán en formato DNS, y no en el formato numérico de dirección IP.

**Mostrar solo las conexiones TCP**: la lista incluye únicamente las conexiones que pertenecen al protocolo TCP.

**Mostrar conexiones en escucha**: seleccione esta opción para mostrar únicamente las conexiones en las que no haya ninguna comunicación establecida actualmente, pero en las que el sistema haya abierto un puerto y esté esperando una conexión.

**Mostrar las conexiones del ordenador**: seleccione esta opción únicamente para mostrar conexiones en las que la ubicación remota sea un sistema local, lo que se denominan conexiones de localhost.

**Velocidad de actualización**: selecciona la frecuencia de actualización de las conexiones activas.

**Actualizar ahora**: vuelve a cargar la ventana **Conexiones de red**.

# Herramientas de seguridad

Abra la ventana principal del programa > **Configuración** > **Herramientas de seguridad** para ajustar los siguientes módulos:

**Banca y navegación seguras**: agrega un nivel adicional de protección de navegadores diseñado para proteger sus datos financieros durante las transacciones en línea. Active **Proteger todos los navegadores** en la configuración avanzada de Banca y navegación seguras para iniciar todos los navegadores web compatibles en un modo seguro.

**Privacidad y seguridad del navegador**: garantiza la privacidad y seguridad de su actividad en línea sin dejar una huella digital.

**Antirrobo**: active Antirrobo para proteger su ordenador en caso de pérdida o robo.

**Secure Data**: con Secure Data activado, puede cifrar sus datos para evitar el uso indebido de información privada y confidencial.

**Password Manager**: Password Manager que protege y almacena sus contraseñas y datos personales.

**VPN** – Proteja los datos y evite el seguimiento no deseado mediante una dirección IP anónima.

# Banca y navegación seguras

La Banca y navegación seguras es un nivel de protección adicional diseñado para proteger sus datos financieros durante las transacciones en línea.

De forma predeterminada, todos los navegadores web compatibles se inician en un modo seguro. Esto le permite navegar por Internet, acceder a la banca a través de Internet y realizar compras y transacciones en línea en un navegador protegido automáticamente.

Se debe activar el sistema de reputación de ESET LiveGrid® (activado de forma predeterminada) para garantizar que la función Banca y navegación seguras funcione correctamente.

Para configurar el comportamiento del navegador protegido, consulte Configuración avanzada de Banca y navegación seguras. Si desactiva **Proteger todos los navegadores**, puede acceder al navegador protegido en la ventana principal del programa > **Descripción general** > **Banca y navegación seguras** o al hacer clic en el icono de escritorio de **Banca y navegación seguras**. El navegador establecido como predeterminado en Windows se abre en un modo seguro.

El uso de la comunicación cifrada HTTPS es necesario para navegar de forma protegida. Los siguientes navegadores son compatibles con Banca y navegación seguras:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+
- Brave 1.65.114.0

Para obtener más información sobre las funciones de Banca y navegación seguras, consulte los siguientes artículos de la Base de conocimiento de ESET disponibles en inglés y otros idiomas:

- ¿Cómo utilizo Banca y navegación seguras de ESET?
- Pausar o desactivar Banca y navegación seguras en los productos para oficina pequeña de ESET para Windows
- Errores comunes de Banca y navegación seguras de ESET

- Glosario de ESET | Banca y navegación seguras

# Notificación del navegador

El navegador protegido le informa de su estado actual con las notificaciones del navegador y el color de la ventana del navegador.

Las notificaciones del navegador se muestran en la ficha del lado derecho.

Para expandir la notificación en el navegador, haga clic en el icono de ESET. Para minimizar la notificación, haga clic en el texto de la notificación. Para descartar la notificación y el marco verde del navegador, haga clic en el icono de cerrar.

Solo pueden descartarse la notificación informativa y el marco verde del navegador.

## Notificaciones del navegador

| Tipo de la notificación | Estado |
|---|---|
| Notificación informativa y marco verde del navegador | Se garantiza la máxima protección y se minimiza la notificación del navegador de forma predeterminada. Expanda la notificación en el navegador y haga clic en **Configuración** para abrir la configuración de Herramientas de seguridad. |
| Advertencia y marco naranja del navegador | El navegador protegido requiere su atención para los problemas que no sean críticos. Para obtener más información sobre un problema o una solución, siga las instrucciones de la notificación del navegador. |
| Alerta de seguridad y marco rojo del navegador | El navegador no cuenta con la protección de Banca y navegación seguras de ESET. Reinicie el navegador para comprobar que la protección esté activa. Para resolver un conflicto con los archivos cargados en el navegador, abra Archivos de registro > **Banca y navegación seguras** y compruebe que los archivos de registro no se carguen la próxima vez que abra el navegador. Si el problema persiste, póngase en contacto con el soporte técnico de ESET siguiendo las instrucciones del artículo de nuestra base de conocimiento. |

# Privacidad y seguridad del navegador

Puede activar la función Privacidad y seguridad del navegador a través de una extensión personalizada disponible en los navegadores compatibles (solo Google Chrome, Mozilla Firefox y Microsoft Edge).

Para instalar y activar la extensión:

1. Asegúrese de usar la última versión de ESET Small Business Security y reinicie correctamente su ordenador después de la actualización.
2. Abra el navegador.
3. La extensión está instalada en el navegador.
4. Active la extensión y se mostrará el navegador con la página de detalles de la extensión.

El menú principal de la extensión Privacidad y seguridad del navegador se divide en las siguientes secciones:

## Visión general

### Búsqueda segura

Haga clic en el icono de interruptor junto a **Analizar resultados de búsqueda** para activar la función y ver

en qué resultados es seguro hacer clic. La búsqueda segura evalúa la lista de direcciones de vínculo y no necesariamente significa que el sitio web no contenga malware. A continuación, nuestro motor de detección detecta la posible presencia de malware en el sitio web.

## Limpieza del navegador

Elimine sus datos de navegación o configure limpiezas periódicas. Puede agregar sitios web en los que desee aceptar cookies y permanecer conectado incluso después de realizar la limpieza del navegador al **agregarlos a una lista**.

- **Limpieza única**: seleccione el intervalo de tiempo en el menú desplegable y el tipo de datos que desea eliminar. Puede eliminar datos privados o selecciones personalizadas.

- **Limpieza periódica**: haga clic en el icono de interruptor  junto a **Limpieza periódica** para activar y configurar la función. Seleccione la frecuencia temporal en el menú desplegable y el tipo de datos que desee eliminar periódicamente. Puede elegir entre la opción privada y selecciones personalizadas.

La opción **Datos personalizados** contiene las siguientes categorías:

- Historial de búsquedas
- Historial de descargas
- Cookies y datos del sitio web
- Imágenes y archivos almacenados en caché
- Contraseñas y datos de inicio de sesión
- Datos de autocompletar formularios
- Service workers

## Limpieza de los metadatos

La función Limpieza de los metadatos controla los datos de privacidad con riesgo de exposición a través de metadatos EXIF compartidos en archivos multimedia, documentos y otros formatos de archivo compatibles. Haga clic en el icono del interruptor  situado junto a **Limpie los metadatos cada vez que suba una imagen** para permitir la supresión de los metadatos.

Haga clic en el icono de interruptor  junto a **Recibir notificaciones en el navegador** para activar la visualización de notificaciones después de la limpieza de los metadatos.

## Análisis de configuración del sitio web

Acceda a los permisos de los sitios web y adminístrelos para controlar qué información pueden usar los sitios web.

- **Notificaciones**: revise de qué sitios web desea **Permitir/Bloquear** las notificaciones.
- **Ubicación**: revise a qué sitios web desea **Permitir/Bloquear** el acceso a su ubicación.

- **Cámara**: revise a qué sitios web desea **Permitir/Bloquear** el acceso a su cámara.
- **Micrófono**: revise a qué sitios web desea **Permitir/Bloquear** el acceso al micrófono.

## Configuración avanzada

### Limpieza del navegador

#### Configuración avanzada de cookies

Lista de sitios web en los que desea aceptar cookies y permanecer conectado incluso después de realizar la limpieza del navegador. Introduzca la dirección URL en el campo de texto y haga clic en **Agregar**. Puede eliminarlo en cualquier momento de la lista al hacer clic en el icono menos junto al sitio web específico.

En la parte inferior de la página se encuentra la lista de dominios sugeridos abiertos actualmente en el navegador. Si no puede ver el sitio web específico, haga clic en **actualizar la lista** y haga clic en el icono más para agregarlo a la lista de cookies aceptadas.

### Análisis de configuración del sitio web

Acceda a los permisos de los sitios web y adminístrelos para controlar qué información pueden usar los sitios web.

- **Notificaciones**: revise de qué sitios web desea **Permitir/Bloquear** las notificaciones.
- **Ubicación**: revise a qué sitios web desea **Permitir/Bloquear** el acceso a su ubicación.
- **Cámara**: revise a qué sitios web desea **Permitir/Bloquear** el acceso a su cámara.
- **Micrófono**: revise a qué sitios web desea **Permitir/Bloquear** el acceso al micrófono.

### Aspecto

Personalice la combinación de colores de la interfaz para que se adapte a sus preferencias. Para elegir la combinación de colores que prefiera, active la casilla de verificación **Claro** u **Oscuro**.

# Antirrobo

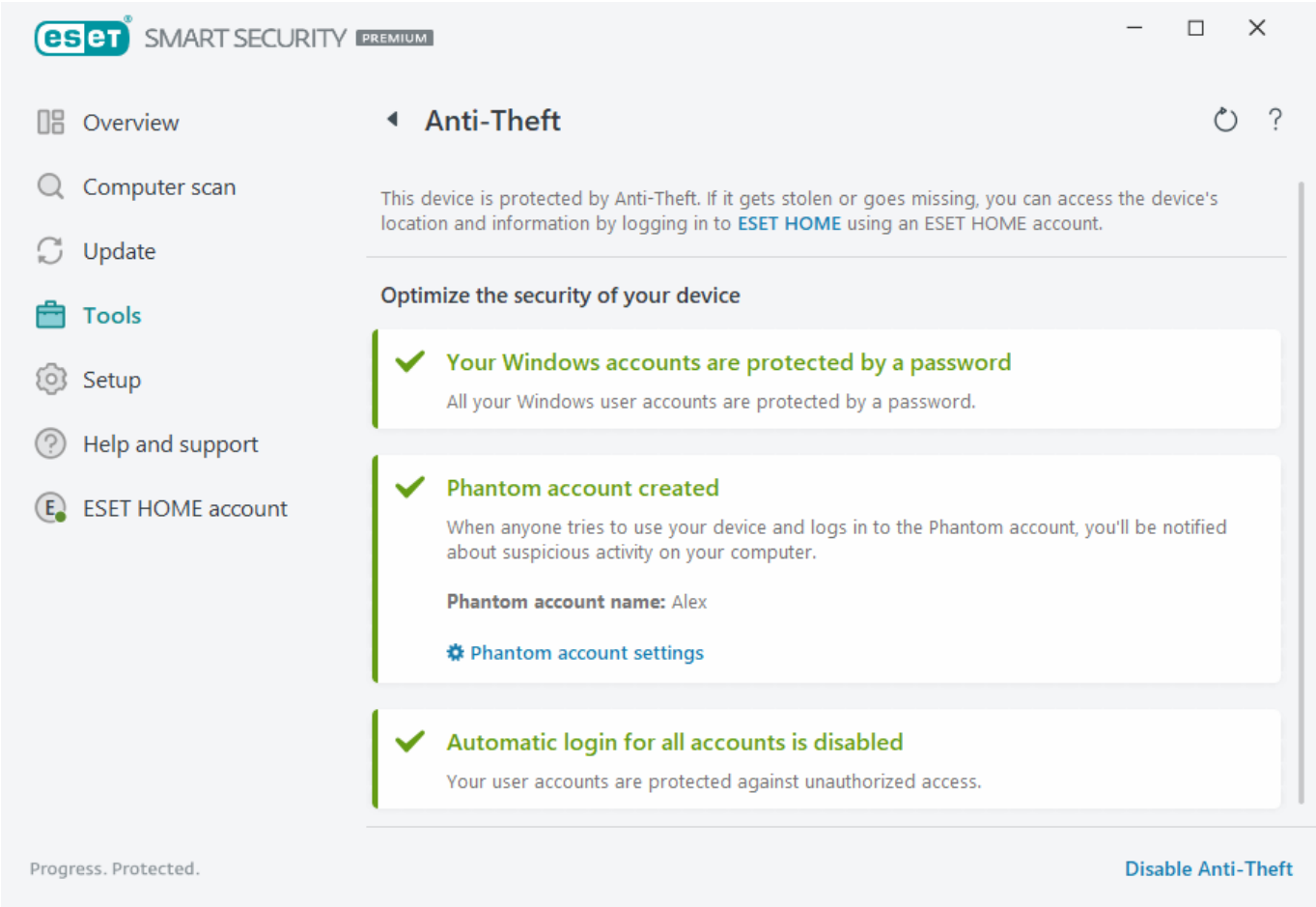
Los dispositivos personales están en constante riesgo de pérdida o robo en los desplazamientos diarios de casa al trabajo u otros lugares públicos. Antirrobo es una es una función que amplía la seguridad a nivel del usuario en caso de robo o pérdida del dispositivo. Antirrobo le permite supervisar el uso del dispositivo y rastrear el dispositivo que le falta por medio de la localización a través de dirección IP en ESET HOME, lo que le ayuda a recuperar su dispositivo y proteger los datos personales.

Mediante el uso de tecnologías modernas como búsqueda geográfica de direcciones IP, captura de imágenes de cámaras web, protección de la cuenta de usuario y supervisión del dispositivo, Antirrobo puede colaborar con usted y las fuerzas del orden para encontrar su ordenador o dispositivo perdido o robado. En ESET HOME, puede ver la actividad que tiene lugar en el ordenador o el dispositivo.

Para obtener más información sobre Antirrobo en ESET HOME, consulte la Ayuda en línea de ESET HOME.

Antirrobo puede no funcionar correctamente en los ordenadores de los dominios debido a restricciones en la administración de cuentas de usuario.

Tras Activar Antirrobo, puede optimizar la seguridad del dispositivo desde la ventana principal del programa > **Configuración** > **Herramientas de seguridad** > **Antirrobo**.




## Opciones de optimización

### No se ha creado ninguna cuenta fantasma

La creación de una cuenta fantasma aumenta la posibilidad de localizar un dispositivo perdido o robado. Si marca su dispositivo como perdido, Antirrobo bloqueará el acceso a las cuentas de usuario activas para proteger los datos confidenciales. Cualquiera que intente utilizar el dispositivo solo podrá utilizar la cuenta fantasma. La cuenta fantasma es una forma de cuenta de invitado con permisos limitados. Se utilizará como la cuenta predeterminada del sistema hasta que se marque el dispositivo como recuperado, lo que impedirá que alguien inicie sesión en otras cuentas de usuario o los datos del usuario.

Siempre que alguien inicie sesión en la cuenta fantasma cuando el ordenador se encuentra en estado normal, se le enviará a usted una notificación por correo electrónico con información sobre actividad sospechosa en el ordenador. Tras recibir la notificación por correo electrónico, puede decidir si desea marcar el ordenador como perdido.

Para crear una cuenta fantasma, haga clic en **Crear cuenta fantasma**, escriba el **nombre de la cuenta fantasma** en el campo de texto y haga clic en **Crear**.

Cuando se haya creado una cuenta fantasma, haga clic en **Configuración de la cuenta fantasma** para cambiar el

nombre de la cuenta o eliminarla.

### Protección por contraseña de las cuentas de Windows

Su cuenta de usuario no está protegida con una contraseña. Recibirá esta advertencia de optimización si al menos una cuenta de usuario no está protegida con una contraseña. La creación de una contraseña para todos los usuarios (excepto para la **Cuenta fantasma**) del ordenador resolverá este problema.

Para crear una contraseña para la cuenta de usuario, haga clic en **Gestionar cuentas de Windows** y cambie la contraseña o siga las instrucciones que se indican a continuación:

1. Pulse CTRL+Alt+Delete en el teclado.
2. Haga clic en **Cambiar una contraseña**.
3. Deje en blanco el campo **Contraseña anterior**.
4. Escriba la contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**, y pulse **Entrar**.

### Inicio de sesión automático en cuentas de Windows

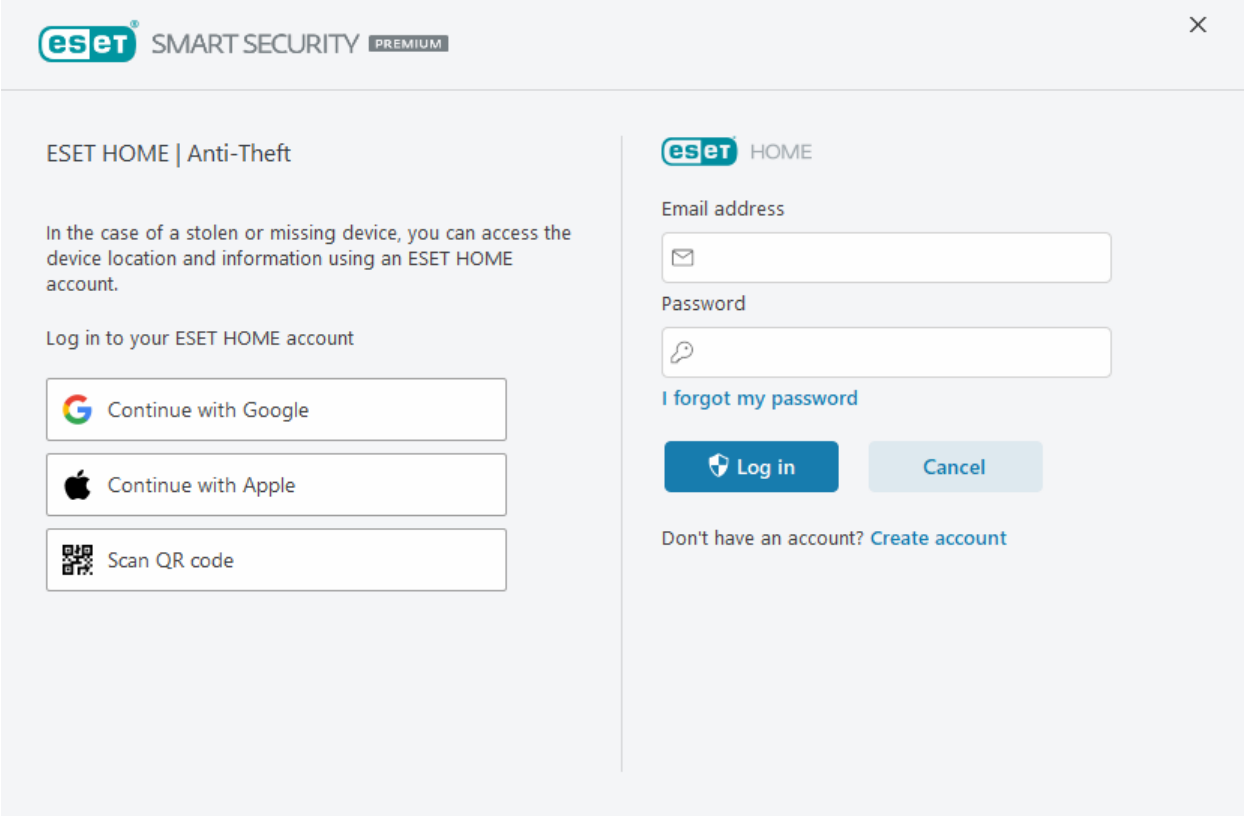
Su cuenta de usuario tiene activado el inicio de sesión automático; por lo tanto, su cuenta no está protegida frente a accesos no autorizados. Recibirá esta advertencia de optimización si al menos una cuenta de usuario tiene activado el inicio de sesión automático. Haga clic en **Desactivar inicio de sesión automático** para resolver este problema de optimización.

### El inicio de sesión automático de la cuenta fantasma

El inicio de sesión automático está activado para la **Cuenta fantasma** de su dispositivo. Cuando el dispositivo está en estado normal, no es recomendable usar el inicio de sesión automático, ya que puede provocar problemas con el acceso a su cuenta de usuario real o enviar falsas alarmas sobre el estado perdido del ordenador. Haga clic en **Desactivar inicio de sesión automático** para resolver este problema de optimización.

# Inicie sesión en su cuenta ESET HOME.

Para activar o desactivar Antirrobo y acceder a la ubicación e información del dispositivo en ESET HOME, inicie sesión en su cuenta de ESET HOME.




Hay varios métodos disponibles para iniciar sesión en su cuenta de ESET HOME:

- **Usar su dirección de correo electrónico y su contraseña de ESET HOME**: escriba la **dirección de correo electrónico** y la **contraseña** que usó para crear su cuenta de ESET HOME y haga clic en **Iniciar sesión**.

- **Usar su cuenta de Google o su AppleID**: haga clic en **Continuar con Google** o en **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se le redirigirá a la página web de confirmación de ESET HOME. Para continuar, vuelva a la ventana del producto de ESET. Para obtener más información sobre el inicio de sesión con la cuenta de Google o con el AppleID, consulte las instrucciones de la Ayuda en línea de ESET HOME.

- **Escanear código QR**: haga clic en **Escanear código QR** para mostrar el código QR. Abra la aplicación móvil de ESET HOME y escanee el código QR o dirija la cámara de su dispositivo hacia el código QR. Para obtener más información, consulte las instrucciones de la Ayuda en línea de ESET HOME.

⚠ Error de inicio de sesión: errores comunes.

Si no tiene una cuenta de ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de ESET HOME.
Si ha olvidado su contraseña, haga clic en **He olvidado mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la Ayuda en línea de ESET HOME.

Antirrobo no es compatible con Microsoft Windows Home Server.

# Defina el nombre del dispositivo

El campo **Nombre del dispositivo** representa el nombre del ordenador (dispositivo) que se mostrará como identificador en todos los servicios de ESET HOME. De forma predeterminada, se usa el nombre de ordenador de

su ordenador. Escriba el nombre del dispositivo o utilice el predeterminado y haga clic en **Continuar**.

# Antirrobo activado o desactivado

Esta ventana contiene un mensaje de confirmación cuando activa o desactiva Antirrobo:

- Activado: su dispositivo ya está protegido por Antirrobo y puede gestionar su seguridad de forma remota en el Portal ESET HOME desde su cuenta.
- Desactivado: Antirrobo está desactivado en este dispositivo y todos los datos relacionados con <%ESET_ANTTHEFT%> correspondientes a se han quitado del Portal ESET HOME.

# Error al agregar el nuevo dispositivo

Ha recibido un error mientras activaba Antirrobo.

Los casos más comunes son:

- Error al iniciar sesión en ESET HOME
- No hay conexión a Internet (o Internet no funciona en ese momento)

Si no puede resolver el problema, póngase en contacto con el Soporte técnico de ESET.

# Secure Data

Secure Data es una función de ESET Small Business Security que le permite cifrar datos en un ordenador y unidades extraíbles para proteger la información privada y evitar su uso indebido. Consulte las preguntas frecuentes de ESET Secure Data para obtener más información.

Para activar Secure Data, elija una de las opciones siguientes:

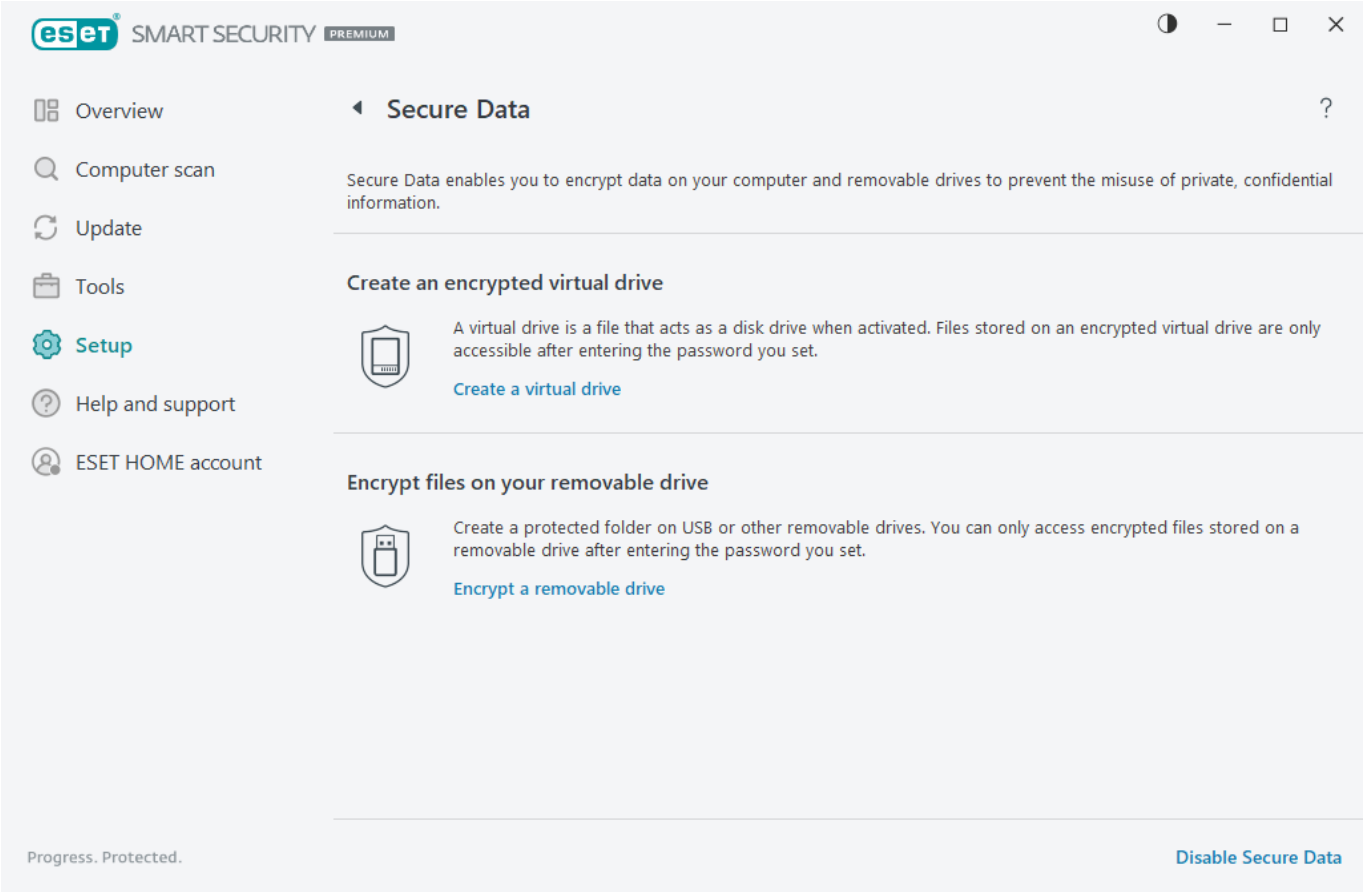
- En la ventana principal del programa > **Información general**, haga clic en **Secure Data**.
- En la ventana principal del programa > **Configuración** > **Herramientas de seguridad**, active el interruptor **Secure Data**.

No se puede instalar ESET Endpoint Encryption en una máquina en la que Secure Data ya está instalado.

Cuando Secure Data esté activado, en la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad** > **Secure Data** y escoja una de las opciones de cifrado siguientes:

- Crear una unidad virtual cifrada
- Cifrar archivos de una unidad extraíble

Secure Data solo admite el estilo de partición Master Boot Record (MBR) para unidades extraíbles.




# Crear una unidad virtual cifrada

Puede utilizar Secure Data para crear unidades virtuales cifradas. No hay límite para el número de unidades que puede crear, siempre que exista espacio en disco duro. Siga los pasos siguientes para crear una unidad virtual cifrada:

1. En la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad** > **Secure Data** > **Crear una unidad virtual**.

2. Haga clic en **Examinar** para seleccionar la ubicación en la que se guardará la unidad virtual.

3. Escriba un nombre para la unidad virtual y haga clic en **Guardar**.

4. Utilice el menú desplegable **Capacidad máxima de la unidad** para establecer el tamaño de la unidad virtual y haga clic en **Continuar**.

5. Establezca una contraseña para la unidad virtual. Si no desea que la unidad virtual se descifre automáticamente al iniciar sesión en su cuenta de Windows, anule la selección de **Descifrar automáticamente en esta cuenta de Windows**. Haga clic en **Continuar**.

6. Haga clic en **Listo**. La unidad virtual cifrada se crea y queda lista para el uso. Aparecerá como un disco local si abre **Este PC**.

Para acceder a la unidad cifrada después de reiniciar el ordenador, localice el archivo de la unidad cifrada (tipo de archivo `.eed`) que ha creado y haga doble clic en él. Si se le solicita, escriba la contraseña que ha configurado al crear la unidad cifrada. La unidad se montará y aparecerá como un disco local en Este PC. Cuando la unidad cifrada esté montada como un disco local, dicho disco local y su contenido descifrado estarán disponibles para

otros usuarios en su ordenador, a menos que cierre sesión o lo reinicie.

> ¿Puedo eliminar una unidad virtual?
> Sí. Para eliminar una unidad virtual cifrada, siga las instrucciones del artículo de preguntas frecuentes sobre ESET Secure Data.

# Cifrar archivos de una unidad extraíble

Secure Data le permite crear una carpeta cifrada en unidades extraíbles. Siga los pasos indicados a continuación para cifrar archivos en la unidad extraíble:

1. Introduzca la unidad extraíble (unidad de memoria flash USB, disco duro USB) en el ordenador.

2. En la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad** > **Secure Data** > **Cifrar una unidad extraíble**.

3. Seleccione la unidad extraíble conectada que quiere cifrar y haga clic en **Continuar**.
Haga clic en **Actualizar** para actualizar la lista de unidades cifrables. Las unidades cifradas o no compatibles no se muestran.
Si desea descifrar la carpeta protegida en la unidad extraíble seleccionada en cualquier dispositivo con Windows sin necesidad de tener ESET Small Business Security instalado, seleccione **Descifrar una carpeta en cualquier dispositivo con Windows**.

4. Establezca una contraseña para el directorio cifrado. Si no desea que la unidad virtual se descifre automáticamente al iniciar sesión en su cuenta de Windows, anule la selección de **Descifrar automáticamente en esta cuenta de Windows**. Haga clic en **Continuar**.

5. Su unidad extraíble está protegida y el directorio cifrado que incluye está listo para su uso.

A partir de este momento, si conecta la unidad extraíble a un ordenador en el que Secure Data no está instalado, la carpeta cifrada no estará visible. Si la unidad extraíble se conecta a un ordenador que tiene Secure Data instalado, se le pedirá que introduzca la contraseña para descifrar la unidad extraíble. Si no escribe la contraseña, la carpeta cifrada estará visible, pero no se podrá acceder a ella.

# Password Manager

Password Manager forma parte del paquete ESET Small Business Security.

Es un administrador de contraseñas que protege y almacena sus contraseñas y datos personales. También incluye una función para rellenar formularios que ahorra tiempo completando formularios web de forma automática y precisa.

Para obtener más información, consulte la ayuda en línea de Password Manager.

- Password Manager instalación
- Empiece a usar Password Manager.
- Administrar almacenes de Password Manager en ESET HOME

# VPN

ESET VPN es parte del paquete ESET Small Business Security. VPN le permite mantener los datos seguros, evitar el seguimiento no deseado y mejorar la privacidad con la seguridad adicional que ofrece una dirección IP anónima.

Para comenzar a usar VPN, haga clic en **Descargar e instalar VPN.**

Para obtener más información, consulte la ayuda en línea de ESET Virtual Private Network.

- VPN Introducción.
- VPN Instalación.
- Trabajo con VPN.

# Importar y exportar configuración

Puede importar o exportar el archivo de configuración .xml de ESET Small Business Security del menú **Configuración**.

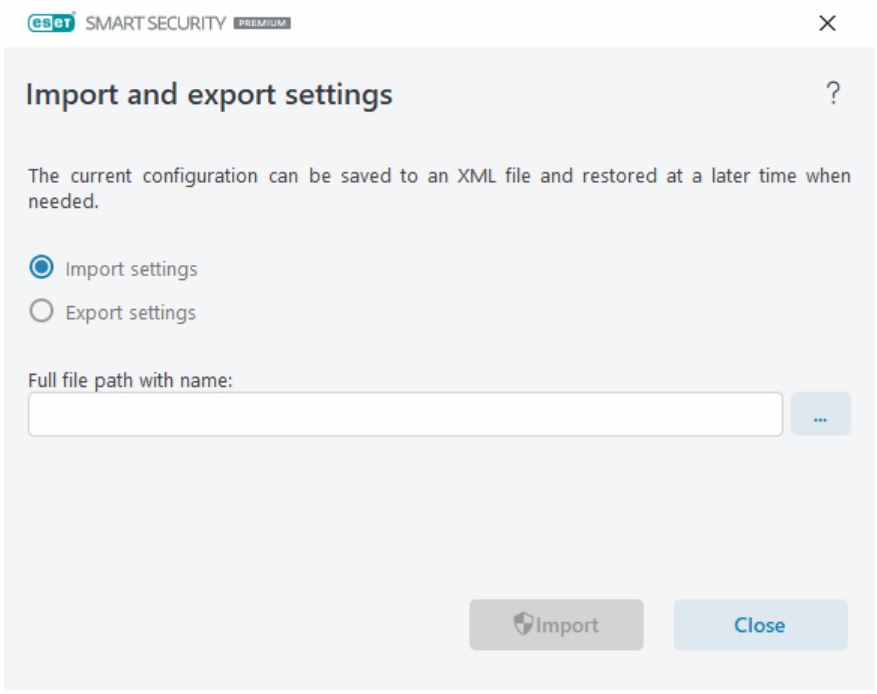
> **Instrucciones con ilustraciones**
> Consulte Importar o exportar los ajustes de configuración de ESET con un archivo .xml para obtener instrucciones con ilustraciones disponibles en inglés y en otros idiomas.

La importación y la exportación de archivos de configuración son útiles cuando necesita realizar una copia de seguridad de la configuración actual de ESET Small Business Security para utilizarla en otro momento. La opción de configuración de exportación también es conveniente cuando desea utilizar su configuración preferida en varios sistemas. Ya que le permite importar un archivo .xml para transferir estos ajustes.

Para importar la configuración, en la ventana principal del programa, haga clic en **Configuración** > **Importar/exportar configuración** y seleccione **Importar configuración**. Escriba el nombre del archivo de configuración o haga clic en el botón **...** para buscar el archivo de configuración que desea importar.

Para exportar la configuración, en la ventana principal del programa, haga clic en **Configuración** > **Importar/exportar configuración**. Seleccione **Exportar configuración** y escriba la ruta de acceso completa del archivo con el nombre. Haga clic en **...** para desplazarse a un lugar del ordenador en el que guardar el archivo de configuración.

> Puede encontrarse con un error al exportar la configuración si no dispone de derechos suficientes para escribir el archivo exportado en el directorio especificado.




# Ayuda y asistencia técnica

Haga clic en **Ayuda y asistencia técnica** en la ventana principal del programa para mostrar información de soporte técnico y herramientas de solución de problemas que le ayudarán a resolver los problemas que pueda encontrar.

## Suscripción

- Resolver problemas con la suscripción: haga clic en este vínculo para buscar soluciones a problemas relacionados con la activación o el cambio de suscripción.

- Cambiar suscripción: haga clic para abrir la ventana de activación y activar el producto. Si el dispositivo está conectado a ESET HOME, elija una suscripción de su cuenta de ESET HOME o agregue una nueva.

## Producto instalado

- Novedades: haga clic aquí para abrir la ventana de información sobre funciones nuevas y mejoradas.

- Acerca de ESET Small Business Security: muestra información sobre su copia de ESET Small Business Security.

- Resolver problemas con el producto: haga clic en este vínculo para buscar soluciones a los problemas más frecuentes.

**Página de ayuda**: haga clic en este enlace para abrir las páginas de ayuda de ESET Small Business Security.

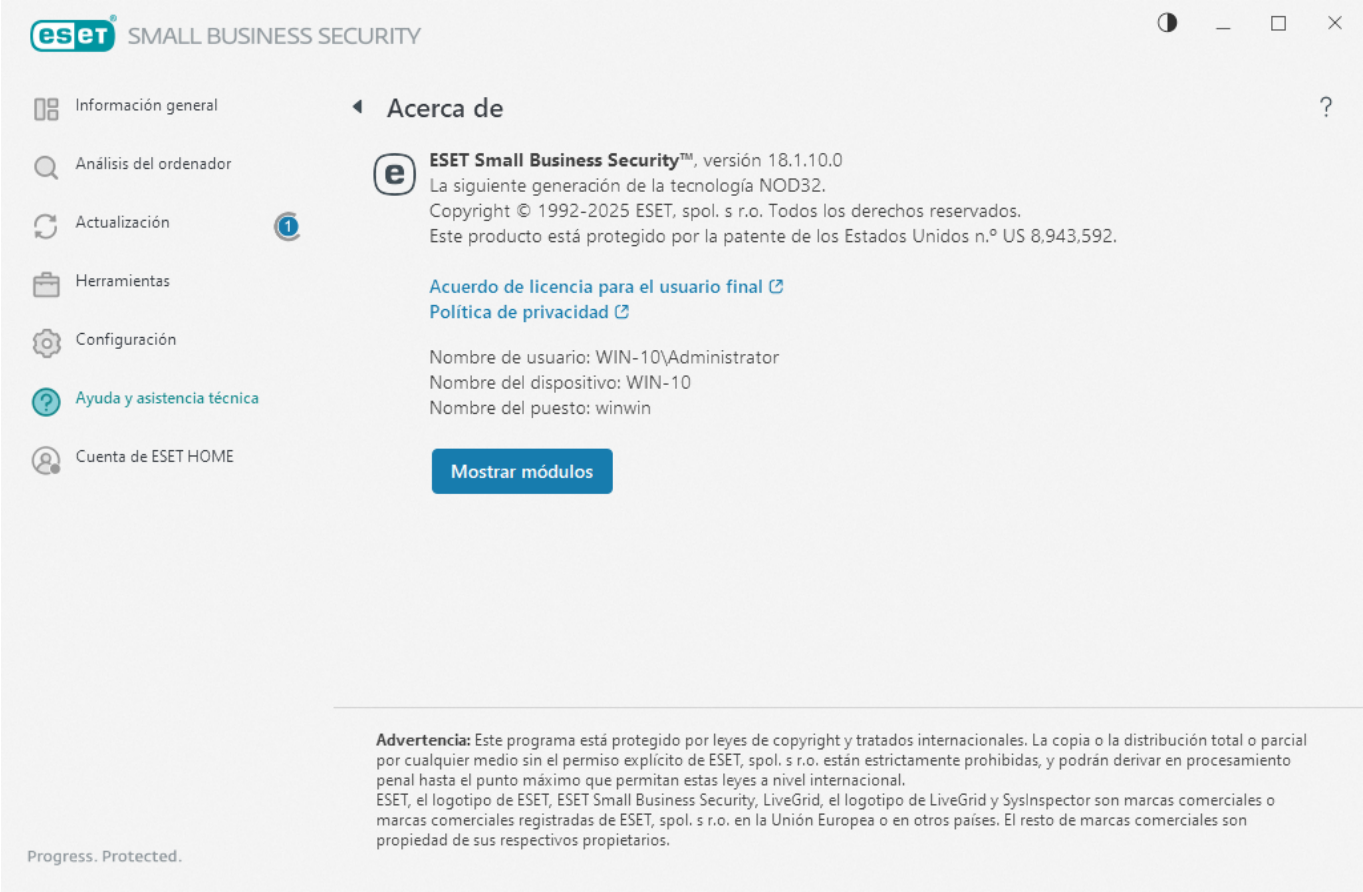
**Soporte técnico**

**Base de conocimientos**: la base de conocimiento de ESET contiene respuestas a las preguntas más frecuentes y posibles soluciones a diferentes problemas. La actualización periódica por parte de los especialistas técnicos de ESET convierte a esta base de conocimientos en la herramienta más potente para resolver diversos

problemas.

# Acerca de ESET Small Business Security

En esta ventana se muestran detalles sobre la versión instalada de ESET Small Business Security y su ordenador.




Haga clic en **Mostrar módulos** para ver información sobre la lista de módulos del programa cargados.

- Para copiar en el portapapeles información sobre los módulos, haga clic en **Copiar**. Esto puede ser útil para resolver problemas o ponerse en contacto con el servicio de soporte técnico.

- Haga clic en **Motor de detección** en la ventana Módulos para abrir el radar de virus de ESET, que contiene información sobre cada versión del Motor de detección de ESET.

# Noticias de ESET

En esta ventana ESET Small Business Security comunica las noticias acerca de ESET de forma periódica.

Los mensajes en el producto están pensados para informar a los usuarios acerca de noticias de ESET y otras comunicaciones. Para que se envíen los mensajes de marketing, es necesario que el usuario dé su consentimiento. Los mensajes de marketing no se envían a los usuarios de forma predeterminada (se muestran como un signo de interrogación).

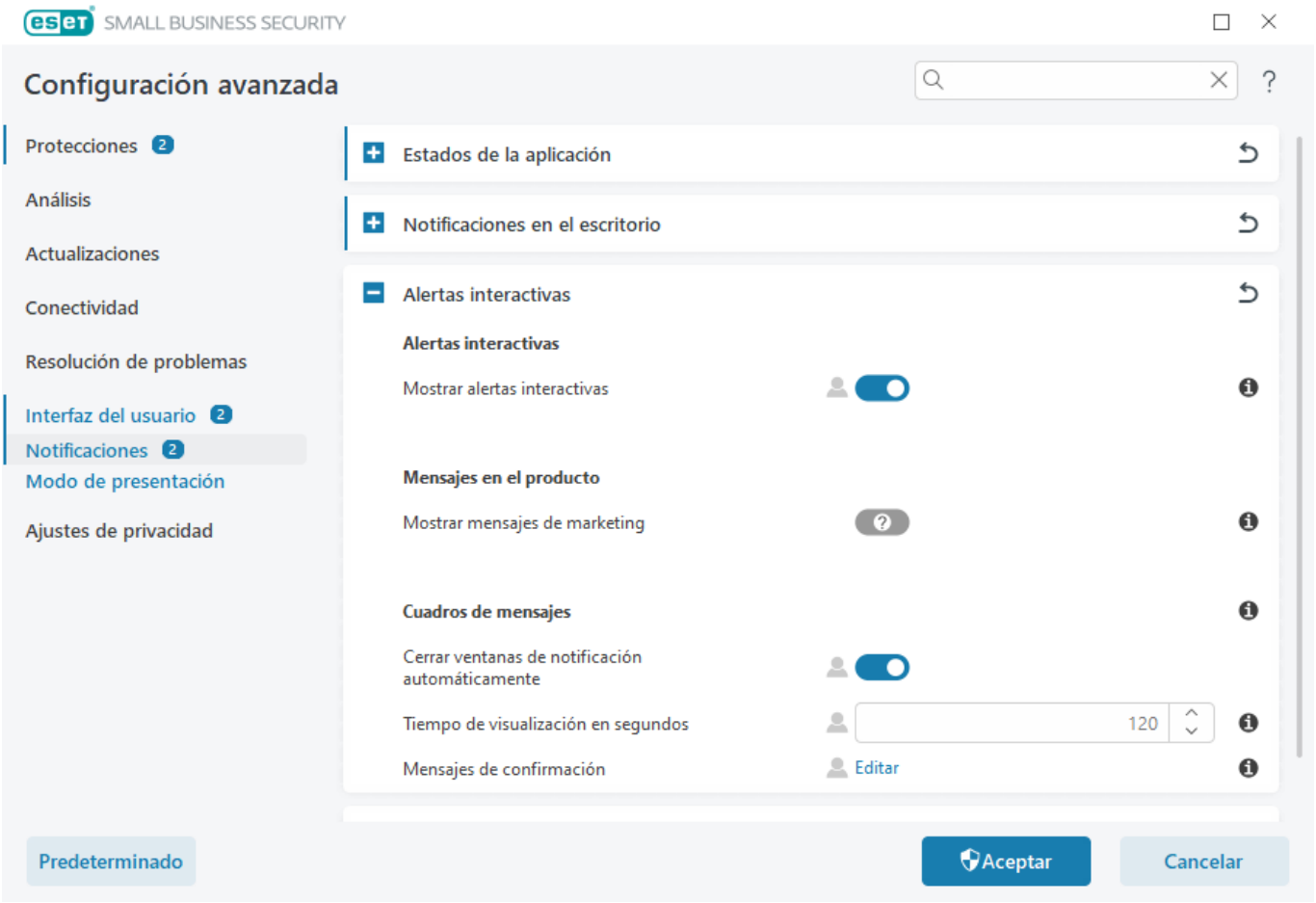
Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no le interesa recibir material de marketing de ESET, desactive la opción **Mostrar mensajes de marketing**.

Para activar o desactivar la recepción de mensajes de marketing mediante una ventana notificación, siga las instrucciones que se indican a continuación.

1. Abre la Configuración avanzada.

2. Haga clic en **Notificaciones** > **Alertas interactivas**.

3. Modifique la opción **Mostrar mensajes de marketing**.




# Enviar datos de configuración del sistema

Con el fin de prestar asistencia con la máxima rapidez y precisión posibles, ESET requiere información sobre la configuración de ESET Small Business Security, información detallada y de los procesos en ejecución (ESET SysInspectorArchivo de registro de ), así como datos del registro. ESET utilizará estos datos solo para prestar asistencia técnica al cliente.

Después de enviar el formulario web, también se enviarán a ESET los datos de configuración de su sistema. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Para enviar el formulario web sin enviar ningún dato, haga clic en **No enviar datos** y continúe.

Puede configurar el envío de los datos de configuración del sistema en Configuración avanzada > **Herramientas** > **Diagnóstico** > Soporte técnico.

Si ha decidido enviar los datos de configuración del sistema, es necesario completar y enviar el formulario web. De lo contrario, no se creará el ticket y se perderán los datos de configuración del sistema. Si no se pueden enviar los datos de configuración del sistema, rellene el formulario web y espere las instrucciones del Soporte técnico.

# Soporte técnico

En la ventana principal del programa, haga clic en **Ayuda y asistencia técnica** > **Soporte técnico**.

## Ponerse en contacto con el servicio de soporte técnico

**Solicitar soporte**: si no encuentra respuesta a su problema, puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con el departamento de soporte técnico de ESET. En función de su configuración, se mostrará la ventana de envío de datos de configuración del sistema antes de rellenar el formulario web.

## Obtener información de soporte técnico

**Detalles para el servicio de soporte técnico**: cuando se le solicite, podrá copiar y enviar información al servicio de soporte técnico de ESET (como, por ejemplo, detalles de la suscripción, nombre del producto, versión del producto, sistema operativo e información sobre el ordenador).

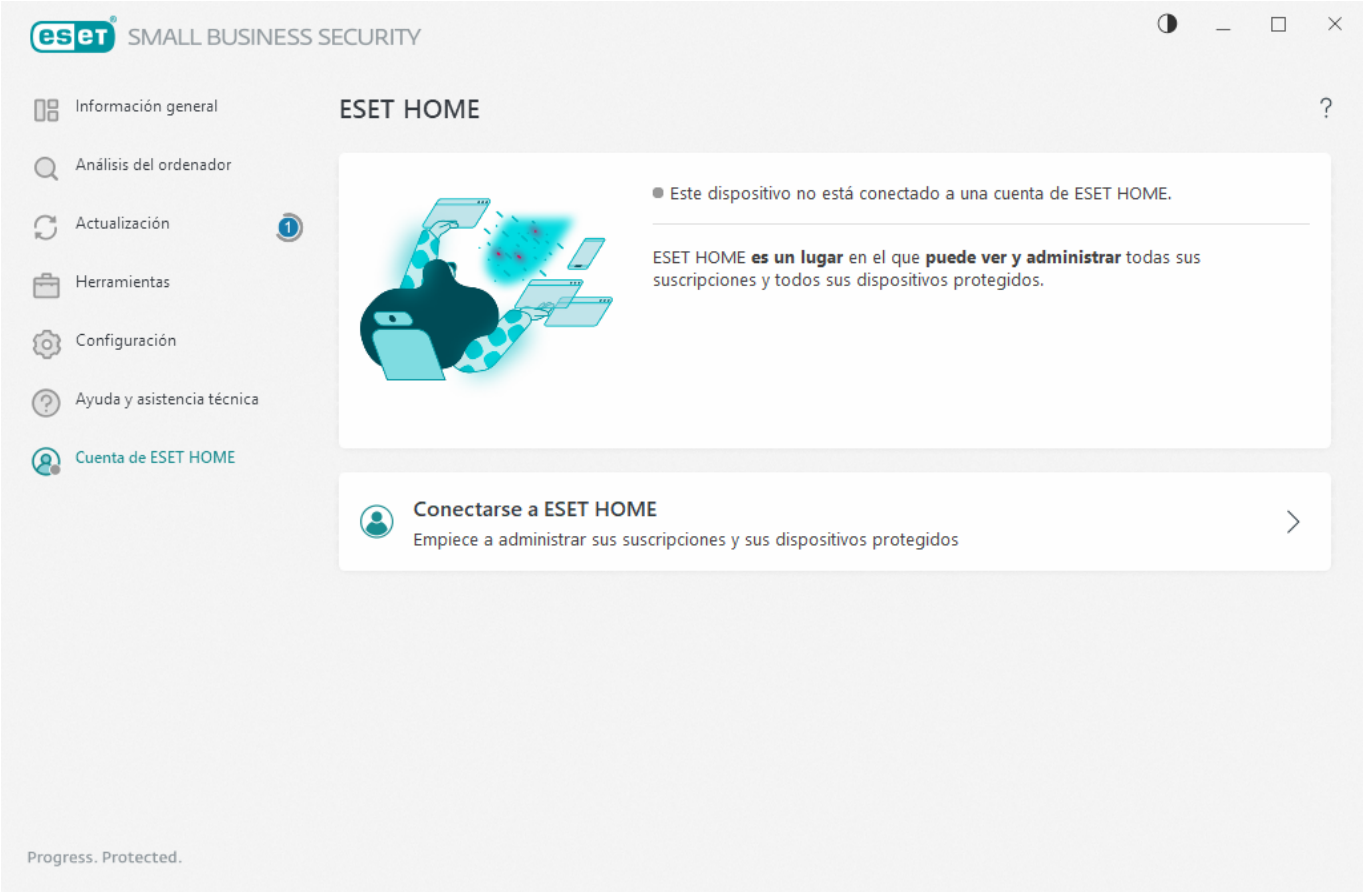
**ESET Log Collector** – Vínculo al artículo de la base de conocimiento de ESET, donde puede descargar ESET Log Collector, aplicación que recopila información y registros de un ordenador automáticamente para ayudar a resolver problemas con mayor rapidez. Si desea obtener más información, consulte la guía del usuario de ESET Log Collector en línea.

Active Registro avanzado para crear registros avanzados de todas las funciones disponibles con el objetivo de ayudar a los desarrolladores a diagnosticar y resolver problemas. El nivel mínimo de detalle del registro es **Diagnóstico**. El registro avanzado se desactivará automáticamente después de dos horas, a menos que lo detenga antes haciendo clic en **Detener registro avanzado**.

Una vez creados todos los registros, aparece la ventana de notificación, que proporciona acceso directo a la carpeta Diagnóstico con los registros creados.

# Cuenta de ESET HOME

Puede consultar el estado de conexión de la cuenta de ESET HOME en la ventana principal del programa > **Cuenta de ESET HOME**.




## Este dispositivo no está conectado a una cuenta de ESET HOME

Haga clic en Conectar a ESET HOME para conectar su dispositivo a ESET HOME y administrar las suscripciónes y los dispositivos protegidos. Puede renovar, actualizar o ampliar la suscripción y ver detalles importantes sobre ella.

En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar suscripciones distintas, descargar productos en sus dispositivos, consultar el estado de seguridad del producto o compartir suscripción por correo electrónico. Para obtener más información, visite la ayuda en línea de ESET HOME.

## Este dispositivo está conectado a una cuenta de ESET HOME

Puede administrar la seguridad de su dispositivo de forma remota en el portal o la aplicación para dispositivos móviles de ESET HOME. Haga clic en **App Store** o **Google Play** para analizar un código QR con su teléfono móvil y descargar la aplicación para dispositivos móviles ESET HOME.

**Cuenta de ESET HOME:** el nombre de su cuenta de ESET HOME.

**Nombre del dispositivo**: nombre de este dispositivo que se muestra en la cuenta de ESET HOME.

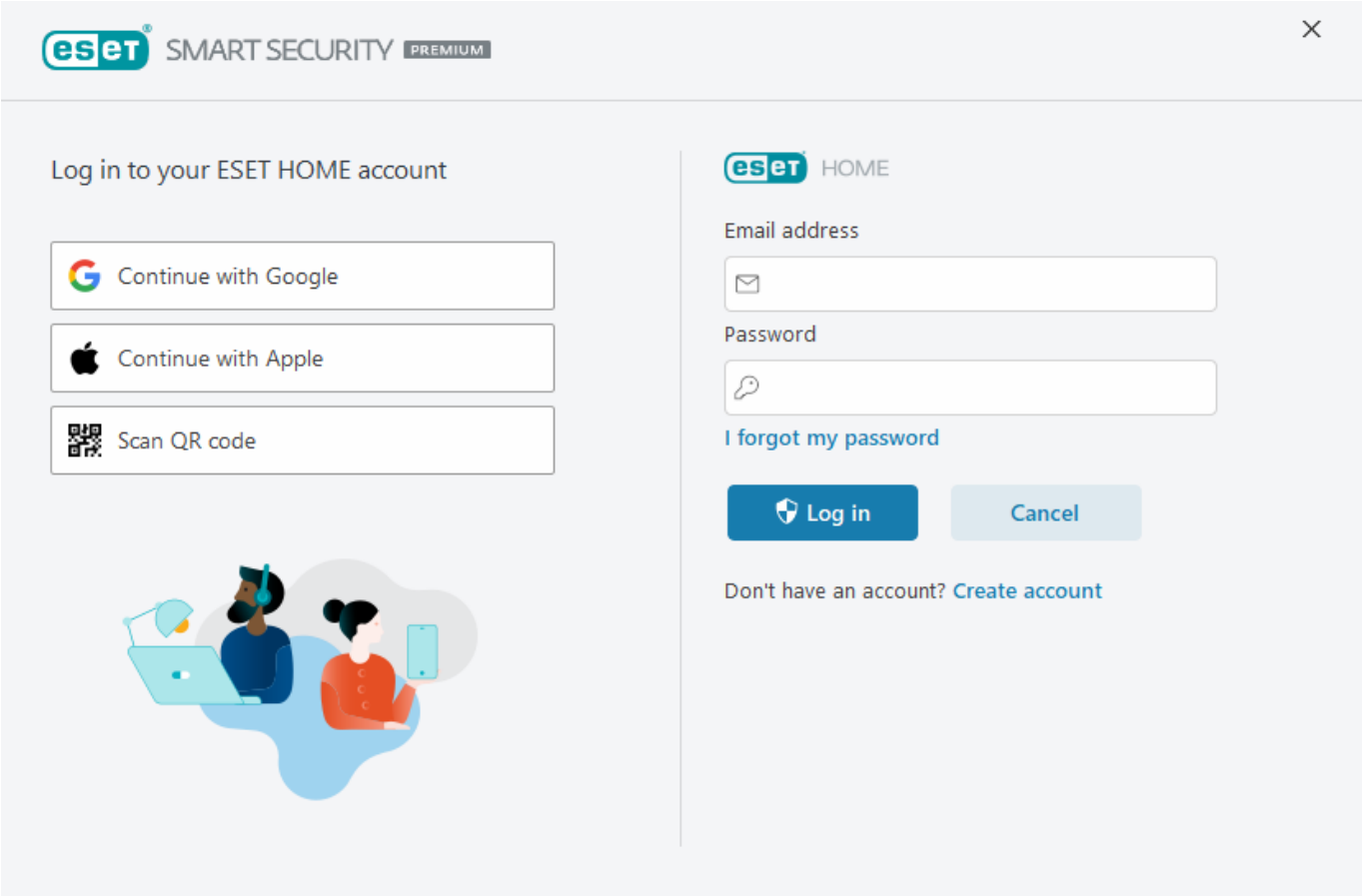
**Abrir ESET HOME**: abre el portal de administración de ESET HOME.

Para desconectar el dispositivo de la cuenta de ESET HOME, haga clic en **Desconectar de ESET HOME** > **Desconectar**. La suscripción utilizada para la activación permanecerá activa, y su dispositivo estará protegido.

# Conéctese a ESET HOME

Conecte el dispositivo a ESET HOME para ver y administrar todas las suscripciones ESET activadas y los dispositivos. Puede renovar, actualizar o ampliar la suscripción y ver detalles importantes sobre ella.

En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar suscripciones distintas, descargar productos en sus dispositivos, consultar el estado de seguridad del producto o compartir suscripciones por correo electrónico. Para obtener más información, visite la ayuda en línea de ESET HOME.




Conecte el dispositivo a ESET HOME:

Si se está conectando a ESET HOME durante la instalación o selecciona **Utilizar una cuenta de ESET HOME** como método de activación, siga las instrucciones del tema Usar cuenta de ESET HOME.
Si ya ha instalado y activado ESET Small Business Security con una suscripción agregada a su cuenta de ESET HOME, puede conectar su dispositivo a ESET HOME mediante el portal ESET HOME. Siga las instrucciones de la Guía de ayuda en línea de ESET HOME y permita la conexión en ESET Small Business Security.

1. En la ventana principal del programa, haga clic en **cuenta ESET HOME** > **Conectar a ESET HOME** o haga clic en **Conectar a ESET HOME** en la notificación **Conectar este dispositivo a una cuenta de ESET HOME**.

2. Inicie sesión en su cuenta ESET HOME.

Si no tiene una cuenta de ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de ESET HOME.
Si ha olvidado su contraseña, haga clic en **He olvidado mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la Ayuda en línea de ESET HOME.

3. Defina el **Nombre del dispositivo** y haga clic en **Continuar**.

4. Tras una conexión correcta, se muestra una ventana de detalles. Haga clic en **Listo**.

# Iniciar sesión en ESET HOME

Hay varios métodos disponibles para iniciar sesión en su cuenta de ESET HOME:

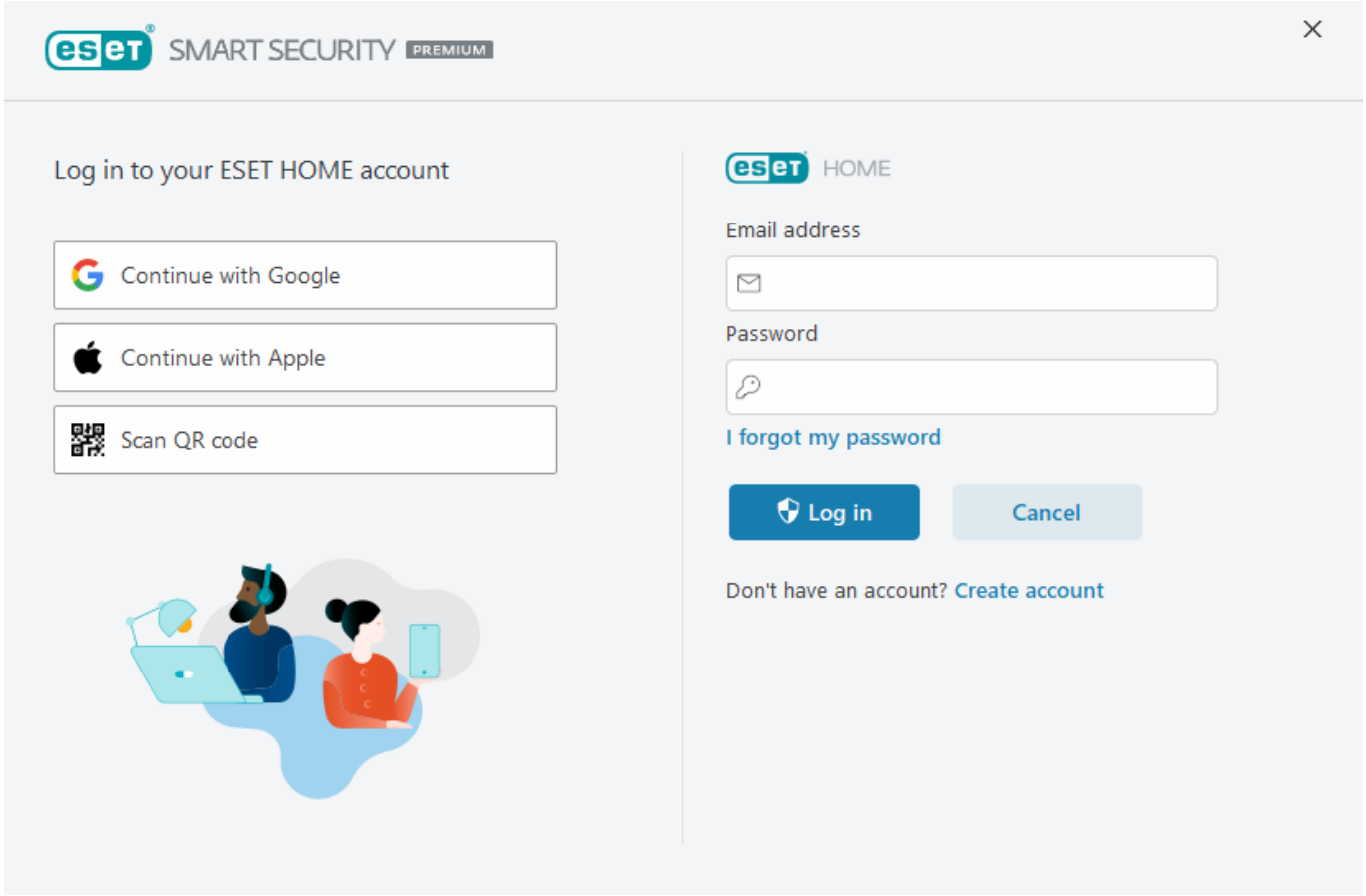
• **Usar su dirección de correo electrónico y su contraseña de ESET HOME**: escriba la **dirección de correo electrónico** y la **contraseña** que usó para crear su cuenta de ESET HOME y haga clic en **Iniciar sesión**.

• **Usar su cuenta de Google o su AppleID**: haga clic en **Continuar con Google** o en **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se le redirigirá a la página web de confirmación de ESET HOME. Para continuar, vuelva a la ventana del producto de ESET. Para obtener más información sobre el inicio de sesión con la cuenta de Google o con el AppleID, consulte las instrucciones de la Ayuda en línea de ESET HOME.

• **Escanear código QR**: haga clic en **Escanear código QR** para mostrar el código QR. Abra la aplicación móvil de ESET HOME y escanee el código QR o dirija la cámara de su dispositivo hacia el código QR. Para obtener más información, consulte las instrucciones de la Ayuda en línea de ESET HOME.

Si no tiene una cuenta de ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de ESET HOME.
Si ha olvidado su contraseña, haga clic en **He olvidado mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la Ayuda en línea de ESET HOME.

Error de inicio de sesión: errores comunes.



# Error de inicio de sesión: errores comunes

## No hemos encontrado ninguna cuenta que coincida con la dirección de correo electrónico introducida

La dirección de correo electrónico que ha introducido no coinciden con ninguna cuenta de ESET HOME. Haga clic en **Atrás** y escriba la dirección de correo electrónico y la contraseña correctas.

Para iniciar sesión debe crear una cuenta de ESET HOME. Si no tiene cuenta de ESET HOME, haga clic en **Atrás** > **Crear cuenta** o consulte Crear una nueva cuenta de ESET HOME.

## El nombre de usuario y la contraseña no coinciden.

La contraseña introducida no coincide con la dirección de correo electrónico introducida. Haga clic en **Atrás**, escriba la contraseña correcta y asegúrese de que la dirección de correo electrónico introducida sea correcta. Si sigue sin poder iniciar sesión, haga clic en **Atrás** > **He olvidado mi contraseña** para restablecer su contraseña y siga los pasos de la pantalla o consulte He olvidado mi contraseña de ESET HOME.

## La opción de inicio de sesión seleccionada no coincide con su cuenta

Su cuenta está vinculada a su cuenta de las redes sociales. Para iniciar sesión en ESET HOME, haga clic en **Continuar con Google** o en **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se le redirigirá a la página web de confirmación de ESET HOME. Puede desconectar su cuenta de las redes sociales de su cuenta de ESET HOME en el portal ESET HOME.

## Contraseña incorrecta

Este error puede producirse si su ESET Small Business Security ya está conectado a ESET HOME, está realizando cambios que requieren que inicie sesión (por ejemplo, desactivar Antirrobo) y la contraseña que ha introducido no coincide con su cuenta.

Haga clic en **Atrás** y escriba la contraseña correcta. Si sigue sin poder iniciar sesión, haga clic en **Atrás** > **He olvidado mi contraseña** para restablecer su contraseña y siga los pasos de la pantalla o consulte He olvidado mi contraseña de ESET HOME.

# Agregar dispositivo en ESET HOME

Si ya ha instalado y activado ESET Small Business Security con una suscripción agregada a su cuenta de ESET HOME, puede conectar su dispositivo a ESET HOME mediante el portal ESET HOME.

1. Envíe una solicitud de conexión a su dispositivo.

2. ESET Small Business Security muestra la ventana de diálogo **Conectar este dispositivo a una cuenta de ESET HOME** con el nombre de una cuenta de ESET HOME. Haga clic en **Permitir** para conectar el dispositivo a la cuenta de ESET HOME.

Si no hay interacción, la solicitud de conexión se cancelará automáticamente transcurridos aproximadamente 30 minutos.

# Configuración avanzada

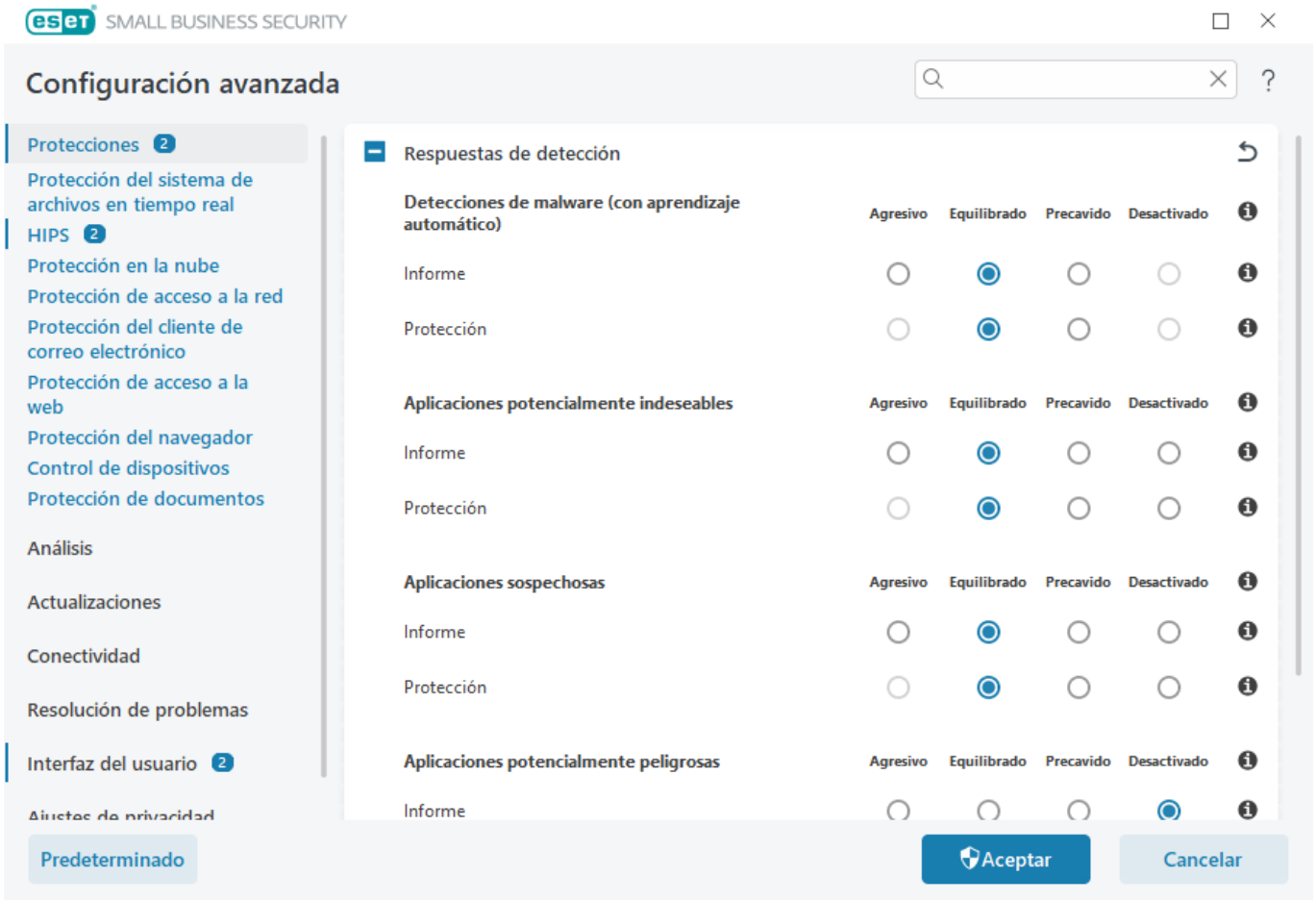
La configuración avanzada le permite configurar ajustes detallados de ESET Small Business Security para satisfacer sus necesidades.

Para abrir Configuración avanzada, abra la ventana principal del programa y presione la tecla **F5** del teclado o haga clic en **Configuración** > **Configuración avanzada**.

En función de la Configuración de acceso, es posible que se le pida que escriba una contraseña para abrir Configuración avanzada.

En la configuración avanzada, puede configurar los siguientes ajustes:

- Protecciones
- Análisis
- Actualizaciones
- Conectividad
- Resolución de problemas
- Interfaz del usuario
- Notificaciones
- Ajustes de privacidad




# Análisis

Configuración avanzada > **Análisis** le permite configurar las siguientes opciones:

- Exclusiones
- Opciones avanzadas
- Análisis de tráfico de red

# Exclusiones

**Exclusiones** le permite excluir objetos del motor de detección. Para garantizar que se analizan todos los objetos, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Entre las situaciones en las que quizá deba excluir un objeto se pueden incluir el análisis de entradas de grandes bases de datos, que ralentizaría su ordenador durante un análisis, o de software que entre en conflicto con el análisis.

Exclusiones de rendimiento: excluya archivos y carpetas del análisis. Las exclusiones de rendimiento son útiles para excluir el análisis a nivel de archivo de aplicaciones de juego o cuando cause un comportamiento anómalo del sistema o un aumento del rendimiento.

Las exclusiones de detección le permiten excluir de la detección objetos mediante el nombre de detección, la ruta de acceso o su hash. Las exclusiones de detección no excluyen archivos y carpetas del análisis como las exclusiones de rendimiento. Las exclusiones de detección solo excluyen objetos cuando los detecta el motor de

detección y existe una regla apropiada en la lista de exclusiones.

No deben confundirse con otros tipos de exclusiones:

- Exclusiones de procesos: todas las operaciones de archivos atribuidas a procesos de aplicaciones excluidos se excluyen del análisis (puede ser necesario para aumentar la velocidad de la copia de seguridad y la disponibilidad del servicio),
- Extensiones de archivo excluidas,
- Exclusiones del HIPS,
- Filtro de exclusión para protección en la nube.

# Exclusiones de rendimiento

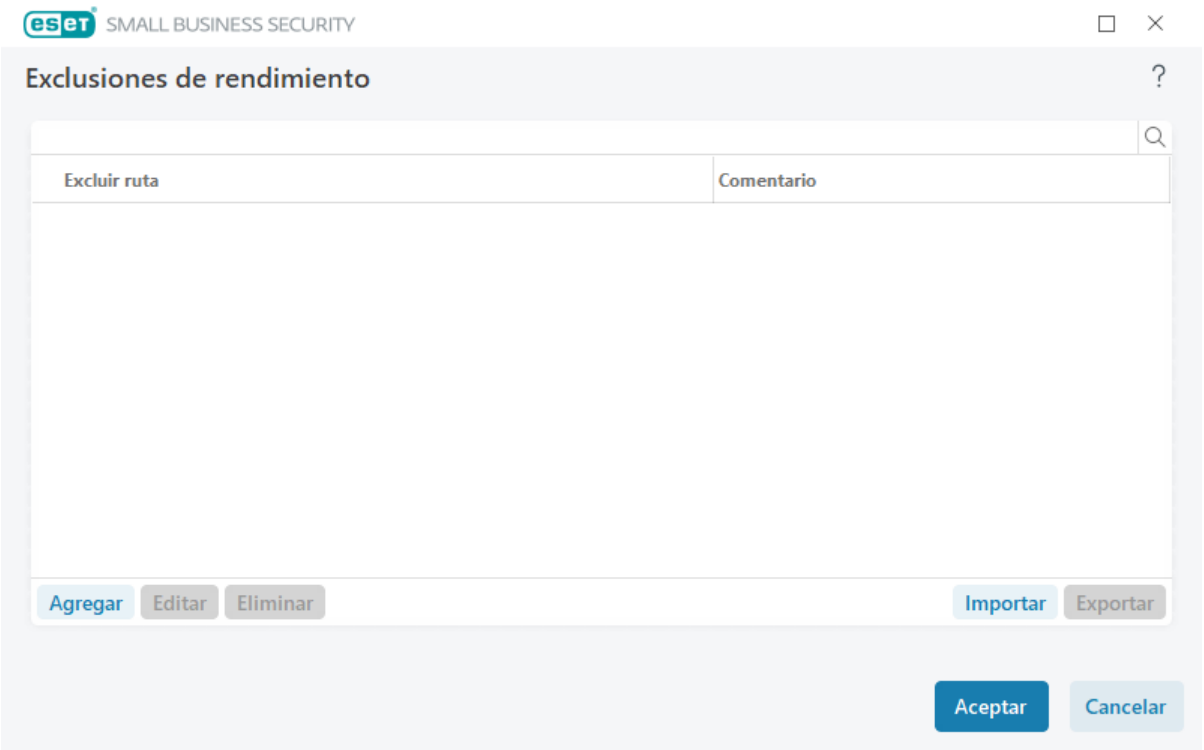
Las exclusiones de rendimiento le permiten excluir archivos y carpetas del análisis.

Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Sin embargo, hay situaciones en las que puede necesitar excluir un objeto, como en el caso de las entradas de bases de datos grandes que ralentizarían su ordenador durante un análisis o en el del software que entre en conflicto con el análisis.

Puede agregar los archivos y las carpetas que se excluirán del análisis a la lista de exclusiones en Configuración avanzada > **Motor de detección** > **Exclusiones** > **Exclusiones de rendimiento** > **Editar**.

> No se debe confundir con Exclusiones de detección, Extensiones de archivo excluidas, Exclusiones del HIPS ni Exclusiones de procesos.

Para excluir un objeto (ruta de acceso: archivo o carpeta) del análisis, haga clic en **Agregar** e introduzca la ruta de acceso aplicable o selecciónelo en la estructura de árbol.



El módulo de **protección del sistema de archivos en tiempo real** o de **análisis del ordenador** no detectará las amenazas que haya contenidas en un archivo si este cumple los criterios de exclusión del análisis.

## Elementos de control

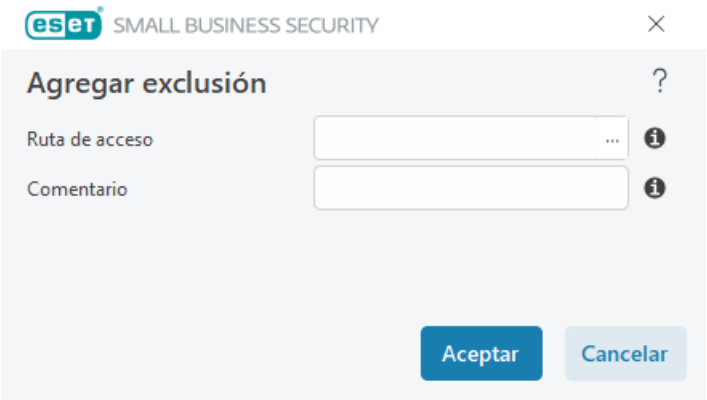
- **Agregar**: excluye los objetos de la detección.
- **Modificar**: le permite modificar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (pulse CTRL y haga clic para seleccionar varias entradas).

# Agregar o modificar la exclusión de rendimiento

Este cuadro de diálogo excluye una ruta de acceso (archivo o directorio) específica de este ordenador.

### Elegir ruta de acceso o introducirla manualmente

Para elegir una ruta de acceso apropiada, haga clic en **...** en el campo **Ruta de acceso**. Cuando la escriba manualmente, vea más ejemplos de formato de exclusión a continuación.




---

Puede utilizar comodines para excluir un grupo de archivos. El signo de interrogación (*?*) representa un carácter único, y el asterisco (***) una cadena variable de cero o más caracteres.

### Formato de exclusión

• Si desea excluir todos los archivos y subcarpetas de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara ***.
• Si desea excluir únicamente los archivos .doc, utilice la máscara **.doc*.
• Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (con caracteres distintos) y solo conoce el primero (por ejemplo, "D"), utilice el siguiente formato: *D????.exe* (los signos de interrogación sustituyen a los caracteres que faltan o son desconocidos)
Ejemplos:
• *C:\Tools**: La ruta de acceso debe terminar con la barra invertida (\) y el asterisco (*) para indicar que es una carpeta y se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
• *C:\Tools*.**: El mismo comportamiento que *C:\Tools**.
• *C:\Tools*: no se excluirá la carpeta *Tools*. Desde la perspectiva del análisis, *Tools* también puede ser un nombre de archivo.
• *C:\Tools*.dat*: esto excluirá los archivos .dat de la carpeta *Tools*.
• *C:\Tools\sg.dat*: Esto excluirá este archivo concreto de la ruta de acceso exacta.

### Variables del sistema en exclusiones

Puede utilizar variables del sistema, como %PROGRAMFILES%, para definir las exclusiones del análisis.

- Para excluir la carpeta Program Files con esta variable del sistema, utilice la ruta de acceso *%PROGRAMFILES%** (recuerde agregar la barra invertida y el asterisco al final de la ruta de acceso) al agregarla a las exclusiones.
- Para excluir todos los archivos y carpetas de un subdirectorio de *%PROGRAMFILES%*, utilice la ruta de acceso *%PROGRAMFILES%\Directorio_excluido**

Ampliar la lista de variables del sistema compatibles

En el formato de exclusión de ruta de acceso se pueden usar las siguientes variables:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

No son compatibles las variables del sistema específicas de usuario (como *%TEMP%* o *%USERPROFILE%*) ni variables de entorno (como *%PATH%*).

### No se admiten comodines en el medio de una ruta de acceso

El uso de comodines en el medio de una ruta de acceso (por ejemplo, *C:\Tools*\Data\file.dat*) puede funcionar, pero no es compatible oficialmente con las exclusiones de rendimiento.
Cuando usa exclusiones de detección, no hay restricciones en lo que respecta al uso de comodines en el medio de una ruta de acceso.

### Orden de las exclusiones

- No hay opciones para ajustar el nivel de prioridad de las exclusiones con los botones arriba/abajo (como sí ocurre con las Reglas del cortafuegos, que se ejecutan desde arriba hacia abajo).
- Cuando el motor de análisis encuentre la primera regla aplicable, no se evaluará la segunda regla aplicable.
- Cuantas menos reglas haya, mayor será el rendimiento de análisis.
- Evite crear reglas simultáneas.

# Formato de exclusión de ruta de acceso

Puede utilizar comodines para excluir un grupo de archivos. El signo de interrogación (*?*) representa un carácter único, y el asterisco (***) una cadena variable de cero o más caracteres.

### Formato de exclusión

• Si desea excluir todos los archivos y subcarpetas de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara *.*.
• Si desea excluir únicamente los archivos .doc, utilice la máscara **.doc*.
• Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (con caracteres distintos) y solo conoce el primero (por ejemplo, "D"), utilice el siguiente formato: *D????.exe* (los signos de interrogación sustituyen a los caracteres que faltan o son desconocidos)

Ejemplos:
• *C:\Tools**: La ruta de acceso debe terminar con la barra invertida (\) y el asterisco (*) para indicar que es una carpeta y se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
• *C:\Tools*.**: El mismo comportamiento que *C:\Tools**.
• *C:\Tools*: no se excluirá la carpeta *Tools*. Desde la perspectiva del análisis, *Tools* también puede ser un nombre de archivo.
• *C:\Tools*.dat*: esto excluirá los archivos .dat de la carpeta *Tools*.
• *C:\Tools\sg.dat*: Esto excluirá este archivo concreto de la ruta de acceso exacta.

### Variables del sistema en exclusiones

Puede utilizar variables del sistema, como %PROGRAMFILES%, para definir las exclusiones del análisis.
• Para excluir la carpeta Program Files con esta variable del sistema, utilice la ruta de acceso *%PROGRAMFILES%** (recuerde agregar la barra invertida y el asterisco al final de la ruta de acceso) al agregarla a las exclusiones.
• Para excluir todos los archivos y carpetas de un subdirectorio de *%PROGRAMFILES%*, utilice la ruta de acceso *%PROGRAMFILES%\Directorio_excluido**

Ampliar la lista de variables del sistema compatibles

En el formato de exclusión de ruta de acceso se pueden usar las siguientes variables:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

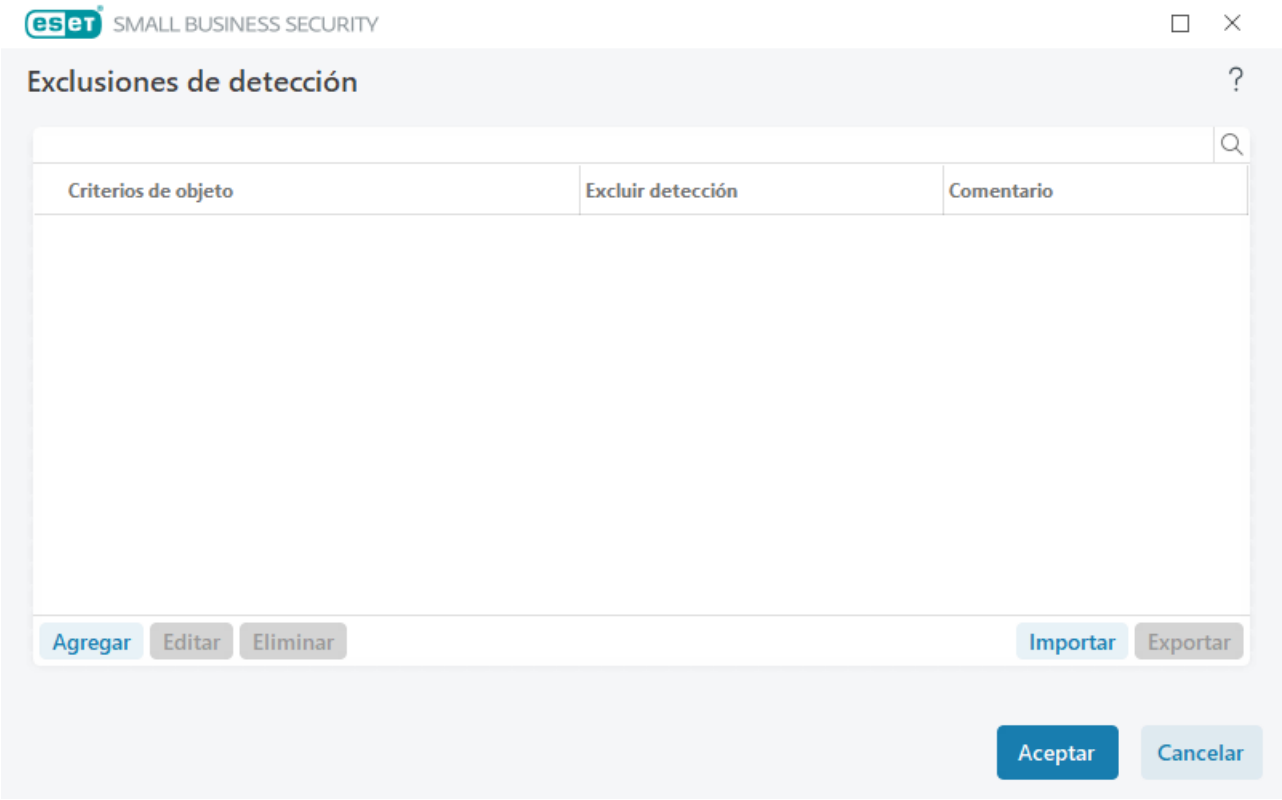
No son compatibles las variables del sistema específicas de usuario (como *%TEMP%* o *%USERPROFILE%*) ni variables de entorno (como *%PATH%*).

# Exclusiones de detección

Las exclusiones de detección le permiten excluir objetos de la detección filtrando el nombre de detección, la ruta de acceso del objeto o su hash.

### Cómo funcionan las exclusiones de detección

Las exclusiones de detección no excluyen archivos y carpetas del análisis como las Exclusiones de rendimiento. Las exclusiones de detección solo excluyen objetos cuando los detecta el motor de detección y existe una regla apropiada en la lista de exclusiones.
Por ejemplo (consulte la primera fila de la imagen que aparece a continuación), cuando un objeto se detecta como Win32/Adware.Optmedia y el archivo detectado es *C:\Recovery\file.exe*. En la segunda fila, cada archivo, que tiene el hash SHA-1 apropiado, se excluirá siempre a pesar del nombre de detección.




Para garantizar que se detecten todas las amenazas, recomendamos crear exclusiones de detección solo cuando sea absolutamente necesario.

Para agregar archivos y carpetas a la lista de exclusiones, abra Configuración avanzada > **Análisis** > **Exclusiones** > **Exclusiones de detección** > **Editar**.

No se confunda con Exclusiones de rendimiento, Extensiones de archivo excluidas, Exclusiones del HIPS ni Exclusiones de procesos.

Para excluir un objeto (por su nombre de detección o hash) del motor de detección, haga clic en **Agregar**.

En el caso de Aplicaciones potencialmente indeseables y Aplicaciones potencialmente peligrosas, también se puede crear la exclusión por su nombre de detección:

- En la ventana de alerta que informa de la detección (haga clic en **Mostrar opciones avanzadas** y, a continuación, seleccione **Excluir de la detección**).
- Desde el menú contextual Archivos de registro con el Asistente de creación de exclusión de detección.
- Haciendo clic en **Herramientas** > **Cuarentena** y, a continuación, haciendo clic con el botón derecho en el archivo en cuarentena y seleccionando **Restaurar y excluir** en el menú contextual.

## Criterios de objetos de exclusiones de detección

- **Ruta de acceso**: limite una exclusión de detección para una ruta de acceso especificada (o para cualquiera).
- **Nombre de la detección**: si se muestra el nombre de una detección junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha detección, pero no por completo. Si más adelante este archivo se infecta con otro malware, se detectará.

- **Hash**: excluye un archivo según el hash especificado SHA-1, sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.

# Agregar o editar una exclusión de detección

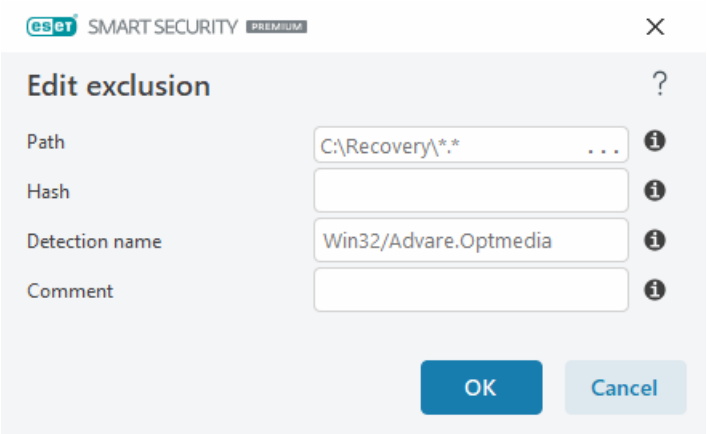
## Excluir detección

Se debe facilitar un nombre de detección de ESET válido. Para obtener un nombre de detección válido, consulte Archivos de registro y, a continuación, seleccione **Detecciones** en el menú desplegable Archivos de registro. Esta opción resulta útil cuando se está detectando un falso positivo en ESET Small Business Security. Excluir infiltraciones reales es muy peligroso, por lo que le recomendamos que excluya únicamente los archivos o los directorios afectados haciendo clic en **...** en el campo **Ruta de acceso** o solo durante un periodo de tiempo concreto. Las exclusiones también se aplican a las Aplicaciones potencialmente indeseables, las aplicaciones potencialmente peligrosas y las aplicaciones sospechosas.

Consulte también Formato de exclusión de ruta de acceso.

### Excluir dirección URL

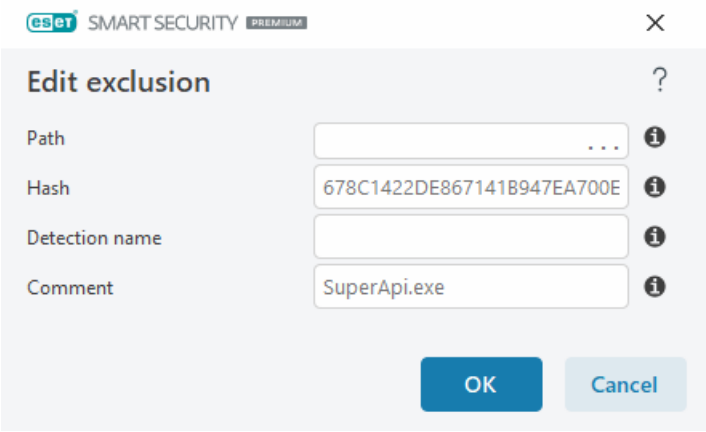
El **campo Ruta** también puede incluir una URL o un carácter comodín "*****". Para excluir la detección, escriba el formato de URL admitido en el campo **Ruta**, p. ej. *https://domain.com* o **domain.com**.




Consulte el Ejemplo de exclusiones de detección a continuación.

## Excluir hash

Excluye un archivo según el hash especificado SHA-1, sea cual sea el tipo de archivo, la ubicación, el nombre o su extensión.




**Exclusiones por nombre de la detección**

Para excluir una detección específica por su nombre, escriba el nombre de detección válido: Win32/Adware.Optmedia

También puede usar el siguiente formato cuando excluye una detección de la ventana de alerta de ESET Small Business Security:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

---

## Elementos de control

- **Agregar**: excluye los objetos de la detección.
- **Modificar**: le permite modificar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (pulse CTRL y haga clic para seleccionar varias entradas).

# Asistente de creación de exclusión de detección

Las exclusiones de detección también se pueden crear desde el menú contextual Archivos de registro (no disponible para detecciones de malware):

1. En la ventana del programa principal, haga clic en **Herramientas** > **Archivos de registro**.
2. Haga clic con el botón derecho en una detección en el **Registro de detecciones**.
3. Haga clic en **Crear exclusión**.

Para excluir una o más detecciones en función de los **Criterios de exclusión**, haga clic en **Cambiar criterios**:

- **Archivos exactos**: excluya cada archivo por su hash SHA-1.
- **Detección**: excluya cada archivo por su nombre de detección.
- **Ruta de acceso + Detección**: excluya cada archivo por su nombre de detección y ruta de acceso, incluido el nombre del archivo (por ejemplo, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

La opción recomendada se preselecciona en función del tipo de detección.

También puede agregar un **Comentario** antes de hacer clic en **Crear exclusión**.

# Antimalware Scan Interface (AMSI)

**Activar análisis avanzado mediante AMSI** es la herramienta Interfaz de análisis contra el código malicioso de Microsoft que permite el análisis de scripts Powershell, scripts ejecutados por Windows Script Host y datos analizados con el SDK de AMSI.

# Análisis de tráfico de red

El análisis de tráfico de red proporciona protección contra malware para protocolos de aplicación, que integra múltiples técnicas avanzadas de análisis de malware. El análisis de tráfico de red analiza los protocolos HTTP(S), POP3(S) e IMAP(S) automáticamente, independientemente del navegador de Internet o del cliente de correo electrónico.

Puede activar/desactivar el análisis de tráfico de red en Configuración avanzada > **Análisis** > **Análisis de tráfico de red**.

**Activar análisis de tráfico de red**: si desactiva esta opción, no se analizarán los protocolos HTTP(S), POP3(S) e IMAP(S). Tenga en cuenta que las siguientes funciones de ESET Small Business Security requieren que el análisis de tráfico de red esté activado:

- Protección del acceso a la Web
- Privacidad y seguridad del navegador
- Banca y navegación seguras
- SSL/TLS
- Protección Anti-Phishing
- Protección de clientes de correo electrónico

# Protección en la nube

ESET LiveGrid® (que se basa en el sistema avanzado de alerta temprana ThreatSense.Net) utiliza los datos enviados por usuarios de ESET de todo el mundo y los envía al laboratorio de investigación de ESET. ESET LiveGrid® Proporciona metadatos y muestras sospechosas, lo cual nos permite reaccionar de forma inmediata a las necesidades de nuestros clientes y hace posible la respuesta de ESET a las amenazas más recientes.

ESET LiveGuard es una función que agrega una capa de protección diseñada específicamente para mitigar las amenazas desconocidas. Cuando esta función está activada, las muestras sospechosas que aún no se han confirmado como maliciosas y pueden incluir malware se envían automáticamente a la nube de ESET.

Están disponibles las opciones siguientes:

# Activar el sistema de reputación ESET LiveGrid®, el sistema de respuesta ESET LiveGrid® y ESET LiveGuard

El sistema de reputación ESET LiveGrid® permite crear listas blancas y listas negras en la nube. El sistema de respuesta ESET LiveGrid® recopila información sobre su ordenador relacionada con nuevas amenazas detectadas. La función ESET LiveGuard detecta nuevas amenazas nunca vistas mediante el análisis de su comportamiento en un entorno de pruebas.

Puede consultar la reputación de los procesos en ejecución y los archivos directamente en la interfaz del programa o en el menú contextual; además, dispone de información adicional de ESET LiveGrid®. Con la protección proactiva de ESET LiveGuard, se bloquea la ejecución de los nuevos archivos hasta recibir el resultado del análisis.

## Activar el sistema de reputación ESET LiveGrid®

El sistema de reputación ESET LiveGrid® permite crear listas blancas y listas negras en la nube.

Puede consultar la reputación de los archivos y Procesos en ejecución directamente en la interfaz del programa o en el menú contextual; además, disponen de información adicional en ESET LiveGrid®.

## Activar el sistema de respuesta ESET LiveGrid®

Además del sistema de reputación ESET LiveGrid®, el sistema de respuesta ESET LiveGrid® recopilará información sobre su ordenador relacionada con las amenazas recién detectadas. Esta información puede incluir:

- Muestra o copia del archivo en el que apareció la amenaza
- Ruta de acceso del archivo
- Nombre de archivo
- Fecha y hora
- El proceso por el que apareció la amenaza en su ordenador
- Información sobre el sistema operativo de su ordenador

De forma predeterminada, ESET Small Business Security está configurado para enviar archivos sospechosos para su análisis detallado en el laboratorio de virus de ESET. Los archivos con extensiones concretas, como *.doc* o *.xls*, se excluyen siempre. También puede agregar otras extensiones para excluir los archivos específicos que usted o su empresa no deseen enviar.

Puede obtener más información sobre el envío de datos relevantes en la Política de privacidad.

## Puede decidir no activar ESET LiveGrid®

El software no perderá ninguna funcionalidad, pero en algunos casos ESET Small Business Security puede responder más rápido a las nuevas amenazas cuando ESET LiveGrid® está activado. Si ha utilizado ESET LiveGrid® anteriormente y lo ha desactivado, es posible que aún haya paquetes de datos pendientes de envío. Estos paquetes se enviarán a ESET incluso después de la desactivación. Una vez que se haya enviado toda la

información actual, no se crearán más paquetes.

Puede obtener más información sobre ESET LiveGrid® en el Glosario.
Consulte nuestras instrucciones con ilustraciones disponibles en inglés y en otros idiomas para activar o desactivar ESET LiveGrid® en ESET Small Business Security.

---

## Configuración de la protección en la nube en Configuración avanzada

Para acceder a la configuración de ESET LiveGrid® y ESET LiveGuard, abra Configuración avanzada > **Protecciones** > **Protección en la nube**.

- **Activar el sistema de reputación ESET LiveGrid® (recomendado)**: el sistema de reputación ESET LiveGrid® mejora la eficiencia de las soluciones contra software malicioso de ESET mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.

- **Activar el sistema de respuesta ESET LiveGrid®**: envía los datos de envío pertinentes (descritos en la sección **Envío de muestras a continuación**) junto con informes de bloqueo y estadísticas al laboratorio de investigación de ESET para su análisis.

- **Activar ESET LiveGuard**: la función ESET LiveGuard detecta nuevas amenazas nunca vistas mediante el análisis de su comportamiento en un entorno de pruebas. ESET LiveGuard puede activarse solo si ESET LiveGrid® está activado.

- **Enviar informes de bloqueo y datos de diagnóstico**: enviar datos de diagnóstico relacionados con ESET LiveGrid® como informes de bloqueo y volcados de la memoria de los módulos. Se recomienda mantenerlo activado para ayudar a ESET a diagnosticar problemas, mejorar productos y garantizar una mejor protección del usuario final.

- **Enviar estadísticas anónimas**: permita a ESET recopilar información sobre nuevas amenazas detectadas, como el nombre de la amenaza, la fecha y hora en las que se detectó, el método de detección y los metadatos asociados. la versión del producto y la configuración del mismo, incluida información sobre su sistema.

- **Correo electrónico de contacto (opcional)**: su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. No recibirá una respuesta de ESET, a no ser que sea necesaria más información.

## Envío de muestras

**Envío manual de muestras:** le permite enviar muestras a ESET manualmente desde el menú contextual, la Cuarentena o Herramientas.

**Envío automático de muestras detectadas**

Seleccione qué tipo de muestras se enviarán a ESET para que las analice y mejorar la detección futura (el tamaño de la muestra predeterminado máximo es de 64 MB). Están disponibles las opciones siguientes:

- **Todas las muestras detectadas**: todos los objetos detectados por el Motor de detección (incluidas aplicaciones potencialmente no deseadas cuando están activadas en los ajustes del análisis).

• **Todas las muestras excepto los documentos**: todos los objetos detectados excepto **Documentos** (consulte más abajo).

• **No enviar**: los objetos detectados no se enviarán a ESET.

**Envío automático de muestras sospechosas**

Estas muestras también se enviarán a ESET si el motor de detección no las detecta. Por ejemplo, las muestras que casi no se detectaron, o si uno de los módulos de protección de ESET Small Business Security considera que las muestras son sospechosas o tienen un comportamiento poco claro (el tamaño máximo predeterminado de la muestra es 64 MB).

• **Documentos**: incluye documentos de Microsoft Office o PDF con o sin contenido activo.

• **Eliminar documentos de los servidores de ESET**: define cuándo eliminar los documentos que ESET LiveGuard envió para su análisis.

Expandir para obtener una lista de todos los tipos de archivo de documentos incluidos

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

**Exclusiones**

Esta opción le permite excluir del envío archivos o carpetas (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Para excluir los archivos descargados de `descarga.dominio.com`, vaya a Configuración avanzada > **Protecciones** > **Protección en la nube** > **Envío de muestra** y haga clic en **Editar** junto a **Exclusiones**. Añada la exclusión `.descarga.dominio.com`.

**Tamaño máximo de las muestras (MB)**: define el tamaño máximo de las muestras enviadas automáticamente (1-64 MB).

## ESET LiveGuard

# Filtro de exclusión para protección en la nube

El filtro de exclusión le permite excluir del envío de muestras determinados archivos o carpetas. Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivo más habituales (como .doc, etc.) se excluyen de forma predeterminada.

Esta función resulta útil para, por ejemplo, excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo.

Para excluir archivos descargados de download.domain.com, haga clic en Configuración avanzada > **Protecciones** > **Protección en la nube** > **Envío de muestras** > **Exclusiones** y agregue la exclusión *download.domain.com*.

# ESET LiveGuard

ESET LiveGuard es una función que agrega una capa de protección basada en la nube diseñada específicamente para mitigar las amenazas desconocidas.

Cuando esta función está activada, las muestras sospechosas que aún no se han confirmado como maliciosas y pueden incluir malware se envían automáticamente a la nube de ESET. Las muestras enviadas se ejecutan en un entorno de pruebas y nuestros motores de detección de malware avanzados las evalúan. Las muestras maliciosas o los correos electrónicos de spam sospechosos se envían a ESET LiveGrid®. Los archivos adjuntos de correo electrónico se gestionan de forma independiente y pueden enviarse a ESET LiveGuard. Puede definir el alcance de los archivos enviados y el periodo de retención de archivos en la nube de ESET. Los documentos y los archivos PDF con contenido activo (macros, JavaScript) no se envían de forma predeterminada.

ESET LiveGuard puede activarse o desactivarse en:

- Ventana principal del programa > **Configuración** > **Protección del ordenador**
- Configuración avanzada > **Protecciones** > **Protección en la nube**

Para acceder a la configuración avanzada de ESET LiveGuard, abra Configuración avanzada > **Protecciones** > **Protección en la nube** > **ESET LiveGuard**.

**Acción tras la detección**: define la acción que se debe realizar si la muestra analizada se evalúa como una amenaza.

**Protección proactiva**: permite o bloquea la ejecución de los archivos que está analizando ESET LiveGuard. Si un archivo es sospechoso, la protección proactiva bloquea su ejecución hasta que finaliza el análisis. La protección proactiva detecta los archivos de las siguientes fuentes:

- Archivos descargados con un navegador web compatible
- Archivos descargados de un cliente de correo
- Archivos extraídos de un archivo cifrado o no cifrado con una de las utilidades de archivos compatibles
- Archivos ejecutados y abiertos ubicados en un dispositivo extraíble

Consulte las aplicaciones compatibles en la tabla siguiente:

| Navegadores web | Clientes de correo | Utilidades de archivos | Dispositivos extraíbles |
|---|---|---|---|
| Internet Explorer | Microsoft Outlook | WinRAR | Unidad flash USB |
| Microsoft Edge | Mozilla Thunderbird | WinZIP | Disco duro USB |
| Chrome | Correo de Microsoft | Descompresor integrado de Microsoft Explorer | CD/DVD |
| Firefox | | 7zip | Disquete |
| Opera | | | Lector de tarjetas integrado |

| Navegadores web | Clientes de correo | Utilidades de archivos | Dispositivos extraíbles |
|---|---|---|---|
| Brave Navegador | | | |

> **Nota**
> La protección proactiva bloquea los archivos copiados con el Explorador de Windows de una ubicación excluida en una ubicación protegida, ya que ESET Small Business Security reconoce `explorer.exe` como una utilidad de archivos.

> Si la protección proactiva está configurada como **Bloquear ejecución hasta que se reciban los resultados del análisis** y desea desbloquear el archivo que se está analizando, haga clic con el botón derecho del ratón en el archivo y haga clic en **Desbloquear archivo analizado por ESET LiveGuard**.

**Tiempo máximo de espera para el resultado del análisis (min)**: define el tiempo tras el que se desbloquearán los archivos analizados, independientemente de si ha finalizado el análisis.

---

ESET LiveGuard le informará del estado del análisis mediante notificaciones. Consulte las notificaciones disponibles a continuación:

| Título de la notificación | Descripción |
|---|---|
| Archivo bloqueado debido al análisis | ESET LiveGuard Ha bloqueado el archivo. ESET LiveGuard analiza el archivo para garantizar que es seguro utilizarlo. Puede esperar o elegir una de las siguientes opciones:<br>• **Desbloquear el archivo**: desbloquea el archivo, pero el análisis continúa. Recibirá una notificación sobre el resultado. No se recomienda si no está garantizada la integridad del archivo.<br>• **Cambiar configuración**: abre la ventana Configuración de la protección del ordenador, donde puede desactivar ESET LiveGuard y su protección proactiva. |
| Archivo desbloqueado | El archivo ya no está bloqueado. El análisis continúa y recibirá una notificación sobre el resultado. Puede abrir el archivo. |
| Archivo aún en análisis | ESET LiveGuard necesita más tiempo para finalizar el análisis. En caso de ser necesario, puede abrir el archivo. |
| Amenaza eliminada | ESET LiveGuard ha finalizado el análisis y el archivo contenía una amenaza. Se ha desinfectado el archivo. |
| Archivo seguro de utilizar | ESET LiveGuard ha finalizado el análisis y es seguro utilizar el archivo. |

Si ESET LiveGuard no funciona correctamente, recibirá una notificación en la ventana principal del programa > **Información general**. Siga las instrucciones de la notificación para resolver el problema. Si no puede resolver el problema, póngase en contacto con el servicio de soporte técnico.

# Análisis de malware

Se puede acceder a la sección **Análisis de dispositivos** desde Configuración avanzada > **Análisis**. Le permite configurar los parámetros de análisis para los perfiles de análisis.

## Análisis a petición

**Perfil seleccionado**: un conjunto específico de parámetros usados por el análisis a petición. Para crear uno nuevo, haga clic en **Modificar** junto a **Lista de perfiles**. Consulte Perfiles de análisis si desea más información.

Después de seleccionar el perfil de escaneo, puede configurar las siguientes opciones:

**Objetos de análisis**: si solo desea analizar un objeto específico, puede hacer clic en **Editar** junto a **Objetos de análisis** y seleccionar una opción en la estructura de carpetas (árbol). Consulte Objetos de análisis si desea más información.

**Protección a petición y de aprendizaje automático**: puede configurar niveles de informes y protección para cada perfil de análisis. De forma predeterminada, los perfiles de análisis utilizan la misma configuración definida en la protección del sistema de archivos en tiempo real. Desactive el interruptor junto a **Usar configuración de protección en tiempo real** para configurar niveles de protección e informes personalizados. Consulte Protecciones para obtener una explicación detallada de los niveles de informes y protección.

**ThreatSense**: Opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

# Perfiles de análisis

Hay 4 perfiles de análisis predefinidos en ESET Small Business Security:

- **Análisis inteligente** – este es el perfil de análisis avanzado predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se han comprobado estaban desinfectados en un análisis anterior y no se han modificado desde ese análisis. Esto permite reducir el tiempo de análisis y la repercusión en la seguridad del sistema.

- **Análisis del menú contextual** – puede iniciar un análisis a petición de cualquier archivo desde el menú contextual. El perfil de análisis del menú contextual le permite definir la configuración del análisis que se utilizará cuando active el análisis de esta forma.

- **Análisis exhaustivo** – De forma predeterminada, el perfil de análisis exhaustivo no utiliza la optimización inteligente, por lo que no se excluye ningún archivo del análisis con este perfil.

- **Análisis del ordenador** – este es el perfil predeterminado que se utiliza en el análisis estándar del ordenador.

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Análisis a petición** > **Lista de perfiles** > **Editar**. En la ventana **Administrador de perfiles** encontrará el menú desplegable **Perfil seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

Supongamos que desea crear su propio perfil de análisis y parte de la configuración de **Análisis del ordenador** es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar la opción **Reparar la detección siempre**. Introduzca el nombre del nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione un perfil nuevo en el menú desplegable **Perfil seleccionado**, ajuste los demás parámetros según sus requisitos y haga clic en **Aceptar** para guardar el nuevo perfil.

# Objetos de análisis

En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos especificados por el perfil de análisis seleccionado.
- **Medios extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Selección personalizada**: cancela todas las selecciones anteriores.

La estructura (de árbol) de carpetas también contiene objetos de análisis específicos.

- **Memoria operativa**: analiza todos los procesos y datos que actualmente utiliza la memoria operativa.
- **Sectores de inicio/UEFI**: analiza los sectores de inicio y la UEFI en busca de malware. Puede obtener más información sobre el análisis UEFI en el glosario.
- **Base de datos de WMI**: analiza toda la base de datos de Windows Management Instrumentation (WMI), todos los espacios de nombres, todas las instancias de clase y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
- **Registro del sistema**: analiza todo el registro del sistema, todas las claves y todas las subclaves. Busca referencias a archivos infectados o malware incrustados como datos. Durante la desinfección de las detecciones, la referencia permanece en el registro para garantizar que no se pierda ningún dato importante.

Para ir rápidamente a un objeto de análisis (archivo o carpeta), escriba su ruta en el campo de texto que aparece debajo de la estructura de árbol. La ruta distingue entre mayúsculas y minúsculas. Para incluir el objeto en el análisis, marque su casilla de verificación en la estructura de árbol.

# Análisis en estado inactivo

Puede activar el análisis en estado inactivo en Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Análisis en estado inactivo**.

## Análisis en estado inactivo

Active el interruptor situado junto a **Activar el análisis de estado inactivo** para activar esta función. Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis silencioso del ordenador en todas las unidades locales.

De forma predeterminada, el análisis en estado inactivo no se ejecutará si el ordenador (portátil) funciona con batería. Para anular este ajuste, active el interruptor situado junto a **Ejecutar aunque el ordenador esté funcionando con la batería** en Configuración avanzada.

Active el interruptor situado junto a **Activar el registro de sucesos** de la configuración avanzada para guardar un informe del análisis del ordenador en la sección Archivos de registro (en la ventana principal del programa, haga clic en **Herramientas** > **Archivos de registro** y seleccione **Análisis del ordenador** en el menú desplegable **Registro**).

### Detección de estado inactivo

Consulte Activadores de la detección del estado inactivo para ver una lista completa de condiciones que se deben cumplir para activar el análisis de estado inactivo.

**ThreatSense**: Opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

## Detección de estado inactivo

Los ajustes de detección de estado inactivo se pueden configurar en Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Análisis de estado inactivo** > **Detección de estado inactivo**. Estos ajustes especifican un activador para el Análisis de estado inactivo:

- **Pantalla apagada o con protector de pantalla**
- **Bloqueo del ordenador**
- **Cierre de sesión de usuario**

Utilice el interruptor de cada estado para activar o desactivar los distintos activadores de la detección del estado inactivo.

## Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o durante actualizaciones del motor de detección. Este análisis depende de las tareas y la configuración de Tareas programadas.

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos en el inicio del sistema** del Planificador de tareas. Para modificar su configuración, desplácese hasta **Herramientas** > **Tareas programadas**, haga clic en **Verificación de la ejecución de archivos en el inicio** y, a continuación, haga clic en **Modificar**. En el último paso, aparece la ventana Verificación de la ejecución de archivos en el inicio. Para obtener instrucciones detalladas acerca de la creación y gestión de tareas del Planificador de tareas, consulte Creación de tareas nuevas.

**ThreatSense**: Opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

# Comprobación de la ejecución de archivos en el inicio

Al crear una tarea programada de comprobación de archivos en el inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Analizar destinos** especifica la profundidad de análisis de los archivos ejecutados al iniciar el sistema basado en un sofisticado algoritmo. Los archivos se organizan en orden descendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrados** (se analiza el mayor número de archivos)
- **Archivos usados pocas veces**
- **Archivos usados ocasionalmente**
- **Archivos usados frecuentemente**
- **Solo los archivos usados con más frecuencia** (se analiza el menor número de archivos)

También se incluyen dos grupos específicos:

- **Archivos ejecutados antes del inicio de sesión del usuario**: contiene archivos de ubicaciones a las que se puede tener acceso sin que el usuario haya iniciado sesión (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, notificación del registro de Windows, entradas del Planificador de tareas de Windows, archivos dll conocidos, etc.).
- **Archivos en ejecución después del registro del usuario**: contiene archivos de ubicaciones a las que solo se puede tener acceso cuando el usuario se ha registrado (incluye archivos que solo ejecuta un usuario específico, generalmente los archivos de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se analizan son fijas para cada grupo de los anteriores. Si elige una profundidad de análisis inferior para los archivos ejecutados al iniciar el sistema, los archivos no analizados se analizarán cuando se abran o se ejecuten.

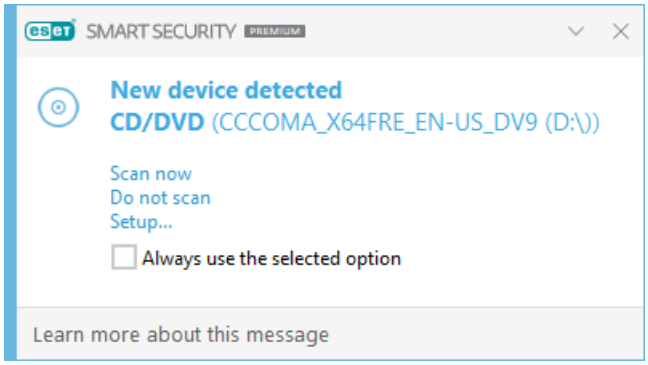
**Prioridad de análisis**: el nivel de prioridad empleado para determinar cuándo se iniciará un análisis:

- **Cuando el procesador esté desocupado**: la tarea se ejecutará solo cuando el sistema esté inactivo.
- **Muy baja**: cuando la carga del sistema es la más baja posible.
- **Baja**: con poca carga del sistema.
- **Normal**: con carga media del sistema.

# Unidades extraíbles

ESET Small Business Security permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática cuando se insertan en un ordenador. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Cuando se inserta un medio extraíble y se establece **Mostrar las opciones de análisis** en Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Medios extraíbles**, aparece la siguiente ventana:




Opciones de este cuadro de diálogo:

- **Analizar ahora**: activa el análisis del medio extraíble.
- **No analizar**: no se analizarán los medios extraíbles.
- **Configuración**: abre la configuración avanzada.
- **Utilizar siempre la opción seleccionada**: cuando se seleccione esta opción, se realizará la misma acción la próxima vez que se introduzca un medio extraíble.

Además, ESET Small Business Security presenta funciones de control de dispositivos, lo que le permite definir reglas para el uso de dispositivos externos en un ordenador dado. Encontrará más detalles sobre el control de dispositivos en la sección Control de dispositivos.

---

Para acceder a los ajustes del análisis de medios extraíbles, abra Configuración avanzada > **Análisis** > **Análisis de dispositivos** > **Medios extraíbles**.

**Acción que debe efectuarse cuando se inserten medios extraíbles**: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el ordenador (CD, DVD o USB). Elija la acción deseada al insertar un medio extraíble en un ordenador:

- **No analizar**: no se realizará ninguna acción y no se abrirá la ventana **Nuevo dispositivo detectado**.
- **Análisis automático del dispositivo**: se realizará un análisis del ordenador del medio extraíble insertado.
- **Mostrar las opciones de análisis**: abre la sección de configuración de **medios extraíbles**.

# Protección de documentos

La característica de protección de documentos analiza los documentos de Microsoft Office antes de que se abran y los archivos descargados automáticamente con Internet Explorer como, por ejemplo, elementos de Microsoft ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección en tiempo real del sistema de archivos, y se puede desactivar para mejorar el rendimiento en sistemas que no gestionan a un volumen elevado de documentos de Microsoft Office.

Para activar Protección de documentos, abra Configuración avanzada > **Protecciones** > **Protección de documentos** y haga clic en el interruptor situado junto a **Activar la protección de documentos**.

**ThreatSense**: Opciones de configuración avanzada, como las extensiones de archivo que desea controlar y los métodos de detección utilizados. Consulte ThreatSense para obtener más información.

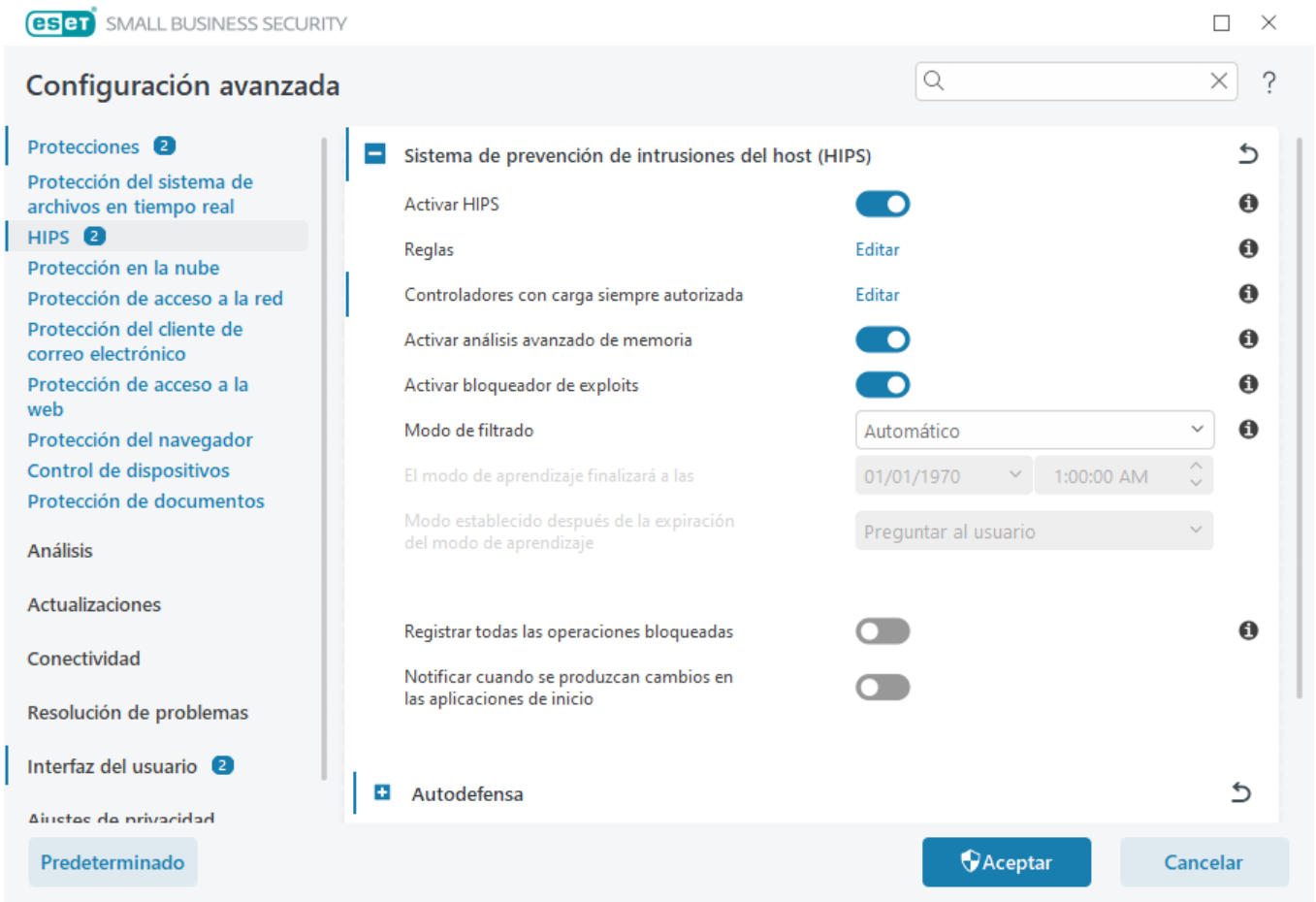
Esta función se activa mediante aplicaciones que utilizan Microsoft Antivirus API (por ejemplo, Microsoft Office 2000 y posteriores o Microsoft Internet Explorer 5.0 y posteriores).

# HIPS: Sistema de prevención de intrusiones del host

Solo debe modificar la configuración de HIPS si es un usuario experimentado. Una configuración incorrecta de los parámetros de HIPS puede provocar inestabilidad en el sistema.

**HIPS** protege el sistema frente a malware y actividad no deseada que intenten menoscabar la seguridad del dispositivo. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos; solo supervisa los procesos que se ejecutan dentro del sistema operativo.

Puede configurar los ajustes del HIPS en Configuración avanzada > **Protecciones** > **HIPS** > **Sistema de prevención de intrusiones del host**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal de ESET Small Business Security, dentro de **Configuración** > **Protección del ordenador**.



## Sistema de prevención de intrusiones del host (HIPS)

**Activar HIPS**: HIPS está activado de forma predeterminada en ESET Small Business Security. Si desactiva HIPS, se desactivarán las demás características de HIPS, como Bloqueador de exploits.

**Activar la Autodefensa**: ESET Small Business Security utiliza la tecnología de **Autodefensa** integrada como parte del HIPS para impedir que software malicioso dañe o desactive su protección antivirus y antiespía. La autodefensa evita la manipulación de procesos, claves de registro y archivos cruciales del sistema y de ESET.

**Activar servicio protegido**: activa la protección para ESET Service (ekrn.exe). Cuando está activado, el servicio se inicia como un proceso de Windows protegido para defenderle de ataques de malware.

**Activar análisis de memoria avanzado**: funciona en combinación con Bloqueador de exploits para reforzar la protección contra malware diseñado para evitar su detección mediante productos antimalware gracias al uso de ofuscación o cifrado. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

**Activar bloqueo de exploits**: se ha diseñado para fortalecer los tipos de aplicaciones que sufren más ataques, como navegadores, lectores de PDF, clientes de correo electrónico y componentes de MS Office. El bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

## Análisis profundo de inspección de comportamiento

**Habilitar Análisis profundo de inspección de comportamiento**: es otra capa de protección que funciona como parte de la función HIPS. Esta extensión del HIPS analiza el comportamiento de todos los programas que se ejecutan en el ordenador y le advierte si el comportamiento del proceso es malicioso.

Las Exclusiones del HIPS del Análisis profundo de inspección de comportamiento le permiten excluir procesos del análisis. Para garantizar que se analicen todos los procesos en busca de posibles amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario.

## Protección contra ransomware

**Activar protección contra ransomware**: es otra capa de protección que funciona como parte de la característica HIPS. Para que la protección contra ransomware funcione, debe tener activado el sistema de reputación ESET LiveGrid®. Más información sobre este tipo de protección.

**Activar Intel® Threat Detection Technology**: ayuda a detectar ataques de ransomware mediante la telemetría de la CPU Intel exclusiva para aumentar la eficacia de detección, reducir las alertas de falsos positivos y ampliar la visibilidad para capturar técnicas de evasión avanzadas. Consulte los procesadores compatibles.

## Configuración de HIPS

El **Modo de filtrado** se puede realizar en uno de los siguientes modos:

| Modo de filtrado | Descripción |
|---|---|
| **Modo automático** | Las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema. |
| **Modo inteligente** | Solo se informará al usuario de los sucesos muy sospechosos. |
| **Modo interactivo** | El usuario debe confirmar las operaciones. |

| Modo de filtrado | Descripción |
| --- | --- |
| **Modo basado en reglas** | Bloquea todas las operaciones no definidas por una regla específica que las permita. |
| **Modo de aprendizaje** | Las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de **reglas del HIPS**, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el **Modo de aprendizaje** en el menú desplegable **Modo de filtrado**, el ajuste **El modo de aprendizaje finalizará a las** estará disponible. Seleccione el periodo de tiempo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada se le pedirá que modifique las reglas creadas por el HIPS mientras estaba en modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje. |

**Modo establecido tras conocer la caducidad del modo**: seleccione el modo de filtrado que se utilizará cuando caduque el modo de aprendizaje. Tras el vencimiento, la opción **Preguntar al usuario** requiere privilegios administrativos para realizar un cambio en el modo de filtrado de HIPS.

El sistema HIPS supervisa los sucesos del sistema operativo y reacciona en consecuencia basándose en reglas similares a las que utiliza el cortafuegos. Haga clic en **Editar** junto a **Reglas** para abrir el editor de **reglas de HIPS**. En la ventana de reglas de HIPS puede seleccionar, agregar, editar o quitar reglas. Puede obtener más información sobre la creación de reglas y las operaciones de HIPS en Editar una regla de HIPS.

# Exclusiones del HIPS

Las exclusiones le permiten excluir procesos del Análisis profundo de inspección de comportamiento que ofrece el HIPS.

Para editar exclusiones de HIPS, abra Configuración avanzada > **Protecciones** > **HIPS** > **Sistema de prevención de intrusiones del host (HIPS)** > **Inspección profunda del comportamiento** > **Exclusiones** > **Editar**.

> No se debe confundir con Extensiones de archivo excluidas, Exclusiones de detección, Exclusiones de rendimiento ni Exclusiones de procesos.

Para excluir un objeto, haga clic en **Agregar** e introduzca la ruta de acceso de un objeto o selecciónelo en la estructura de árbol. También puede Editar o Eliminar las entradas seleccionadas.

# Configuración avanzada de HIPS

Las opciones siguientes son útiles para depurar y analizar el comportamiento de una aplicación:

Controladores con carga siempre autorizada: los controladores seleccionados pueden cargarse siempre sea cual sea el modo de filtrado configurado, a menos que la regla del usuario los bloquee de forma explícita.

**Registrar todas las operaciones bloqueadas**: las operaciones bloqueadas se escribirán en el registro de HIPS. Utilice esta función solo para resolver problemas o cuando el equipo de soporte técnico de ESET lo solicite, ya que puede generar un archivo de registro muy grande y ralentizar su ordenador.

**Notificar cuando se produzcan cambios en las aplicaciones de inicio**: muestra una notificación en el escritorio cada vez que se agrega o se elimina una aplicación del inicio del sistema.

# Controladores con carga siempre autorizada

Los controladores que aparezcan en esta lista podrán cargarse siempre, sea cual sea el modo de filtrado de HIPS, a menos que una regla del usuario los bloquee de forma específica.

**Agregar**: agrega un nuevo controlador.

**Modificar**: modifica el controlador seleccionado.

**Quitar**: quita un controlador de la lista.

**Restablecer**: carga de nuevo una serie de controladores del sistema.

Haga clic en **Restablecer** si no desea incluir los controladores que ha agregado manualmente. Esto puede resultar útil si ha agregado varios controladores y no puede eliminarlos de la lista manualmente.

Tras la instalación, la lista de controladores está vacía. ESET Small Business Security rellena la lista automáticamente a medida que pasa el tiempo.

# Ventana interactiva de HIPS

La ventana de notificación de HIPS le permite crear una regla basada en nuevas acciones que detecta HIPS y, a continuación, definir las condiciones en las que se permitirá o bloqueará esa acción.

Las reglas creadas en la ventana de notificación se consideran equivalentes a las reglas creadas manualmente. Una regla creada en una ventana de notificación puede ser menos específica que la regla que desencadenó esa ventana de diálogo. Esto significa que, después de crear una regla en el cuadro de diálogo, la misma operación puede desencadenar la misma ventana. Si desea obtener más información, consulte Prioridad de las reglas de HIPS.

Si la acción predeterminada para una regla es **Preguntar siempre**, se mostrará una ventana de diálogo cada vez que se desencadene la regla. Puede seleccionar **Bloquear** o **Permitir** la operación. Si no selecciona una acción en el tiempo indicado, se seleccionará una nueva acción basada en las reglas.

**Recordar hasta el cierre de la aplicación** provoca que se use la acción (**Permitir/Bloquear**) hasta que se cambien las reglas o el modo de filtrado, se actualice el módulo HIPS o se reinicie el sistema. Después de cualquiera de estas tres acciones, las reglas temporales se eliminarán.

La opción **Crear regla y recordar permanentemente** creará una nueva regla de HIPS que podrá modificarse más tarde en la sección Gestión de reglas de HIPS (requiere privilegios de administración).

Haga clic en **Detalles** en la parte inferior para ver qué aplicación desencadena la operación, la reputación del archivo o el tipo de operación que debe permitir o bloquear.

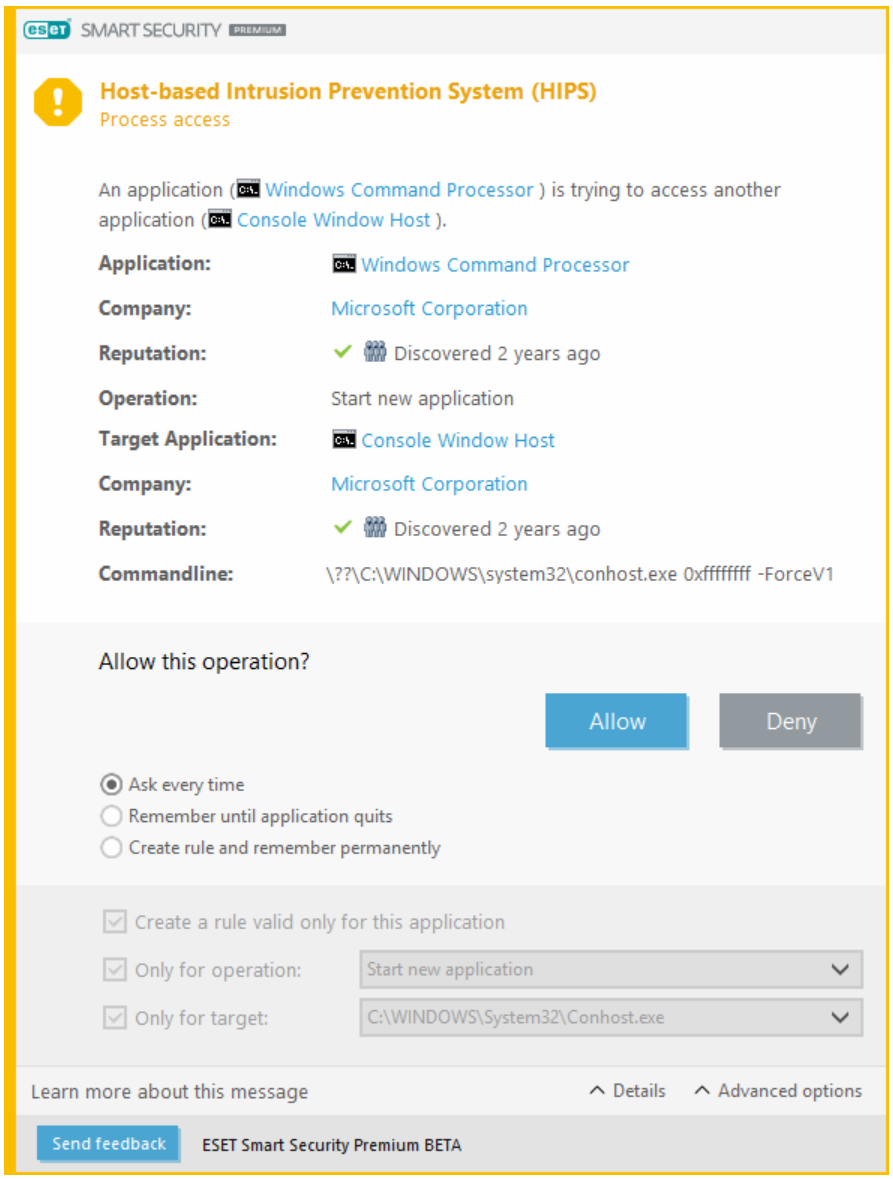
Para acceder a los ajustes de los parámetros más detallados de la regla, haga clic en **Opciones avanzadas**. Las siguientes opciones están disponibles si selecciona **Crear regla y recordar permanentemente**:

- **Crear una regla válida solo para esta aplicación**: si desactiva esta casilla de verificación, la regla se creará para todas las aplicaciones de origen.
- **Solo para la operación**: seleccione las operaciones de archivo/aplicación/registro de la regla. Consulte las

descripciones de todas las operaciones de HIPS.

- **Solo para el destino**: seleccione los destinos de archivo/aplicación/registro de la regla.

> **¿Infinitas notificaciones de HIPS?**
> Para que dejen de aparecer las notificaciones, cambie el modo de filtrado a **Automático** en Configuración avanzada > **Protecciones** > **HIPS** > **Sistema de prevención de intrusiones del host (HIPS)**.



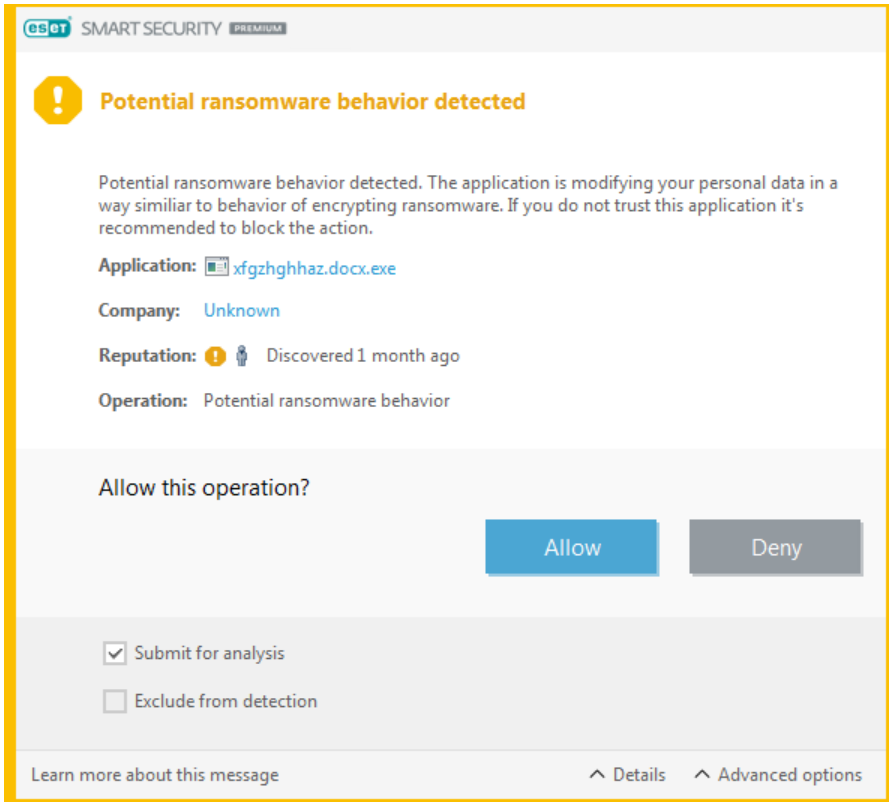

# Modo de aprendizaje finalizado

El modo de aprendizaje crea y guarda reglas automáticamente. Puede comprobar todas las reglas creadas en la configuración de reglas de HIPS. Este modo se utiliza mejor para la configuración inicial de HIPS, pero solo debe mantenerse activado durante un breve período de tiempo. No es necesaria la intervención del usuario, pues ESET Small Business Security guarda las reglas según los parámetros predefinidos.

Cambie al modo **interactivo** o al **modo basado en reglas** después de que se hayan creado todas las reglas para los procesos necesarios que se ejecutan en el sistema operativo para evitar riesgos de seguridad. Puede posponer esta decisión si no desea cambiar la configuración.

# Se ha detectado un comportamiento potencial de ransomware

Esta ventana interactiva aparecerá cuando se detecte un comportamiento potencial de ransomware. Puede seleccionar **Bloquear** o **Permitir** la operación.




Haga clic en **Detalles** para ver parámetros de detección concretos. La ventana de diálogo le permite **Enviar para su análisis** o **Excluir de la detección**.

Para que la protección contra ransomware funcione correctamente, ESET LiveGrid® debe estar activado.

# Gestión de reglas de HIPS

Esta es una lista de reglas del sistema HIPS agregadas automáticamente o definidas por el usuario. Encontrará más información sobre la creación de reglas y el funcionamiento del HIPS en el capítulo Configuración de regla de HIPS. Consulte también Principio general de HIPS.

## Columnas

**Regla**: nombre de la regla definido por el usuario o seleccionado automáticamente.

**Activado**: desactive el interruptor si desea conservar la regla en la lista, pero no desea utilizarla.

**Acción**: la regla especifica la acción (**Permitir**, **Bloquear** o **Preguntar**) que debe realizarse cuando se cumplen las condiciones.

**Orígenes**: la regla solo se utilizará si una aplicación activa el suceso.

**Objetos**: la regla solo se usará si la operación está relacionada con un archivo, una aplicación o una entrada del registro específicos.

**Registro de severidad**: si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.

**Notificar**: cuando se activa un suceso se abre una ventana notificación pequeña en la esquina inferior derecha.

## Elementos de control

**Agregar**: crea una nueva regla.

**Modificar**: le permite modificar las entradas seleccionadas.

**Eliminar**: quita las entradas seleccionadas.

## Prioridad de las reglas de HIPS

No hay opciones para ajustar el nivel de prioridad de las reglas de HIPS con los botones arriba/abajo (como sí puede hacerse con las Reglas del cortafuegos, donde las reglas se ejecutan de arriba a abajo).

- Todas las reglas que cree tendrán la misma prioridad
- Cuanto más específica sea la regla, mayor será su prioridad (por ejemplo, la regla para una aplicación específica tiene más prioridad que la regla para todas las aplicaciones)
- Internamente, HIPS contiene reglas de mayor prioridad a las que usted no puede acceder (por ejemplo, no puede anular las reglas de Autodefensa definidas)
- Si crea una regla que podría bloquear su sistema operativo, dicha regla no se aplicará (tendrá la prioridad más baja)

# Editar una regla de HIPS

En primer lugar, consulte Gestión de reglas de HIPS.

**Nombre de la regla**: nombre de la regla definido por el usuario o seleccionado automáticamente.

**Acción**: especifica la acción (**Permitir**, **Bloquear** o **Preguntar**) que debe realizarse si se cumplen las condiciones.

**Operaciones afectadas**: debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se utilizará para este tipo de operación y para el destino seleccionado.

**Activado**: desactive el interruptor si desea conservar la regla en la lista, pero no aplicarla.

**Registro de severidad**: si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.

**Notificar al usuario**: cuando se activa un suceso, se abre una ventana de notificación pequeña en la esquina inferior derecha.

La regla consta de partes que describen las condiciones que activan esta regla:

**Aplicaciones de origen**: la regla solo se utilizará si esta aplicación activa el suceso. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

**Archivos de destino**: la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todos los archivos** en el menú desplegable para agregar todas los archivos.

**Aplicaciones**: la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

**Entradas del registro**: la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Entradas especificadas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede hacer clic en **Abrir editor del registro** para seleccionar una clave del registro. Además, puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

> Algunas operaciones de reglas específicas predefinidas por HIPS no se pueden bloquear y se permiten de forma predeterminada. Además, HIPS no supervisa todas las operaciones del sistema; HIPS supervisa las operaciones que se pueden considerar inseguras.

Descripción de las operaciones importantes:

## Operaciones del archivo

- **Eliminar archivo**: la aplicación solicita permiso para eliminar el archivo objetivo.
- **Escribir en archivo**: la aplicación solicita permiso para escribir en el archivo objetivo.
- **Acceso directo al disco**: la aplicación está intentando realizar una operación de lectura o escritura en el disco de una forma no convencional que burlará los procedimientos habituales de Windows. Esto puede provocar la modificación de archivos sin la aplicación de las reglas correspondientes. Esta operación puede estar provocada por un código malicioso que intente evadir el sistema de detección, un software de copia de seguridad que intente realizar una copia exacta de un disco o un gestor de particiones que intente reorganizar los volúmenes del disco.
- **Instalar enlace global**: hace referencia a la activación de la función SetWindowsHookEx desde la biblioteca MSDN.
- **Cargar controlador**: instalación y carga de controladores en el sistema.

## Operaciones de la aplicación

- **Depurar otra aplicación**: conexión de un depurador al proceso. Durante el proceso de depuración de una aplicación es posible ver y modificar muchos aspectos de su comportamiento, así como acceder a sus datos.
- **Interceptar sucesos de otra aplicación**: la aplicación de origen está intentando capturar sucesos dirigidos a una aplicación concreta (por ejemplo un registrador de pulsaciones que intenta capturar sucesos del navegador).

• **Terminar/suspender otra aplicación**: suspende, reanuda o termina un proceso (se puede acceder a esta operación directamente desde el Process Explorer o el panel Procesos).

• **Iniciar una aplicación nueva**: inicia aplicaciones o procesos nuevos.

• **Modificar el estado de otra aplicación**: la aplicación de origen está intentando escribir en la memoria de la aplicación de destino o ejecutar código en su nombre. Esta función puede ser de utilidad para proteger una aplicación fundamental mediante su configuración como aplicación de destino en una regla que bloquee el uso de esta operación.

## Operaciones del registro

• **Modificar la configuración de inicio**: cambios realizados en la configuración que definan las aplicaciones que se ejecutarán al iniciar Windows. Estos cambios se pueden buscar, por ejemplo, buscando la clave Run en el Registro de Windows.

• **Eliminar del registro**: elimina una clave del registro o su valor.

• **Cambiar el nombre de la clave del registro**: cambia el nombre de las claves del registro.

• **Modificar el registro**: crea valores nuevos para las claves del registro, modifica los valores existentes, mueve los datos en el árbol de la base de datos o configura los permisos de usuarios y grupos en las claves del registro.

Puede utilizar comodines, con determinadas restricciones, para especificar un destino. En las rutas de acceso al registro se puede utilizar el símbolo * (asterisco) en vez de una clave determinada. Por ejemplo *HKEY_USERS*\software* puede significar *HKEY_USER\.default\software*, pero no *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** no es una ruta válida para la clave del registro. Una ruta de la clave del registro que tenga * incluye "esta ruta, o cualquier ruta de cualquier nivel después del símbolo". Este es el único uso posible de los comodines en los destinos. Primero se evalúa la parte específica de una ruta de acceso y, después, la ruta que sigue al comodín (*).

Si crea una regla muy genérica, se mostrará una advertencia sobre este tipo de regla.

En el siguiente ejemplo, mostraremos cómo restringir comportamientos no deseados de una aplicación específica:

1. Asigne un nombre a la regla y seleccione **Bloquear** (o **Preguntar** si prefiere decidir más tarde) en el menú desplegable **Acción**.

2. Active el interruptor situado junto a **Notificar al usuario** para mostrar una notificación siempre que se aplique una regla.

3. Seleccione al menos una operación en la sección **Operaciones afectadas** a la que se le aplicará la regla.

4. Haga clic en **Siguiente**.

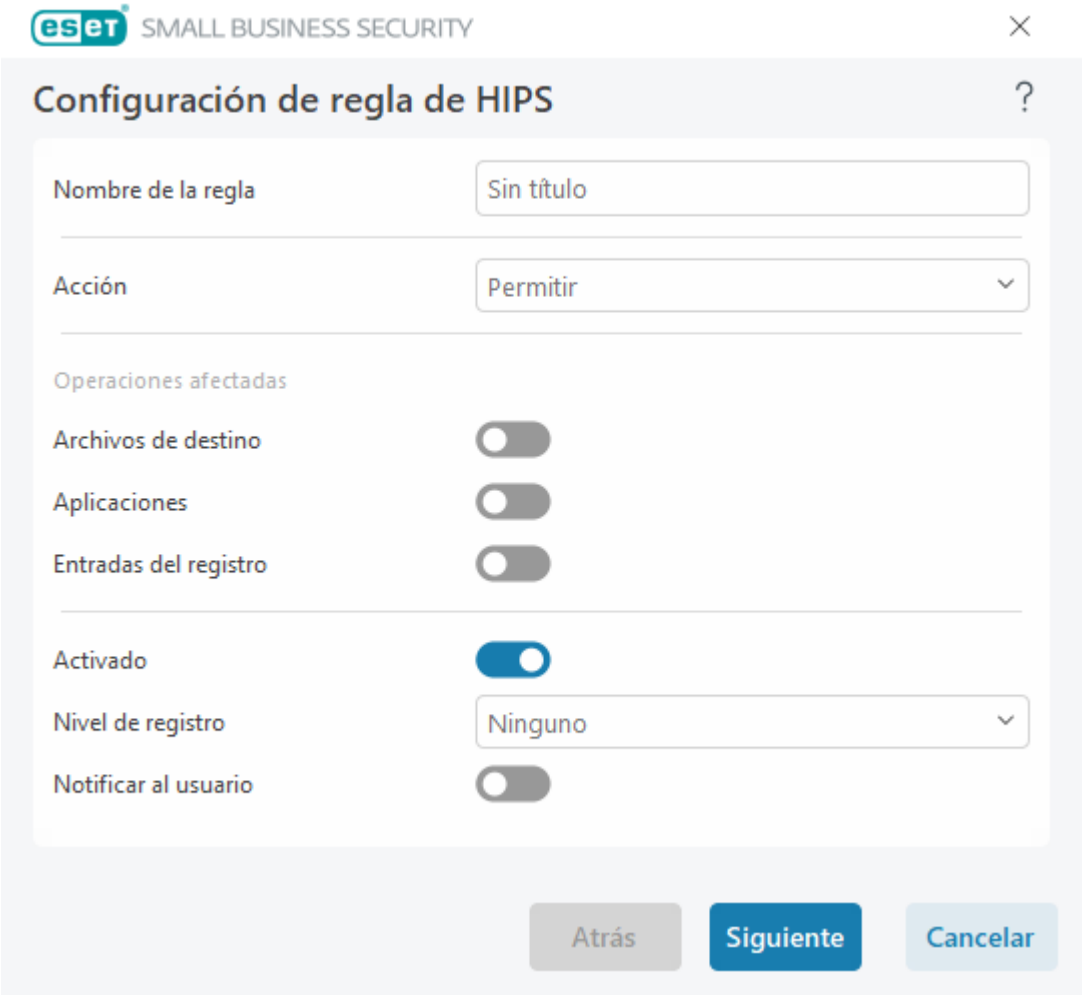
5. En la ventana **Aplicaciones de origen**, seleccione **Aplicaciones específicas** en el menú desplegable para aplicar la nueva regla a todas las aplicaciones que intenten realizar cualquiera de las operaciones de aplicación seleccionadas en las aplicaciones especificadas.

6. Haga clic en **Agregar** y, a continuación, en **…** para elegir una ruta de acceso de una aplicación específica y, a continuación, pulse **Aceptar**. Agregue más aplicaciones si lo prefiere.
Por ejemplo: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Seleccione la operación **Escribir en archivo**.

8. Seleccione **Todos los archivos** en el menú desplegable. Cuando una aplicación seleccionada en el paso anterior intente escribir en un archivo, se bloqueará dicho intento.

9. Haga clic en **Finalizar** para guardar la nueva regla.




# Agregar ruta de acceso de aplicación/registro para el HIPS

Haga clic en la opción **...** para seleccionar la ruta de acceso a la aplicación de un archivo. Si selecciona una carpeta, se incluirán todas las aplicaciones que se encuentren en esa ubicación.

La opción **Abrir editor del registro** iniciar el editor del registro de Windows (regedit). Si añade la ruta de acceso de un registro, introduzca la ubicación correcta en el campo **Valor**.

Ejemplos de ruta de acceso a un archivo o registro:

- *C:\Archivos de programa\Internet Explorer\iexplore.exe*

• *HKEY_LOCAL_MACHINE\system\ControlSet*

# Actualizaciones

Las opciones de configuración de la actualización están disponibles en Configuración avanzada > **Actualización**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización utilizados y sus datos de autenticación.

## Actualizaciones

El perfil de actualización que se está utilizando se muestra en el menú desplegable **Seleccionar perfil de actualización predeterminado**.

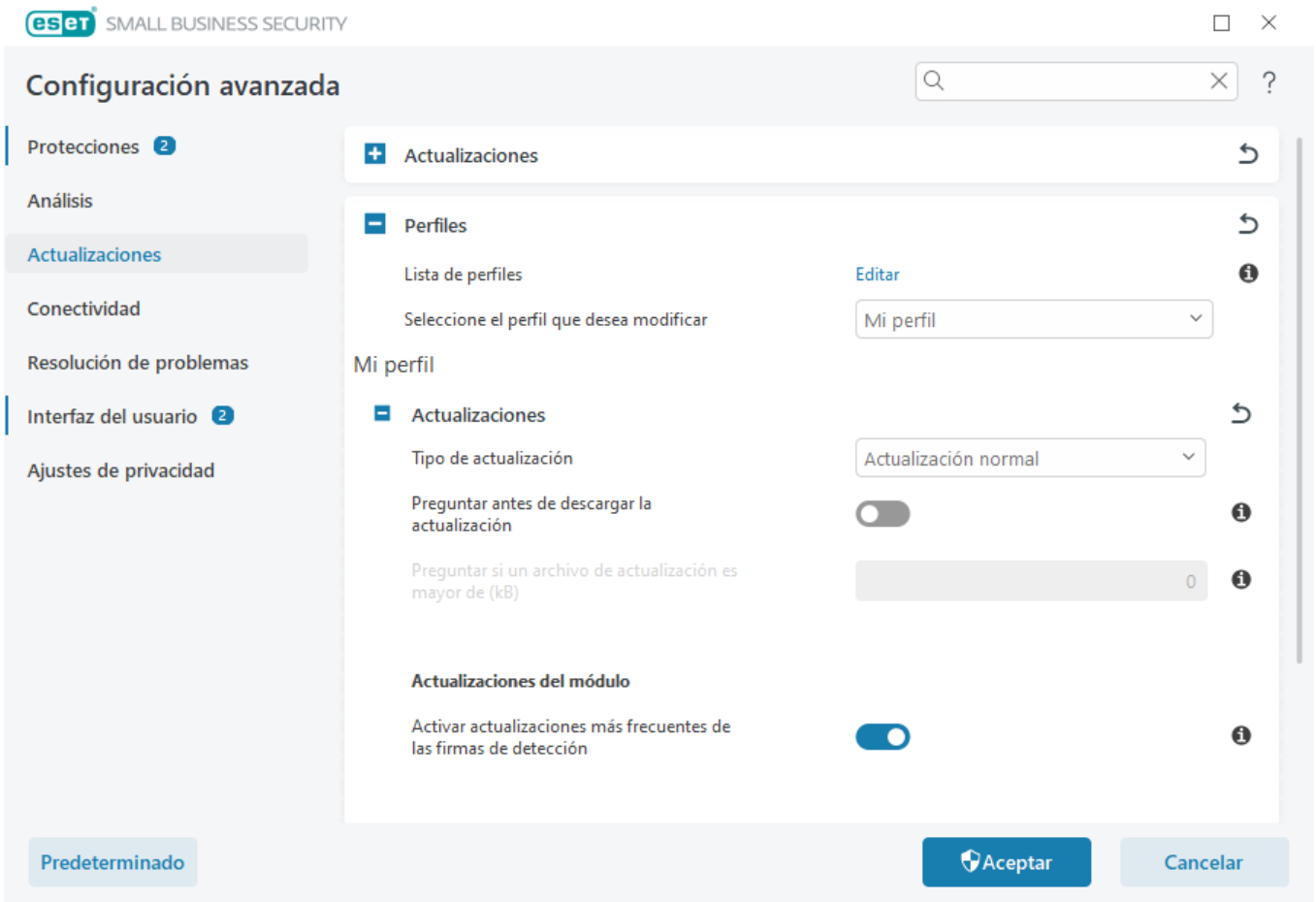
Para crear un nuevo perfil, consulte la sección Perfiles de actualización.

**Cambio automático de perfil**: permite asignar un perfil de actualización a un perfil de conexión de red específico.

Si tiene problemas al descargar actualizaciones de los motores de detección o módulos, haga clic en **Borrar** junto a **Borrar caché de actualización** para borrar la memoria caché/los archivos de actualización temporales.

## Reversión de módulos

Si sospecha que una nueva actualización del motor de detección o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido.



Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente todos los parámetros de actualización. Si utiliza un cortafuegos, asegúrese de que su programa de ESET goza de permiso para comunicarse con Internet (por ejemplo, comunicación HTTP).

## Perfiles

Se pueden crear perfiles de actualización para diferentes tareas y configuraciones de actualización. Estos perfiles son especialmente útiles para los usuarios móviles, que necesitan un perfil alternativo para las propiedades de conexión a Internet que cambian periódicamente.

El menú desplegable **Seleccione el perfil que desea modificar** muestra el perfil seleccionado actualmente y está configurado como **Mi perfil** de forma predeterminada. Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**.

## Actualizaciones

De forma predeterminada, el menú **Tipo de actualización** está definido en **Actualización normal** para garantizar que todos los archivos de actualización se descarguen automáticamente del servidor de ESET cuando la carga de red sea menor. Las actualizaciones de prueba (opción **Actualización de prueba**) son actualizaciones que han superado rigurosas pruebas internas y estarán pronto disponibles.

Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. No obstante, la actualización de prueba no siempre es estable, por lo que NO debe utilizarse en servidores de producción y estaciones de trabajo que requieran un elevado nivel de disponibilidad y estabilidad.

**Preguntar antes de descargar la actualización**: el programa mostrará una notificación en la que podrá confirmar o rechazar las descargas de archivos de actualización.

**Preguntar si un archivo de actualización es mayor de (kB)**: el programa mostrará un cuadro de diálogo de confirmación si el tamaño del archivo de actualización es mayor que el valor especificado. Si el tamaño del archivo de actualización se establece en 0 kB, el programa siempre mostrará un cuadro de diálogo de confirmación.

### Actualizaciones del módulo

**Activar actualizaciones más frecuentes de firmas de detección**: las firmas de detección se actualizarán en intervalos más cortos. Desactivar este ajuste puede afectar negativamente a la velocidad de detección.

### Actualizaciones del producto

**Actualizaciones de características de la aplicación**: instala automáticamente versiones nuevas de ESET Small Business Security.

## Opciones de conexión

Si desea utilizar un servidor proxy para descargar las actualizaciones, consulte la sección Opciones de conexión.

# Reversión de actualización

Si sospecha que un nuevo módulo del programa o una nueva actualización del motor de detección pueden ser inestables o estar dañados, puede revertir a la versión anterior y desactivar las actualizaciones temporalmente. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

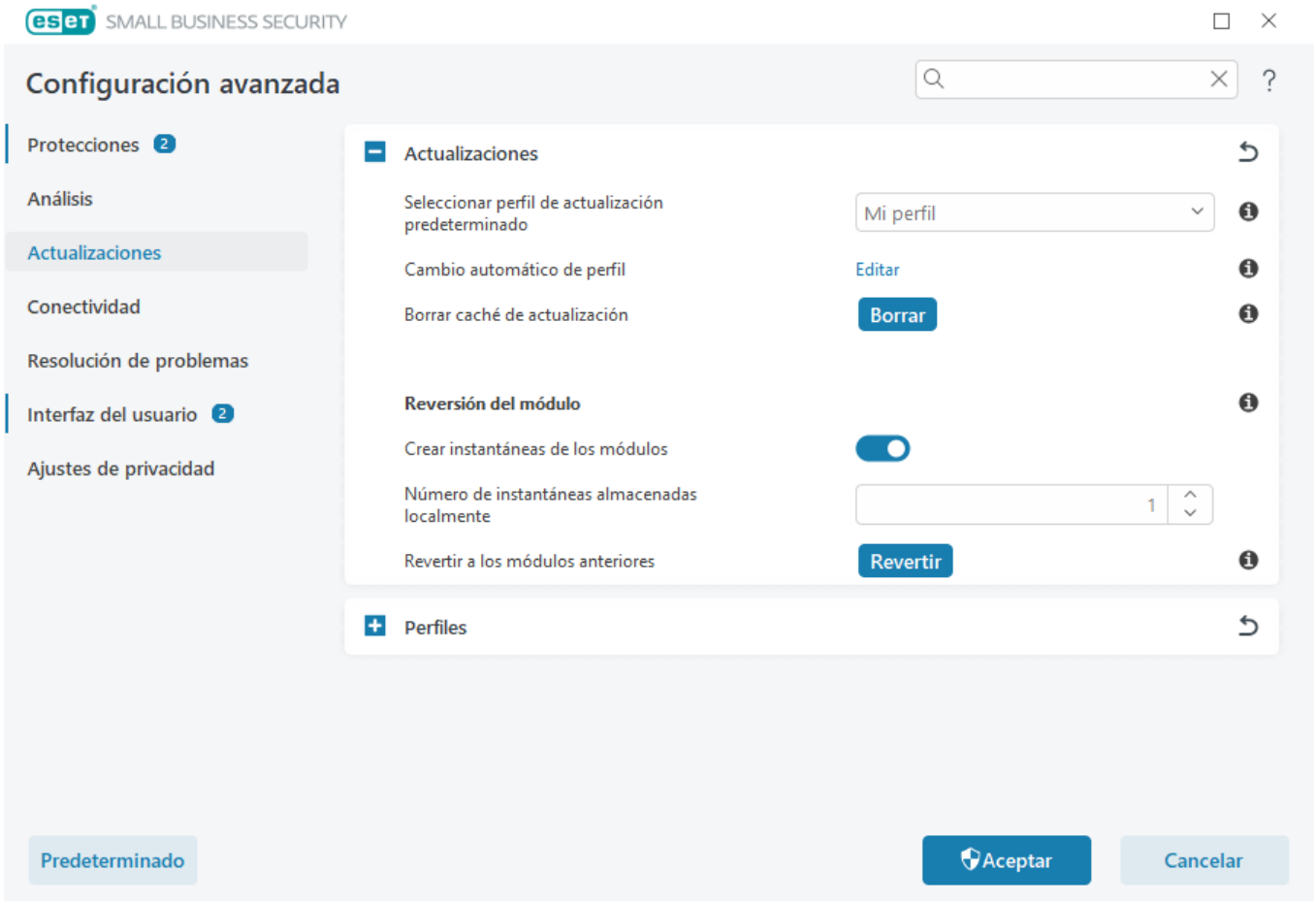
ESET Small Business Security registra instantáneas del motor de detección y los módulos del programa para usarlas con la función de reversión. Para crear instantáneas de la base de datos de virus, deje activada la opción **Crear instantáneas de los módulos**. Cuando la opción **Crear instantáneas de los módulos** está activada, se crea la primera instantánea durante la primera actualización. La siguiente se crea después de 48 horas. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas del motor de detección almacenadas.

> Cuando se alcanza la cantidad máxima de instantáneas (por ejemplo, tres), se sustituye la instantánea más antigua por una nueva cada 48 horas. ESET Small Business Security revierte las versiones de actualización del motor de detección y de los módulos del programa a la instantánea más antigua.

Si hace clic en **Revertir** en Configuración avanzada > **Actualizaciones** > **Actualizaciones**, deberá seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.


Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, ESET no recomienda que se seleccione esta opción.

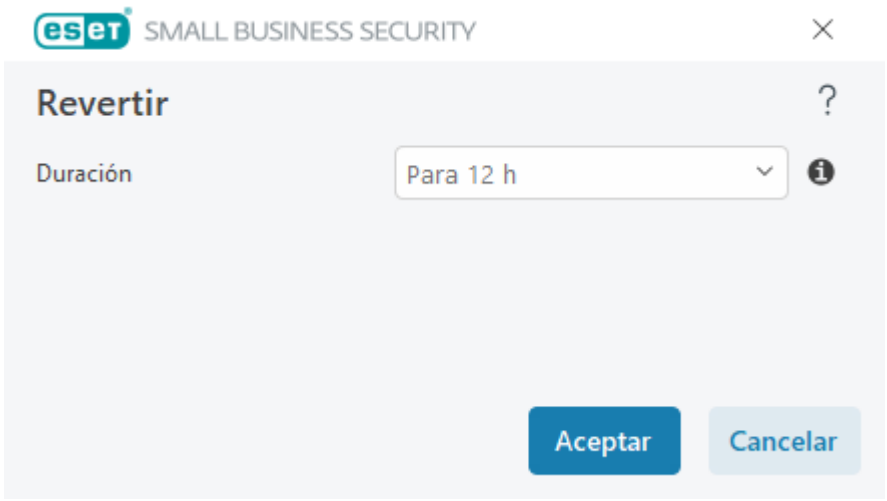
Si se lleva a cabo una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permitirán actualizaciones para el intervalo de tiempo seleccionado en el menú desplegable **Suspender actualizaciones**. La versión del motor de detección se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del equipo local.




Suponga que 22700 es el número de versión del motor de detección más reciente, y que 22698 y 22696 están almacenadas como instantáneas del motor de detección. Tenga en cuenta que 22697 no está disponible. En este ejemplo, el equipo se desactivó durante la actualización de 22697 y se puso a disposición de los usuarios una actualización más reciente antes de que se descargara 22697. Si el campo **Número de instantáneas almacenadas de forma local** es dos y hace clic en **Revertir**, el motor de detección (incluidos los módulos del programa) se restaura a la versión número 22696. Este proceso puede llevar cierto tiempo. Compruebe que la versión del motor de detección se haya degradado en la pantalla Actualización.

# Intervalo de tiempo de reversión

Si hace clic en **Revertir** en Configuración avanzada > **Actualizaciones** > **Actualizaciones**, deberá seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.




Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, ESET no recomienda que se seleccione esta opción.

# Actualizaciones del producto

La sección **Actualizaciones del producto** le permite instalar actualizaciones de características nuevas cuando están disponibles automáticamente.

Las actualizaciones de características de la aplicación presentan nuevas funciones o cambian las que ya existen de versiones anteriores. Se pueden realizar de manera automática, sin la intervención del usuario, o puede elegir que se le envíen notificaciones. Después de instalar la actualización de una característica de la aplicación, puede que sea necesario reiniciar el ordenador.

**Actualizaciones de características de la aplicación**: cuando esta opción está activada, las actualizaciones de las características de la aplicación se realizarán automáticamente.

# Opciones de conexión

Para acceder a las opciones de configuración del servidor proxy para un perfil de actualización específico, abra Configuración avanzada > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión**. Haga clic en el menú desplegable **Modo proxy** y seleccione una de las tres opciones siguientes:

- No usar servidor Proxy
- Conexión a través de un servidor Proxy específico
- Utilizar la configuración predeterminada

Seleccione **Usar la configuración global del servidor proxy** para utilizar la configuración del servidor proxy ya especificada en la sección Configuración avanzada > **Conectividad** > **Servidor proxy**.

Seleccione **No usar servidor Proxy** para especificar que no se utilice ningún servidor Proxy para actualizar ESET Small Business Security.

La opción **Conexión a través de un servidor proxy** debe seleccionarse si:

- Se utiliza un servidor proxy distinto del definido en Configuración avanzada > **Conectividad** para actualizar ESET Small Business Security. En esta configuración, la información del nuevo proxy se debe especificar en **Servidor proxy**: dirección, **Puerto** de comunicación (3128 de forma predeterminada), **Nombre de usuario** y **Contraseña** del servidor proxy, en caso de ser necesarios.

- La configuración del servidor proxy no se ha definido globalmente, pero ESET Small Business Security se conecta a un servidor proxy para las actualizaciones.

- El ordenador se conecta a Internet mediante un servidor Proxy. La configuración se obtiene de Internet Explorer durante la instalación del programa; no obstante, si se modifica (por ejemplo, al cambiar de proveedor de Internet), asegúrese de que la configuración del servidor proxy que aparece en esta ventana es la correcta. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

La configuración predeterminada del servidor Proxy es **Utilizar la configuración predeterminada**.

**Usar conexión directa si el proxy no está disponible**: si no puede accederse al proxy durante la actualización, se omitirá.

Los campos **Nombre de usuario** y **Contraseña** de esta sección son específicos del servidor proxy. Rellene estos campos solo si se requiere un nombre de usuario y una contraseña para acceder al servidor proxy. Únicamente debe completar estos campos si sabe que se necesita una contraseña para acceder a Internet a través de un servidor proxy.

# Protecciones

La protección protege contra ataques maliciosos al sistema mediante el control de las comunicaciones por Internet, el correo electrónico y los archivos. Por ejemplo, si se detecta un objeto clasificado como malware, se inicia la corrección. Las protecciones pueden eliminar este objeto bloqueándolo primero y, a continuación, desinfectándolo, eliminándolo o poniéndolo en cuarentena.

Para configurar las protecciones en detalle, abra Configuración avanzada > **Protecciones**.

Solo debe modificar Protecciones si es un usuario experimentado. Una configuración incorrecta de los ajustes puede provocar un menor nivel de protección.

En esta sección:

- Respuestas de detección
- Configuración de informes
- Configuración de la protección

---

## Respuestas de detección

Las respuestas de detección permiten configurar niveles de informes y protección para las siguientes categorías:

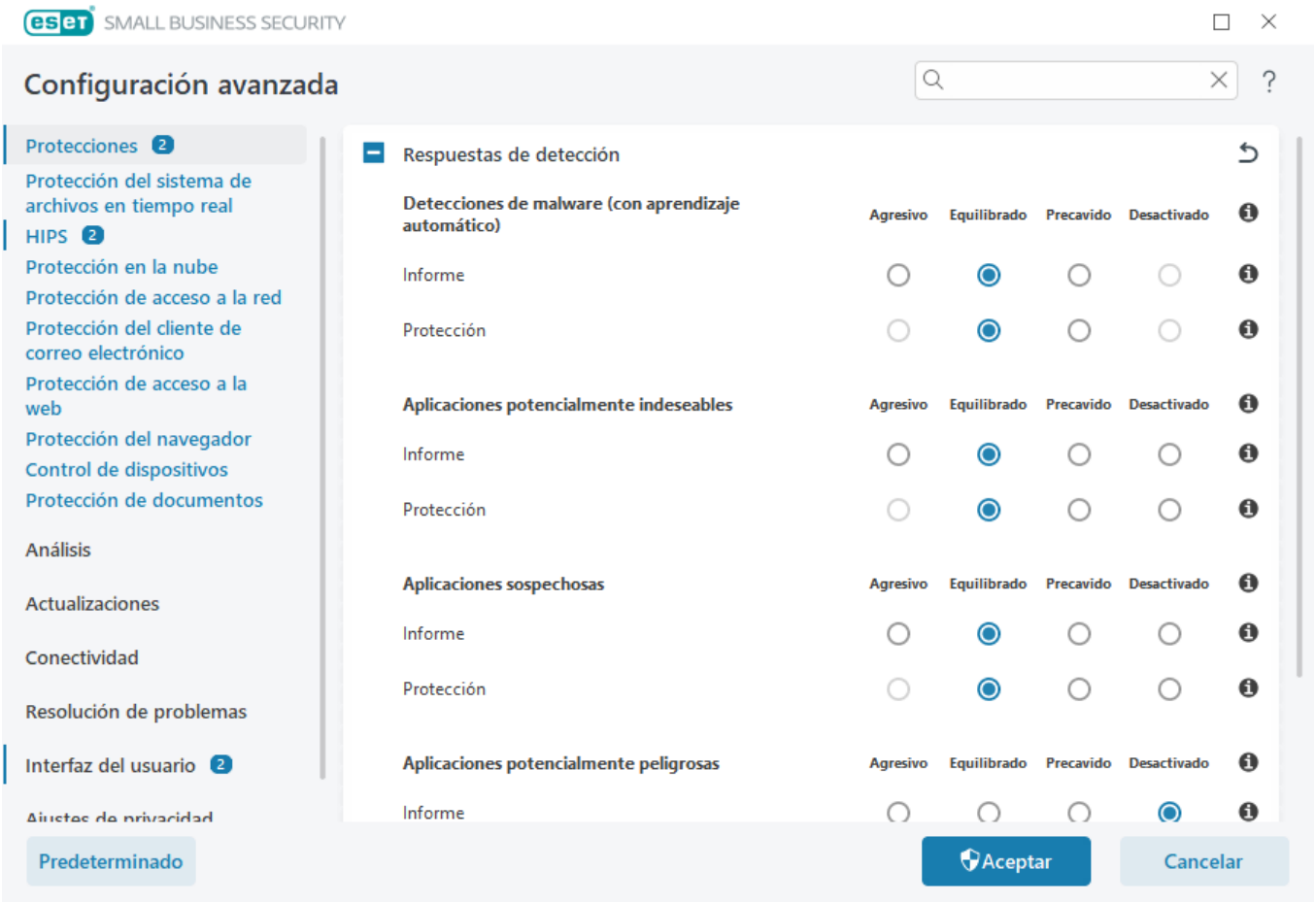
- **Detecciones de malware (con aprendizaje automático**: un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su ordenador. Sin embargo, el término "virus"

suele utilizarse de forma inadecuada. "Malware" (software malicioso) es un término más exacto. La detección de malware la realiza el módulo del motor de detección en combinación con el componente de aprendizaje automático. Puede obtener más información sobre estos tipos de aplicaciones en el Glosario.

- **Aplicaciones potencialmente indeseables**: el grayware, o aplicaciones potencialmente indeseables (PUA), es una amplia categoría de software no inequívocamente malicioso, al contrario de lo que sucede con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar software adicional indeseable, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas o esperadas por el usuario. Puede obtener más información sobre estos tipos de aplicaciones en el Glosario.

- Entre las **aplicaciones sospechosas** se incluyen los programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia aprovechan estos tipos de protectores para evitar que se detecte.

- **Aplicaciones potencialmente peligrosas**: hace referencia a software comercial legítimo que puede utilizarse con fines maliciosos. Entre los ejemplos de este tipo de aplicaciones potencialmente peligrosas (PUA) encontramos herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Puede obtener más información sobre estos tipos de aplicaciones en el Glosario.




## Protección mejorada

Aprendizaje automático avanzado forma ahora parte de las protecciones como capa avanzada de protección que mejora la detección con aprendizaje automático. Lea más información sobre este tipo de protección en el glosario.

# Configuración de informes

Cuando se produce una detección (por ejemplo, se encuentra una amenaza y se clasifica como malware), se registra información en el Registro de detecciones, y se producen Notificaciones en el escritorio si está configurado en ESET Small Business Security.

Se configura el umbral de informes para cada categoría (denominada "CATEGORÍA"):

1. Detecciones de malware
2. Aplicaciones potencialmente indeseables
3. Potencialmente peligrosas
4. Aplicaciones sospechosas

Se realizan informes con el motor de detección, incluido el componente de aprendizaje automático. Puede establecer un umbral de informes más alto que el umbral de protección actual. Estos ajustes de informes no influyen en la acción de bloquear, desinfectar o eliminar objetos.

Lea lo siguiente antes de modificar un umbral (o nivel) de informes de CATEGORÍA:

| Umbral | Explicación |
|---|---|
| **Agresivo** | Informes de CATEGORÍA configurados con la máxima sensibilidad. Se informa de más detecciones. El ajuste **Agresivo** pude identificar falsos positivos de CATEGORÍA. |
| **Equilibrado** | Informes de CATEGORÍA configurados como equilibrados. Este ajuste está optimizado para equilibrar el rendimiento y la precisión de las detecciones y el número de falsos positivos notificados. |
| **Precavido** | Informes de CATEGORÍA configurados para reducir al mínimo los falsos positivos a la vez que se mantiene un nivel de protección suficiente. Solo se informa de los objetos cuando la probabilidad es evidente y coincide con el comportamiento de CATEGORÍA. |
| **Desactivado** | Los informes de CATEGORÍA no están activos, y no se encuentran, notifican ni desinfectan detecciones de este tipo. Por lo tanto, este ajuste desactiva la protección frente a este tipo de detecciones.<br>Desactivado no está disponible para los informes de malware y es el valor predeterminado para las aplicaciones potencialmente peligrosas. |

Disponibilidad de los módulos de protección de ESET Small Business Security

La disponibilidad (activado o desactivado) de un módulo de protección de un umbral de CATEGORÍA seleccionado es la siguiente:

| | Agresivo | Equilibrado | Precavido | Desactivado* |
|---|---|---|---|---|
| Módulo de aprendizaje automático avanzado | ✓ (modo agresivo) | ✓ (modo conservador) | X | X |
| Módulo del motor de detección | ✔ | ✔ | ✔ | X |
| Otros módulos de protección | ✔ | ✔ | ✔ | X |

* No recomendado

Determinar versión del producto, versiones de los módulos del programa y fechas de compilación

1. Haga clic en **Ayuda y asistencia técnica** > **Acerca de ESET Small Business Security**.
2. En la pantalla **Acerca de**, la primera línea de texto muestra el número de versión de su producto ESET.
3. Haga clic en **Componentes instalados** para acceder a información sobre módulos específicos.

### Notas

Varias notas útiles a la hora de configurar un umbral apropiado para su entorno:

- El umbral **Equilibrado** es el recomendado para la mayoría de las configuraciones.
- Cuando más alto sea el umbral de informes, mayor será el número de detecciones, pero también será mayor la posibilidad de que se produzcan falsos positivos.
- Desde la perspectiva del mundo real, no se pueden garantizar el 100 % de detección ni el 0 % de falsos positivos.
- Mantenga ESET Small Business Security y sus módulos actualizados para optimizar el equilibrio entre rendimiento y precisión en la detección y el número de falsos positivos.

---

## Configuración de la protección

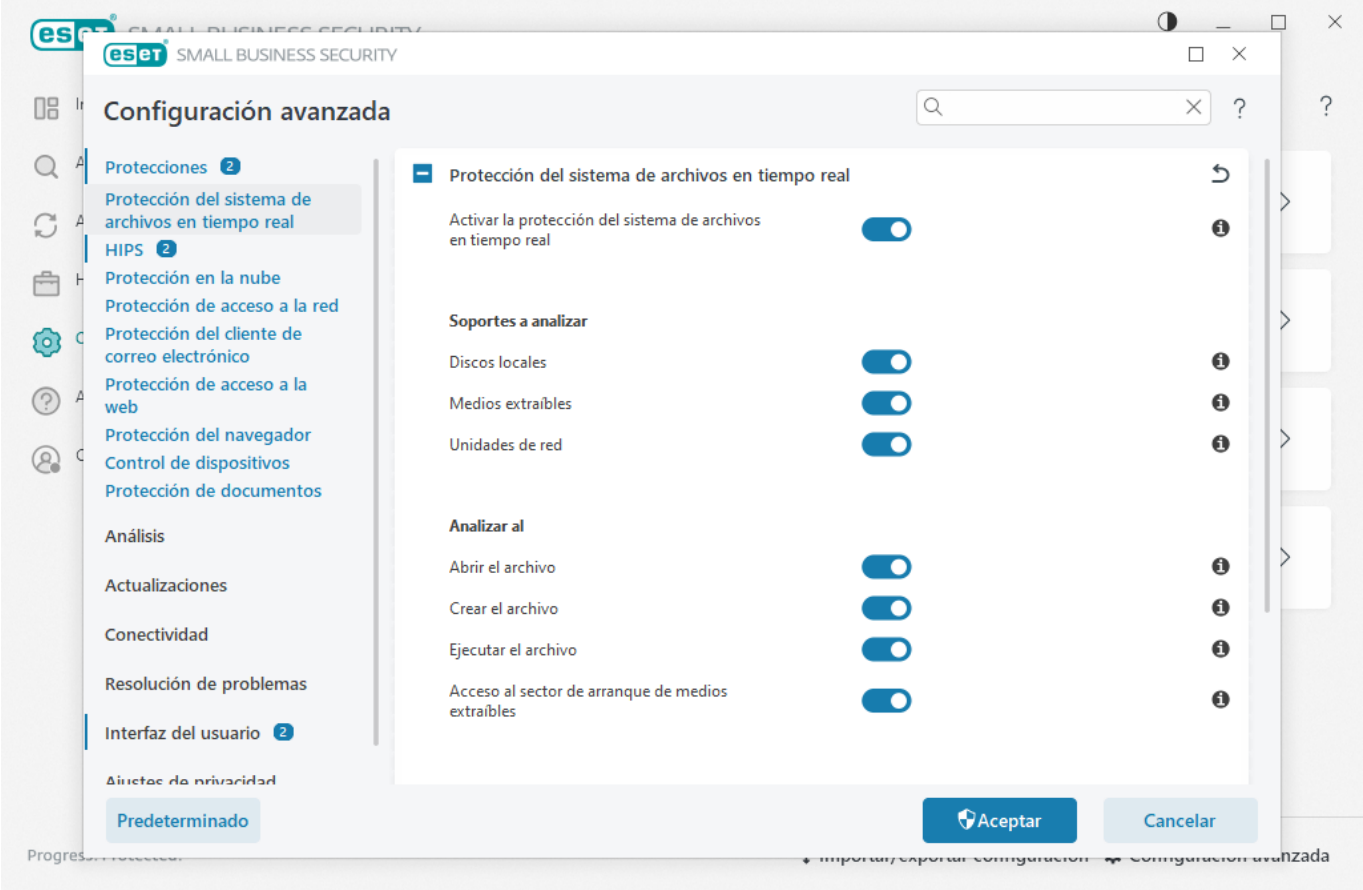
Si se informa de un objeto clasificado como CATEGORÍA, el programa bloquea el objeto y, a continuación, lo desinfecta, elimina o mueve a Cuarentena.

Lea lo siguiente antes de modificar un umbral (o nivel) de protección de CATEGORÍA:

| Umbral | Explicación |
|---|---|
| **Agresivo** | Las detecciones de nivel agresivo (o inferior) de las que se informa se bloquean, y se inicia la corrección automática (es decir, la desinfección). Este ajuste se recomienda cuando se han analizado todos los puntos de conexión con ajustes agresivos y se han agregado los falsos positivos a las exclusiones de detección. |
| **Equilibrado** | Las detecciones de nivel equilibrado (o inferior) se bloquean, y se inicia la corrección automática (es decir, la desinfección). |
| **Precavido** | Las detecciones de nivel precavido se bloquean, y se inicia la corrección automática (es decir, la desinfección). |
| **Desactivado** | Útil para identificar y excluir falsos positivos.<br>Desactivado no está disponible para la protección contra malware y es el valor predeterminado para las aplicaciones potencialmente peligrosas. |

# Protección del sistema de archivos en tiempo real

Protección del sistema de archivos en tiempo real controla todos los archivos del sistema para garantizar que no contengan código malicioso al abrirlos, crearlos o ejecutarlos.




La protección del sistema de archivos en tiempo real comienza de forma predeterminada cuando se inicia el sistema y proporciona un análisis ininterrumpido. No recomendamos desactivar **Activar la protección del sistema de archivos en tiempo real** en Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Protección del sistema de archivos en tiempo real**.

## Objetos a analizar

De forma predeterminada, se buscan posibles amenazas en todos los tipos de objetos:

- **Unidades locales**: analiza todos los discos duros del sistema (ejemplo: *C:*\, *D:*\).
- **Medios extraíbles**: analiza CD/DVD, almacenamiento USB, tarjetas de memoria, etc.
- **Unidades de red**: analiza todas las unidades de red asignadas (ejemplo: *H:*\ como *store04*) o las unidades de red de acceso directo (ejemplo: *store08*).

Recomendamos que esta configuración predeterminada se modifique solo en casos específicos como, por ejemplo, cuando el control de ciertos objetos ralentiza significativamente las transferencias de datos.

## Analizar al

De forma predeterminada, se analizan todos los archivos cuando se crean, se abren o se ejecutan. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador:

- **Abrir el archivo**: analiza cuándo se abre un archivo.

- **Crear el archivo**: analiza un archivo creado o modificado.
- **Ejecutar el archivo**: analiza cuándo se ejecuta un archivo.
- **Acceso al sector de inicio de medios extraíbles**: cuando se insertan en el dispositivo medios extraíbles que contienen un sector de inicio, el sector de inicio se analiza inmediatamente. Esta opción no activa el análisis de archivos de medios extraíbles. El análisis de archivos de medios extraíbles está en **Medios que se analizarán** > **Medios extraíbles**. Para que **Acceso al sector de inicio de medios extraíbles** funcione correctamente, mantenga activado **Sectores de inicio/UEFI** en ThreatSense.

## Exclusiones de procesos

Ver Exclusiones de procesos.

## ThreatSense

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y se activa con varios sucesos del sistema como, por ejemplo, cuando se accede a un archivo.

Si se utilizan métodos de detección con la tecnología **ThreatSense** (tal como se describe en la sección ThreatSense), la protección del sistema de archivos en tiempo real se puede configurar para que trate de forma diferente los archivos recién creados y los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se analizan de nuevo inmediatamente tras cada actualización del motor de detección. Este comportamiento se controla con la opción **Optimización inteligente**.

Si la opción **Optimización inteligente** está desactivada, se analizan todos los archivos cada vez que se accede a ellos. Para modificar esta configuración, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real**. Haga clic en **ThreatSense** > **Otros** y seleccione o anule la selección de **Activar la optimización inteligente**.

La protección del sistema de archivos en tiempo real también le permite configurar Parámetros adicionales de ThreatSense.

# Exclusiones de procesos

La característica Exclusiones de procesos le permite excluir procesos de aplicación de Protección del sistema de archivos en tiempo real. Para aumentar la velocidad de la copia de seguridad, la integridad de los procesos y la disponibilidad del servicio, se utilizan durante la copia de seguridad algunas técnicas que entran en conflicto con la protección contra malware a nivel de archivo. La única forma eficaz de evitar estas situaciones es desactivar el software antimalware. Al excluir un proceso específico (por ejemplo, un proceso de la solución de copia de seguridad), todas las operaciones de archivo atribuidas a dicho proceso excluido se ignoran y consideran seguras, lo que reduce al mínimo las interferencias con el proceso de copia de seguridad. Le recomendamos tener precaución al crear exclusiones: una herramienta de copia de seguridad excluida puede acceder a archivos infectados sin desencadenar una alerta, por lo que los permisos extendidos solo se permiten en el módulo de protección en tiempo real.

No se debe confundir con Extensiones de archivo excluidas, Exclusiones del HIPS, Exclusiones de detección ni Exclusiones de rendimiento.

Las exclusiones de procesos ayudan a reducir al mínimo el riesgo de conflictos potenciales y mejoran el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo sobre el rendimiento y la estabilidad generales del sistema operativo. La exclusión de un proceso/una aplicación es una exclusión de su archivo ejecutable (*.exe*).

Puede agregar archivos ejecutables a la lista de procesos excluidos en Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Protección del sistema de archivos en tiempo real** > **Exclusiones de procesos**.

Esta característica se diseñó para excluir herramientas de copia de seguridad. Excluir del análisis el proceso de la herramienta de copia de seguridad no solo garantiza la estabilidad del sistema, sino que, además, no afecta al rendimiento de la copia de seguridad, pues esta no se ralentiza durante su ejecución.

Haga clic en **Editar** para abrir la ventana de gestión **Exclusiones de procesos**, en la que puede agregar exclusiones y buscar el archivo ejecutable (por ejemplo, *Backup-tool.exe*) que se excluirá del análisis. En cuanto el archivo *.exe* se agrega a las exclusiones, ESET Small Business Security deja de supervisar la actividad de este proceso y no se ejecuta ningún análisis en ninguna de las operaciones de archivo realizadas por este proceso.

Si no utiliza la función de examinar al seleccionar el ejecutable del proceso, debe introducir manualmente una ruta de acceso completa del ejecutable. De lo contrario, la exclusión no funcionará correctamente y HIPS puede informar de errores.

También puede **Editar** procesos existentes o **Eliminar** dichos procesos de las exclusiones.

Protección de acceso a la web no tiene en cuenta esta exclusión, de modo que, si excluye el archivo ejecutable de su navegador, los archivos descargados se analizan de todas formas. Así, las infiltraciones pueden detectarse igualmente. Este caso es solo un ejemplo, y no le recomendamos crear exclusiones para navegadores.

# Agregar o modificar exclusiones de procesos

Este cuadro de diálogo le permite **agregar** procesos excluidos del motor de detección. Las exclusiones de procesos ayudan a reducir al mínimo el riesgo de conflictos potenciales y mejoran el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo sobre el rendimiento y la estabilidad generales del sistema operativo. La exclusión de un proceso/una aplicación es una exclusión de su archivo ejecutable (*.exe*).

Para seleccionar la ruta de acceso del archivo de una aplicación que es una excepción, haga clic en … (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). No escriba el nombre de la aplicación. En cuanto el archivo *.exe* se agrega a las exclusiones, ESET Small Business Security deja de supervisar la actividad de este proceso y no se ejecuta ningún análisis en ninguna de las operaciones de archivo realizadas por este proceso.

Si no utiliza la función de examinar al seleccionar el ejecutable del proceso, debe introducir manualmente una ruta de acceso completa del ejecutable. De lo contrario, la exclusión no funcionará correctamente y HIPS puede informar de errores.

También puede **Editar** procesos existentes o **Eliminar** dichos procesos de las exclusiones.

# Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más importante para mantener un sistema seguro. Por lo que debe tener cuidado cuando modifique los parámetros correspondientes. Es aconsejable que los modifique únicamente en casos concretos.

Una vez instalado ESET Small Business Security, se optimizará toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en ↩ junto a Configuración avanzada > **Protecciones** > **Respuestas de detección**.

# Análisis de protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, use un archivo de prueba de *www.eicar.com*. Este archivo de prueba es un archivo inofensivo que pueden detectar todos los programas antivirus. El archivo fue creado por el instituto EICAR (European Institute for Computer Antivirus Research: 'Instituto Europeo para la Investigación de Antivirus') con el fin de comprobar la funcionalidad de los programas antivirus.

Puede descargar el archivo aquí: http://www.eicar.org/download/eicar.com.
Tras escribir esta URL en el navegador, debe ver el mensaje de que la amenaza se ha eliminado.

# Qué debo hacer si la protección en tiempo real no funciona

En este capítulo, describimos los problemas que pueden surgir cuando se utiliza la protección en tiempo real y cómo resolverlos.

## Protección en tiempo real desactivada

Si un usuario desactiva sin darse cuenta la protección en tiempo real, debe reactivar la función. Para reactivar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del ordenador** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no se activa al iniciar el sistema, probablemente se deba a que la opción **Activar la protección del sistema de archivos en tiempo real** está desactivada. Para asegurarse de que esta opción está activada, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real**.

## Si la protección en tiempo real no detecta ni desinfecta amenazas

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si dos programas antivirus están instalados simultáneamente, pueden entrar en conflicto entre sí. Recomendamos que desinstale del sistema cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

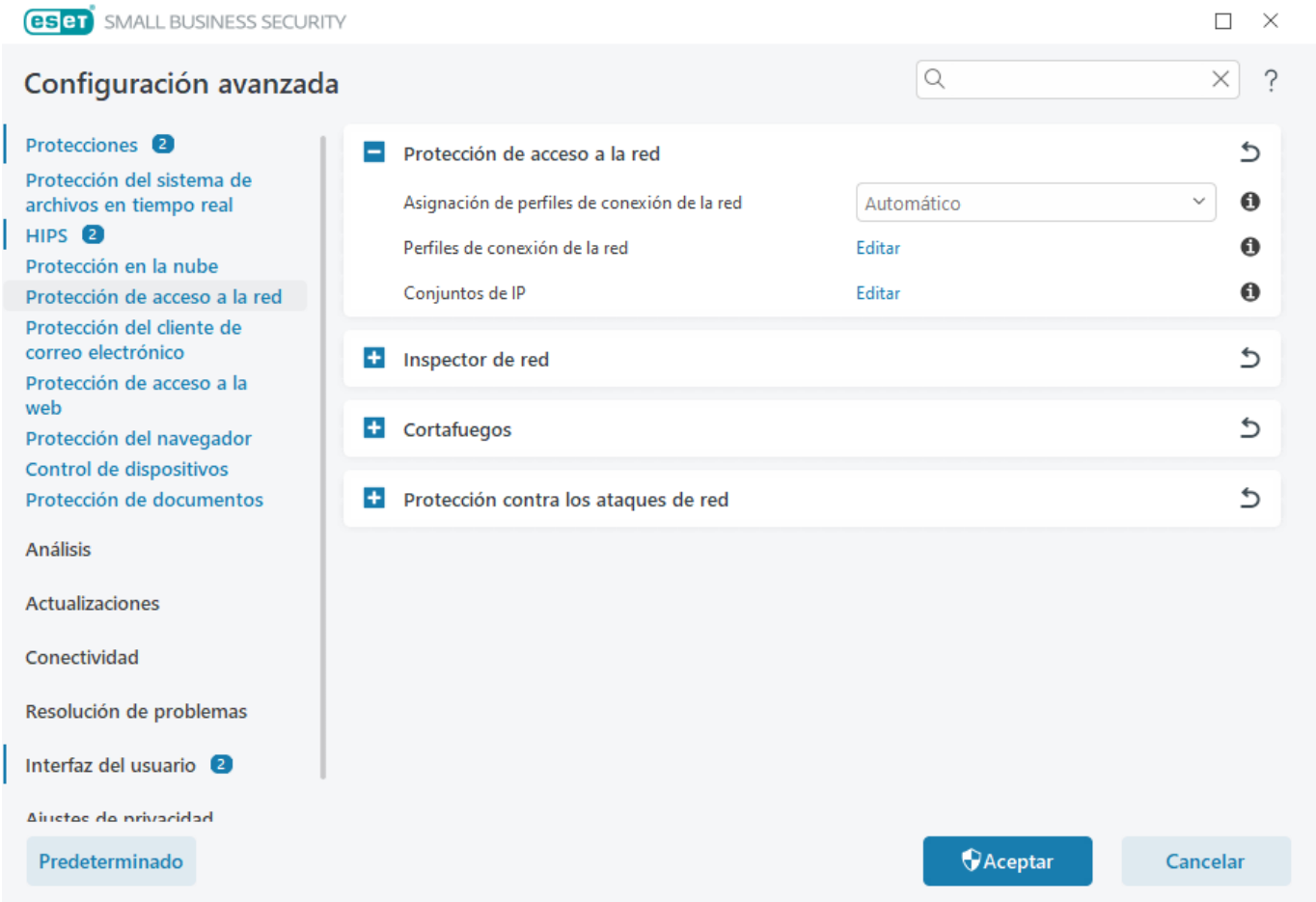
## La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y la opción **Activar la protección del sistema de archivos en tiempo real** está activada), es posible que se deba a conflictos con otros programas. Para resolver el problema, cree un registro del ESET SysInspector y envíelo al servicio de soporte técnico de ESET para que lo analice.

# Protección de acceso a la red

La protección de acceso a la red le permite configurar todas las conexiones de red en detalle. Puede permitir/denegar el acceso al ordenador en redes específicas, permitir/denegar el acceso a dispositivos de red desde su ordenador y más según la configuración.

De forma predeterminada, ESET Small Business Security tiene reglas de cortafuegos preconfiguradas y protección de acceso a la red para ofrecer la máxima seguridad. Sin embargo, es posible que determinados entornos requieran una configuración personalizada. Solo deben cambiar la configuración predeterminada usuarios experimentados.




Puede configurar los siguientes ajustes en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** (haga clic en los vínculos siguientes para obtener una descripción detallada de cada opción de protección de acceso a la red):

## Protección de acceso a la red

Perfiles de conexión de red: puede utilizar perfiles para controlar el comportamiento del cortafuegos para conexiones de red específicas.

Conjuntos de IP: puede definir colecciones de direcciones IP que creen un grupo lógico de direcciones IP, que puede utilizar para las reglas del cortafuegos.

Inspector de red

Cortafuegos

Protección contra los ataques de red

# Perfiles de conexión de la red

Los perfiles se pueden utilizar para controlar el comportamiento de la protección de la red de ESET Small Business Security para conexiones de red específicas. Al crear o editar una regla del cortafuegos, una regla de IDS o una regla de protección contra ataques de fuerza bruta, puede asignarla a un perfil específico o aplicarla a todos los perfiles.

Cuando hay un perfil activo en una conexión de red, solo se aplican las reglas globales (que no tienen un perfil especificado) y las reglas que se han asignado a dicho perfil. Es posible crear varios perfiles con diferentes reglas asignadas a conexiones de red para modificar fácilmente el comportamiento del cortafuegos.

Puede configurar los perfiles y las asignaciones de conexión de red en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección de acceso a la red**.

**Asignación de perfiles de conexión de red**: le permite elegir si a las conexiones de red recién descubiertas se les asigna automáticamente (seleccione **Automático** en el menú desplegable) un perfil predefinido o personalizado basado en Activadores configurados en perfiles de conexión de red o si desea que se le solicite (seleccione **Preguntar** en el menú desplegable) Configurar protección de la red y asignar un perfil manualmente cada vez que se detecte una nueva conexión de red.

También puede asignar manualmente un perfil de conexión de red específico en la ventana principal del programa > **Configurar** > **Protección de la red** > **Conexiones de red**. Desplácese sobre una conexión de red específica y haga clic en el icono ⋮ > **Editar** del menú para abrir la ventana Configurar protección de la red y seleccionar un perfil.

**Perfiles de conexión de red**: haga clic en **Editar** para Agregar o editar perfiles de conexión de red.

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

**Privado**: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible).

Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Pública**: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado.

Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

Cuando la conexión de red cambia de perfil, se muestra una notificación en la esquina inferior derecha de la pantalla.

# Agregar o editar perfiles de conexión de red

Puede agregar o editar perfiles de conexión de red en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección de acceso a la red** > **Perfiles de conexión de red** > **Editar**. Para editar un perfil, debe seleccionarse en la lista de **Perfiles de conexión de red**.

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

**Privado**: para una red de confianza (red doméstica o de oficina). El ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible).

Se recomienda utilizar esta configuración al acceder a una red local segura. Este perfil se asigna automáticamente a una conexión de red si está configurado como Dominio o Red privada en Windows.

**Pública**: para una red que no es de confianza (red pública). Los archivos y las carpetas de su sistema no se comparten ni son visibles para otros usuarios de la red, y el uso compartido de recursos del sistema está desactivado.

Se recomienda utilizar esta configuración al acceder a las redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

**Superior/Arriba/Abajo/Inferior**  : permite ajustar el nivel de prioridad de los perfiles de conexión de red (los perfiles de conexión de red se evalúan y aplican según la prioridad. Siempre se aplica el primer perfil coincidente).

## Agregar o editar un perfil

El perfil de conexión de red personalizado permite aplicar reglas de cortafuegos y definir configuraciones adicionales para conexiones de red específicas. En la sección Activadores, se especifica a qué conexiones de red debe asignarse el perfil personalizado.

Para abrir el editor de perfiles, en la ventana **Perfiles de conexión de red**:

- Haga clic en **Agregar**.
- Seleccione uno de los perfiles existentes y haga clic en **Editar**.
- Seleccione uno de los perfiles existentes y haga clic en **Copiar**.

**Nombre**: nombre personalizado de su perfil.

**Descripción**: descripción del perfil para ayudar a identificarlo.

**Direcciones de confianza adicionales**: las direcciones definidas aquí se agregan a la zona de confianza de la conexión de red a la que se aplica este perfil (independientemente del tipo de protección de la red).

**Conexión de confianza**: el ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red (el acceso a los archivos y las impresoras compartidos está activado, la comunicación RPC entrante está activada y el escritorio remoto compartido está disponible). Se recomienda usar esta configuración al crear un perfil para una conexión de red local segura. Todas las subredes de red conectadas directamente también se consideran de confianza.

Por ejemplo, si un adaptador de red está conectado a esta red con la dirección IP 192.168.1.5 y la máscara de subred 255.255.255.0, la subred 192.168.1.0/24 se agrega a la red de confianza de la conexión de red de dicho adaptador. Si el adaptador tiene más direcciones/subredes, todas serán de confianza.

**Informe sobre cifrado WiFi débil**: ESET Small Business Security mostrará una notificación en el escritorio cuando se conecte a una red inalámbrica no protegida o a una red con un nivel de protección débil.

**Activadores**: condiciones personalizadas que deben cumplirse para asignar este perfil de conexión de red a una conexión de red. Consulte Activadores para obtener una explicación detallada.

# Activadores

Los activadores son condiciones personalizadas que deben cumplirse para asignar un Perfil de conexión de red a una Conexión de red. Si la red conectada tiene los mismos atributos que los definidos en los activadores de un perfil de red conectada, el perfil se aplicará a la red. Un perfil de conexión de red puede tener uno o varios activadores. Si hay varios activadores, se aplica la lógica OR (se debe cumplir al menos una condición). Puede definir activadores en el Editor de perfil de conexión de red. La creación de perfiles de conexión de red personalizados debe llevarla a cabo un usuario experimentado.

Los siguientes activadores están disponibles (si desea conocer los detalles de la red actual, consulte Conexiones de red):

Adaptador

**Tipo de adaptador**: aplique el perfil si la conexión de red se establece en el tipo de adaptador seleccionado.
**Nombre del adaptador**: aplique el perfil si el nombre del adaptador de red coincide.
**IP del adaptador**: aplica el perfil si la dirección IP del adaptador de red o un intervalo de direcciones coinciden.

DNS

**Sufijo DNS**: aplique el perfil si el nombre de dominio coincide.
**IP DNS**: aplica el perfil si la dirección IP o un intervalo de direcciones IP del servidor DNS coinciden.

WINS

Aplique el perfil si la dirección IP asignada de Windows Internet Name Service (WINS) coincide.

DHCP

**IP DHCP**: coincide con la dirección IP del servidor DHCP.

Puerta de enlace predeterminada

**IP**: aplica el perfil si la dirección IP o un intervalo de direcciones IP de la puerta de enlace predeterminada coinciden.
**Dirección MAC**: aplique el perfil si la dirección MAC de la puerta de enlace predeterminada coincide.

Wi-Fi

**SSID:**: aplique el perfil si el SSID (nombre de la red Wi-Fi) coincide.
**Nombre de perfil**: aplique el perfil si el nombre del perfil de Wi-Fi coincide.
**Tipo de seguridad**: aplique el perfil si el tipo de seguridad coincide con el seleccionado en el menú desplegable. Si desea hacer coincidir más de uno, cree otro activador.
**Tipo de cifrado**: aplique el perfil si el tipo de cifrado coincide con el seleccionado en el menú desplegable. Si desea hacer coincidir más de uno, cree otro activador.
**Seguridad de red**: aplique el perfil si la red está **Abierta**/**Protegida**.

Perfil de Windows

Aplique el perfil si la red está configurada en Windows como **Dominio**/**Privada**/**Pública**.

Autenticación

La autenticación de red busca un servidor específico de la red y utiliza el cifrado asimétrico (RSA) para autenticar al servidor. El nombre de la red que se autentica debe coincidir con el nombre establecido en la configuración del servidor de autenticación. El nombre distingue entre mayúsculas y minúsculas. El nombre del servidor se puede escribir como una dirección IP, DNS o nombre NetBios.
Descargue ESET Authentication Server
La clave pública se puede importar con cualquiera de estos tipos de archivo:
- Clave pública cifrada PEM (.pem); puede generar esta clave utilizando ESET Authentication Server
- Clave pública cifrada.
- Certificado de clave pública (.crt).

Haga clic en **Probar** para probar su configuración. Si la autenticación se realiza correctamente, se muestra que la autenticación del servidor se ha realizado correctamente. Si la autenticación no está configurada correctamente, aparecerá uno de los mensajes de error siguientes:
Error en la autenticación del servidor. Firma no válida o no concordante.
La firma del servidor no coincide con la clave pública introducida.
Error en la autenticación del servidor. El nombre de la red no coincide.
El nombre de la red configurada no se corresponde con el nombre de red del servidor de autenticación. Repase ambos nombres y asegúrese de que son idénticos.
Error en la autenticación del servidor. El servidor no respondió o la respuesta no es válida.
Si el servidor no se está ejecutando o no está accesible, el usuario no recibe ninguna respuesta. Puede recibir una respuesta no válida si hay otro servidor HTTP ejecutándose en la dirección especificada.
Clave pública introducida no válida.
Compruebe que el archivo de clave pública que ha introducido no esté dañado.

# Conjuntos de IP

Un conjunto de IP es una colección de direcciones IP que forman un grupo lógico de direcciones IP. Resulta útil cuando se reutiliza el mismo conjunto de direcciones en varias reglas de cortafuegos o reglas de protección contra ataques de fuerza bruta.

ESET Small Business Security también contiene conjuntos de IP predefinidos a los que se aplican reglas internas.

Un ejemplo de dicho grupo es una **Zona de confianza**.

Zona de confianza representa un grupo de direcciones de red donde su ordenador y los archivos compartidos almacenados en el ordenador son visibles para otros usuarios de la red, y los recursos del sistema están disponibles para otros usuarios de la red.

Para agregar un conjunto de IP:

1. Abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Conjuntos de IP** > **Editar**.

2. Haga clic en **Agregar**, escriba un **Nombre** y una **Descripción** para la zona, y escriba una dirección IP remota en **Dirección del ordenador remoto (IPv4/IPv6, intervalo, máscara)**.

3. Haga clic en **Aceptar**.

Para obtener más información, consulte Editar conjuntos de IP.

# Editar conjuntos de IP

Para obtener más información acerca de los conjuntos de IP, consulte Conjuntos de IP.

## Columnas

**Nombre**: nombre de un grupo de ordenadores remotos.

**Descripción**: descripción general del grupo.

**Direcciones IP**: direcciones IP remotas que pertenecen a un conjunto de IP.

## Elementos de control

Al **agregar** o **editar** un conjunto de IP, los siguientes campos están disponibles:

**Nombre**: nombre de un grupo de ordenadores remotos.

**Descripción**: descripción general del grupo.

**Dirección del ordenador remoto (IPv4, IPv6, intervalo, máscara)**: le permite agregar una dirección remota, un rango de direcciones o una subred.

**Eliminar**: quita una zona de la lista.

Los conjuntos de IP predefinidos no se pueden quitar.

### Ejemplos de direcciones IP

Agregar dirección IPv4:

**Dirección única**: agrega la dirección IP de un ordenador concreto (por ejemplo, *192.168.0.10*).

**Rango de direcciones**: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones de varios ordenadores (por ejemplo, *192.168.0.1-192.168.0.99*).

**Subred**: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red de la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.

Agregar dirección IPv6:

**Dirección única**: agrega la dirección IP de un ordenador concreto (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).

**Subred**: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

# Inspector de red

Inspector de red puede ayudar a identificar vulnerabilidades en su red de confianza (doméstica o de oficina; ejemplo, puertos abiertos o una contraseña débil de router). También ofrece una lista de los dispositivos conectados, categorizados por tipo de dispositivo (por ejemplo, impresora, router, dispositivo móvil, etc.) para mostrarle lo que está conectado a su red (por ejemplo, videoconsola, IoT u otros dispositivos domésticos inteligentes).

Puede configurar el Inspector de red en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Inspector de red**.

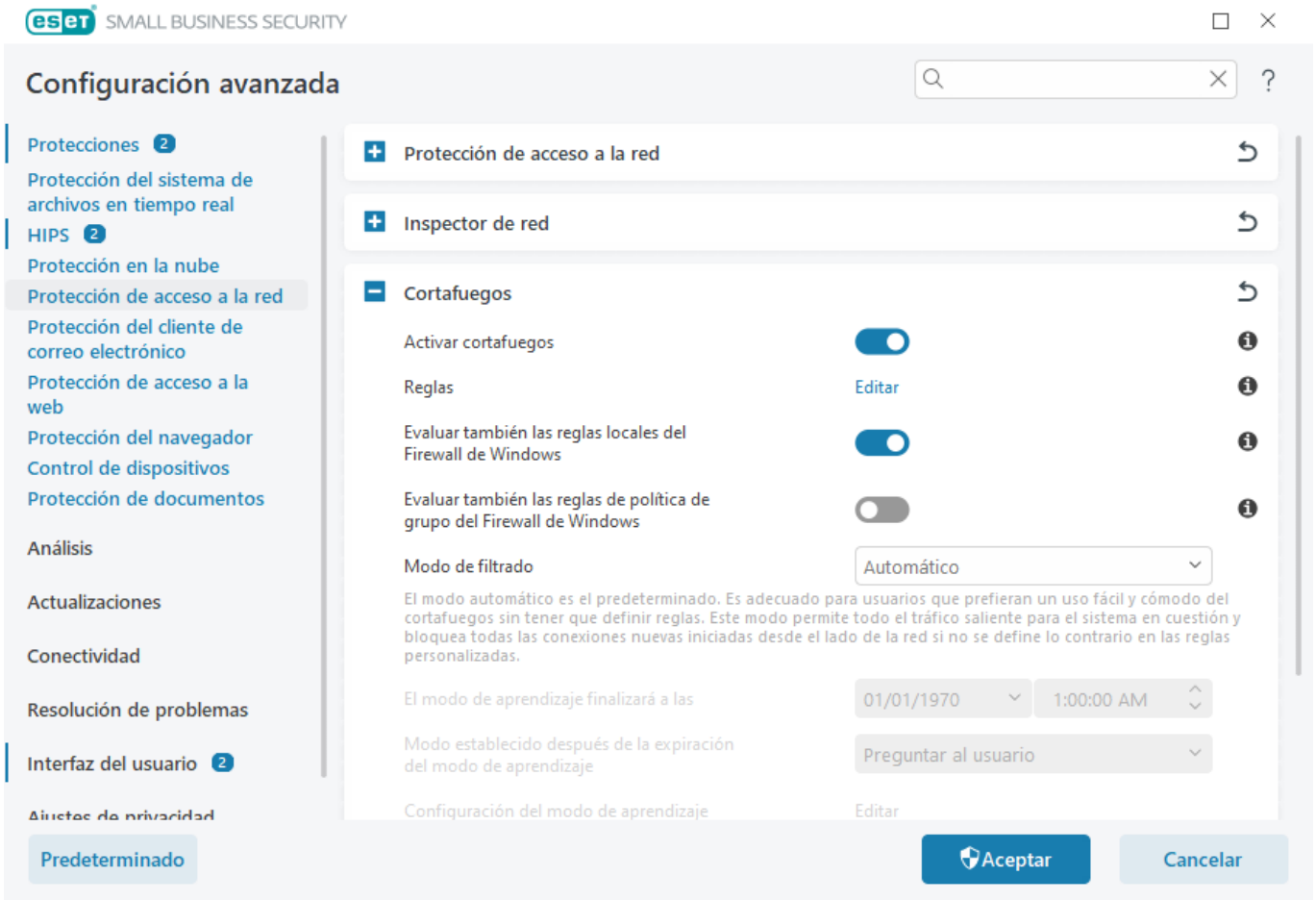
**Activar Inspector de red**: Inspector de red ayuda a identificar vulnerabilidades en la red doméstica, como puertos abiertos o una contraseña de router poco segura. También contiene una lista de dispositivos conectados, clasificados por tipo de dispositivo.

**Notificaciones de dispositivos de red recién detectados**: le avisa cuando se detecta un dispositivo nuevo en la red.

# Cortafuegos

El cortafuegos controla todo el tráfico de red en función de reglas internas y definidas por el usuario. Permite o deniega conexiones de red individuales. El cortafuegos proporciona protección frente a ataques procedentes de dispositivos remotos y puede bloquear servicios potencialmente peligrosos.

Para configurar el cortafuegos, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Cortafuegos**.




# Cortafuegos

## Activar cortafuegos

Le recomendamos que mantenga esta función habilitada para proteger su sistema. Con el cortafuegos activado, el tráfico de red se analiza en ambas direcciones.

## Reglas

La configuración de reglas le permite ver y editar todas las Reglas del cortafuegos aplicadas al tráfico generado por aplicaciones individuales dentro de conexiones de confianza e Internet.

Puede crear una regla de IDS para protegerse contra varios tipos de ataques de red, incluidos los ataques de botnet. Para modificar una regla, vaya a Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red** > **Reglas de IDS** y haga clic en **Editar**.

## Evaluar también las reglas del Firewall de Windows

En el modo automático de filtrado, permita también el tráfico entrante permitido por las reglas del cortafuegos de Windows, a menos que las reglas de ESET lo bloqueen explícitamente.

## Modo de filtrado

El comportamiento del cortafuegos cambia en función del modo de filtrado. Los modos de filtrado también influyen en el nivel necesario de interacción del usuario.

El cortafuegos de ESET Small Business Security cuenta con los modos de filtrado siguientes:

| Modo de filtrado | Descripción |
|---|---|
| **Modo automático** | El modo predeterminado. Este modo es adecuado para usuarios que prefieren usar el cortafuegos sin definir reglas. Se pueden crear reglas personalizadas, definidas por el usuario, pero no son obligatorias en **modo automático**. Modo automático permite todo el tráfico saliente para un sistema en cuestión y bloquea casi todo el tráfico entrante, excepto determinado tráfico procedente de la zona de confianza, como se especifica en Sistema de detección de intrusos y opciones avanzadas/Servicios permitidos, y las respuestas a las comunicaciones salientes recientes. |
| **Modo interactivo** | Modo interactivo: le permite crear una configuración personalizada para el cortafuegos. Cuando se detecta una comunicación para la que no existen reglas, aparece un cuadro de diálogo que notifica la existencia de una conexión desconocida. El cuadro de diálogo ofrece la opción de permitir o denegar la comunicación; la decisión de permitirla o denegarla se puede recordar como una regla nueva para el cortafuegos. Si el usuario opta por crear una nueva regla, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla. |
| **Modo basado en reglas** | Bloquea todas las conexiones que no se hayan definido en una regla específica que las permita. Este modo permite a los usuarios avanzados definir reglas que autoricen únicamente las conexiones especificadas y seguras. El cortafuegos bloqueará todas las demás conexiones no especificadas. |
| **Modo de aprendizaje** | Crea y guarda reglas automáticamente. Este modo está recomendado para la configuración inicial del cortafuegos, pero no se debe mantener activado durante periodos de tiempo prolongados. No es necesaria la intervención del usuario, pues ESET Small Business Security guarda las reglas según los parámetros predefinidos. El modo de aprendizaje solo debe utilizarse hasta que se hayan creado todas las reglas para las comunicaciones necesarias para evitar riesgos de seguridad. |

**El modo de aprendizaje finalizará a las**: establezca la fecha y la hora a las que desea que el modo de aprendizaje finalice automáticamente. También puede desactivar el modo de aprendizaje manualmente cuando lo desee.

**Modo establecido tras conocer la caducidad del modo**: defina a qué modo de filtrado revertirá el cortafuegos una vez que transcurra el período de tiempo para el modo de aprendizaje. Lea más sobre los modos de filtrado en la tabla anterior. Tras la finalización, la opción **Preguntar al usuario** requiere privilegios administrativos para realizar cambios en el Modo de filtrado del cortafuegos.

Configuración del modo de aprendizaje: haga clic en **Editar** para configurar los parámetros para guardar las reglas creadas en el modo de aprendizaje.

## Detección de modificaciones de la aplicación

La función de detección de modificaciones de la aplicación muestra notificaciones si las aplicaciones modificadas, para las que existe una regla de cortafuegos, intentan establecer conexiones.

# Configuración del modo de aprendizaje

En el modo de aprendizaje, se pueden crear y guardar reglas automáticamente para cada comunicación que se haya establecido en el sistema. No es necesaria la intervención del usuario, pues ESET Small Business Security guarda las reglas según los parámetros predefinidos.

Este modo puede exponer su sistema a riesgos, por lo que solo se recomienda para la configuración inicial del cortafuegos.

Seleccione **Aprendizaje** en el menú desplegable de Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Cortafuegos** > **Cortafuegos** > **Modo de filtrado** para activar las opciones del modo de aprendizaje. Haga clic en **Editar** junto a **Configuración del modo de aprendizaje** para configurar las siguientes opciones:

El cortafuegos no filtra la comunicación cuando el modo de aprendizaje está activado. Se permiten todas las comunicaciones de entrada y salida. En este modo el ordenador no cuenta con la protección completa del cortafuegos.

**Tráfico entrante desde la zona de confianza**: un dispositivo remoto de la zona de confianza que intenta comunicarse con una aplicación local del ordenador sería un ejemplo de conexión entrante.

**Tráfico saliente hacia la zona de confianza**: una aplicación local intenta establecer una conexión con otro ordenador dentro de la red local, o dentro de una red en la zona de confianza.

**Tráfico de Internet entrante**: un dispositivo remoto intenta comunicarse con una aplicación que se está ejecutando en el ordenador.

**Tráfico de Internet saliente**: una aplicación local que intenta establecer una conexión con otro dispositivo.

En todas las secciones puede definir los parámetros que desea agregar a las reglas de reciente creación:

**Agregar puerto local**: incluye el número de puerto local de la comunicación de red. Para las comunicaciones salientes, normalmente se generan números aleatorios. Por este motivo, le recomendamos que active esta opción solo para las comunicaciones entrantes.

**Agregar aplicación**: incluye el nombre de la aplicación local. Esta opción es útil para reglas futuras a nivel de aplicaciones (reglas que definen la comunicación para una aplicación entera). Por ejemplo, puede activar la comunicación solo para un navegador web o para un cliente de correo electrónico.

**Agregar puerto remoto**: incluye el número de puerto remoto de la comunicación de red. Por ejemplo, puede aceptar o denegar un servicio específico asociado con un número de puerto estándar (HTTP – 80, POP3 – 110, etc.).

**Agregar dirección IP remota/zona de confianza**: se puede utilizar una dirección IP remota o una zona como un parámetro para nuevas reglas que definan todas las conexiones de red entre el sistema local y dicha dirección remota o zona. Esta opción resulta útil a la hora de definir acciones para un dispositivo concreto o un grupo de dispositivos en red.

**Cantidad máxima de reglas distintas para una aplicación**: si una aplicación se comunica a través de diferentes puertos con varias direcciones IP, etc., el cortafuegos en modo de aprendizaje crea un número adecuado de reglas para esta aplicación. Esta opción le permite limitar el número de reglas que se pueden crear para una sola aplicación.

# Reglas del cortafuegos

Las reglas del cortafuegos representan un conjunto de condiciones que se utilizan para probar de manera significativa todas las conexiones de red y acciones asignadas a estas condiciones. Utilice las reglas del cortafuegos para definir la acción que se emprende al establecer diferentes tipos de conexión de red.

Las reglas se evalúan de arriba a abajo y puede ver la prioridad en la primera columna. La acción de la primera regla coincidente se utiliza para todas las conexiones de red evaluadas.

Las conexiones se pueden dividir en entrantes y salientes. Las conexiones entrantes se inician en dispositivos remotos que intentan establecer una conexión con el sistema local. Las conexiones salientes funcionan de la forma opuesta: el sistema local se pone en contacto con un dispositivo remoto.

Si se detecta una comunicación desconocida, debe considerar detenidamente su admisión o denegación. Las conexiones no solicitadas, no seguras o desconocidas suponen un riesgo de seguridad para el sistema. Si se establece una conexión de este tipo, debe prestar atención al dispositivo remoto y a la aplicación que intente conectarse a su ordenador. Muchas amenazas intentan obtener y enviar datos privados, o descargar otras aplicaciones maliciosas en las estaciones de trabajo host. El cortafuegos le permite detectar e interrumpir estas conexiones.

Puede ver y editar las reglas del cortafuegos en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Cortafuegos Reglas** > **Editar**.

Si tiene muchas reglas de cortafuegos, puede usar un filtro para mostrar solo reglas específicas. Para filtrar las reglas del cortafuegos, haga clic en **Más filtros** encima de la lista Reglas del cortafuegos. Puede filtrar las reglas en función de los siguientes criterios:

- Origen
- Dirección
- Acción
- Disponibilidad

De forma predeterminada, las reglas de cortafuegos predefinidas están ocultas. Para mostrar todas las reglas predefinidas, desactive el interruptor situado junto a **Ocultar reglas integradas (predefinidas).** Las reglas predefinidas pueden desactivarse, pero no eliminarse.

Haga clic en el icono de búsqueda de la parte superior derecha para buscar reglas por nombre, protocolo o puerto.

## Columnas

**Prioridad**: las reglas se evalúan de arriba a abajo y puede ver la prioridad en la primera columna.

**Activado**: muestra si la regla está activada o desactivada; seleccione la casilla de verificación para activar la regla.

**Aplicación**: indica la aplicación a la que se aplica la regla.

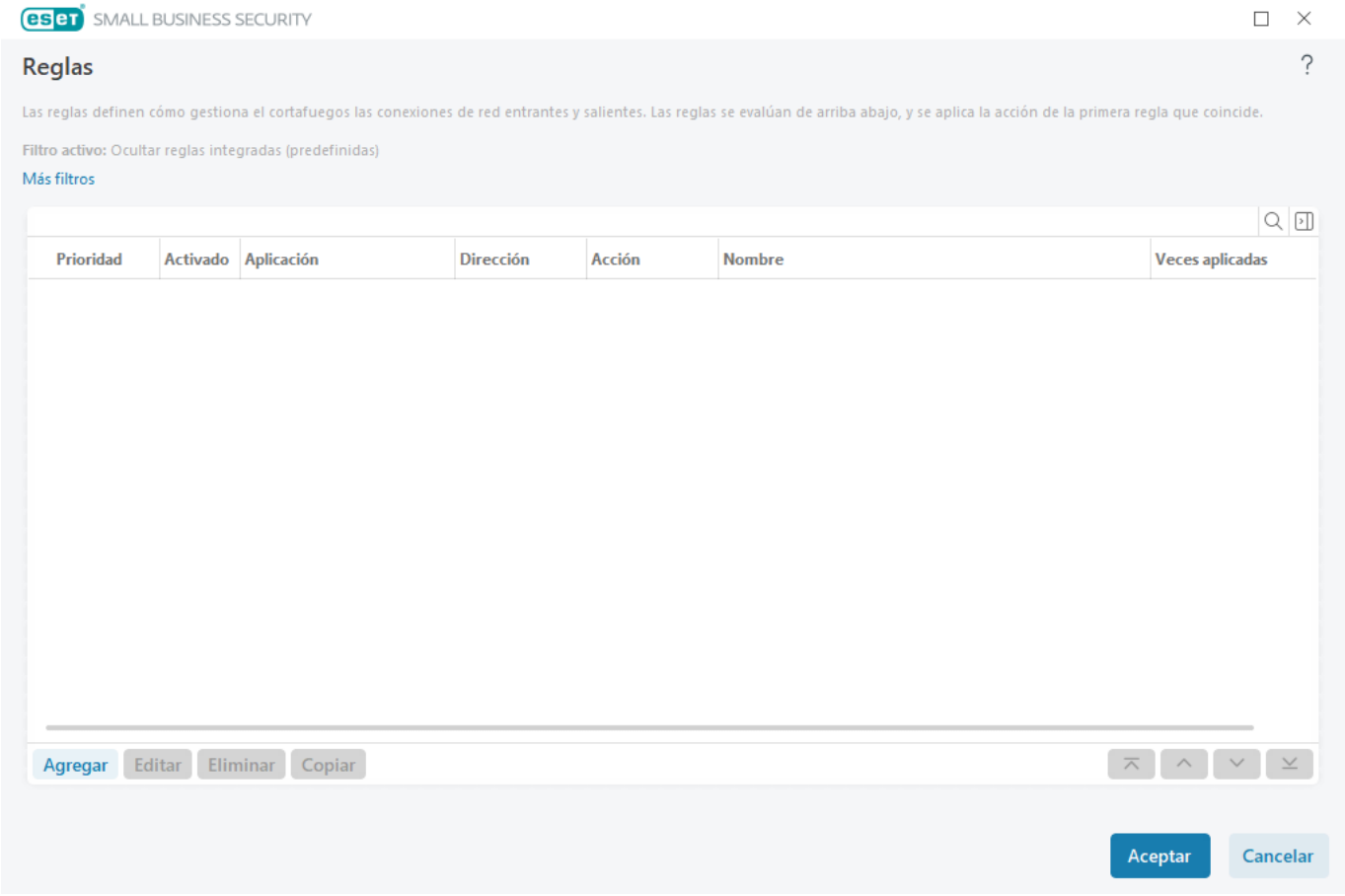
**Dirección**: dirección de la comunicación (entrante, saliente o ambas).

**Acción**: muestra el estado de la comunicación (bloquear, permitir o preguntar).

**Nombre**: nombre de la regla. El icono de ESET representa una regla predefinida.

**Veces aplicadas**: número total de veces que se ha aplicado la regla.

Haga clic en el icono de expansión para mostrar los detalles de la regla.




## Elementos de control

**Agregar**: crea una nueva regla.

**Modificar**: modifique una regla existente.

**Quitar**: elimina una regla existente.

**Copiar**: cree una copia de una regla seleccionada.


**Superior/Arriba/Abajo/Inferior**: le permite ajustar el nivel de prioridad de las reglas (las reglas se ejecutan de arriba abajo).

# Agregar o modificar reglas del cortafuegos

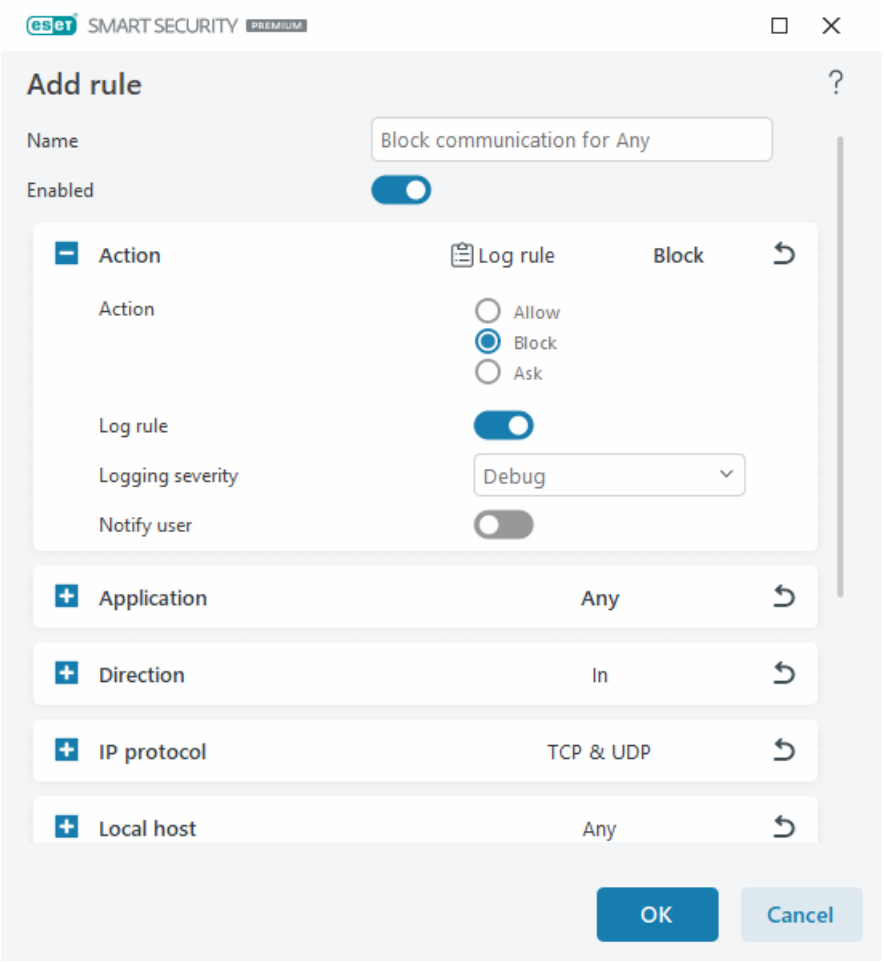
Las reglas del cortafuegos representan condiciones que se utilizan para probar de manera significativa todas las conexiones de red y acciones asignadas a estas condiciones. Cuando la configuración de red cambia (por ejemplo, si se ha cambiado la dirección de red o el número de puerto de la ubicación remota), puede ser necesario editar o agregar reglas de cortafuegos para garantizar el correcto funcionamiento de una aplicación a la que se haya aplicado una regla. Un usuario experimentado debe crear reglas de cortafuegos personalizadas.

### Instrucciones con ilustraciones

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- Abrir o cerrar (permitir o denegar) un puerto específico utilizando un cortafuegos
- Crear una regla del cortafuegos a partir de los archivos de registro en ESET Small Business Security

Para agregar o editar una regla de cortafuegos, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Cortafuegos** > **Reglas** > **Editar**. En la ventana Reglas del cortafuegos, haga clic en **Agregar** o **Editar**.




**Nombre**: escriba un nombre para la regla.

**Activado**: haga clic en el interruptor para activar la regla.

Agregue acciones y condiciones para la regla del cortafuegos:

Acción

**Acción**: seleccione si desea **Permitir**/**Bloquear** la comunicación que coincida con las condiciones definidas en esta regla o si desea que ESET Small Business Security **pregunte** cada vez que se establezca la comunicación.
**Regla de registro**: si se aplica la regla, se registrará en Archivos de registro.
**Registro de severidad**: seleccione la gravedad del registro para esta regla.
**Advertir al usuario**: muestra una notificación cuando se aplica la regla.

Aplicación

Especifique una aplicación en la que se aplicará esta regla.
**Rutas de acceso de la aplicación**: haga clic en **...** y desplácese hasta una aplicación o escriba la ruta completa de la aplicación (por ejemplo C:\Program Files\Firefox\Firefox.exe). NO escriba únicamente el nombre de la aplicación.
**Firma de la aplicación**: puede aplicar la regla a las aplicaciones en función de las firmas (nombre del editor). Seleccione en el menú desplegable si desea aplicar la regla a aplicaciones con **Cualquier firma válida** o a **Firmado por un firmante específico**. Si selecciona aplicaciones con **Firmado por un firmante específico**, debe definir el firmante en el campo **Nombre del firmante**.
**Aplicación de Microsoft Store**: seleccione en el menú desplegable una aplicación instalada desde Microsoft Store.
**Servicio**: puede seleccionar un servicio del sistema en lugar de una aplicación. Abra el menú desplegable para seleccionar un servicio.
**Aplicar a procesos secundarios**: algunas aplicaciones pueden ejecutar más procesos aunque solo se vea la ventana de una aplicación. Haga clic en el interruptor para activar la regla para todos los procesos de la aplicación especificada.

### Dirección

Seleccione la **Dirección** de comunicación para esta regla:
- **Ambos**: comunicación entrante y saliente.
- **Entrante**: solo comunicación entrante.
- **Saliente**: solo comunicación saliente.

### Protocolo IP

Seleccione un **Protocolo** en el menú desplegable si solo desea que esta regla se aplique a un protocolo específico.

### Cliente local

Direcciones locales, intervalo de direcciones o subred donde se aplica esta regla. Si no hay ninguna dirección especificada, la regla se aplicará a todas las comunicaciones con clientes locales. Puede agregar direcciones IP, intervalos de direcciones o subredes directamente en el campo de texto **IP** o seleccionar entre los Conjuntos de IP existentes haciendo clic en **Editar** junto a **Conjuntos de IP**.

### Puerto local

Número(s) de **puertos** locales. Si no se proporcionan números, la regla se aplicará a cualquier puerto. Agregue un solo puerto de comunicación o un rango de puertos de comunicación.

### Host remoto

Dirección remota, intervalo de direcciones o subred donde se aplica esta regla. Si no se especifica ninguna dirección, la regla se aplicará a todas las comunicaciones con clientes remotos. Puede agregar direcciones IP, intervalos de direcciones o subredes directamente en el campo de texto **IP** o seleccionar entre los Conjuntos de IP existentes haciendo clic en **Editar** junto a **Conjuntos de IP**.

### Puerto remoto

Número(s) de **puertos** remotos. Si no se proporcionan números, la regla se aplicará a cualquier puerto. Agregue un solo puerto de comunicación o un rango de puertos de comunicación.

### Perfil

Se puede aplicar una regla de cortafuegos a Perfiles de conexión de la red específicos.
**Cualquiera**: la regla se aplicará a cualquier conexión de red independientemente del perfil utilizado.
**Seleccionado**: la regla se aplicará a una conexión de red específica en función del perfil seleccionado. Active la casilla de verificación situada junto a los perfiles que desee seleccionar.

Creamos una regla nueva para permitir que el navegador web Firefox acceda a Internet o a los sitios web de la red local.
1.En la sección **Acción**, seleccione **Acción** > **Permitir**.
2.En la sección **Aplicación**, especifique la **Rutas de acceso de la aplicación** del navegador web (por ejemplo, C:\Program Files\Firefox\Firefox.exe). NO escriba únicamente el nombre de la aplicación.
3.En la sección **Dirección**, seleccione **Dirección** > **Saliente**.
4.En la sección **Protocolo IP**, seleccione **TCP y UDP** en el menú desplegable **Protocolo**.
5.En la sección **Puerto remoto**, agregue los números de **Puerto**: *80, 443* para permitir la navegación estándar.

# Detección de modificaciones de la aplicación

Esta función de detección de modificaciones de la aplicación muestra una notificación cuando las aplicaciones modificadas (para las que existe una regla del cortafuegos) intentan establecer una conexión. La modificación de aplicaciones es un mecanismo para reemplazar una aplicación original por otra de forma temporal o peramente con un archivo ejecutable diferente (protege frente al abuso de reglas de cortafuegos).

Tenga en cuenta que esta característica no pretende detectar modificaciones en ninguna aplicación en general. Su objetivo es evitar el mal uso de las reglas existentes del cortafuegos, y que solo se supervisen las aplicaciones para las que hay reglas del cortafuegos específicas.

Para editar **Detección de modificaciones de la aplicación**, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red Cortafuegos** > **Detección de modificaciones de la aplicación**.

**Activar la detección de modificaciones en las aplicaciones**: si se selecciona esta opción, el programa controlará las aplicaciones en busca de cambios (actualizaciones, infecciones u otras modificaciones). Cuando una aplicación modificada intente establecer una conexión, recibirá una notificación del cortafuegos.

**Permitir la modificación de aplicaciones firmadas (de confianza)**: no se envía una notificación si la aplicación tiene la misma firma digital válida antes y después de la modificación.

**Lista de aplicaciones excluidas de la detección**: en esta ventana puede agregar o quitar aplicaciones individuales en las que se permiten modificaciones sin notificación.

# Lista de aplicaciones excluidas de la detección

El cortafuegos de ESET Small Business Security detecta los cambios realizados en las aplicaciones que ya tienen reglas (consulte Detección de modificaciones de la aplicación).

En algunos casos, tal vez no le interese utilizar esta funcionalidad para algunas aplicaciones si quiere excluirlas del análisis que realiza el cortafuegos.

**Agregar**: abre una ventana donde puede seleccionar una aplicación para agregarla a la lista de aplicaciones excluidas de la detección de modificaciones. Puede elegir entre una lista de aplicaciones en ejecución con comunicación de red abierta, para la que existe una regla del cortafuegos o agregar una aplicación concreta.

**Editar**: abre una ventana donde puede cambiar la ubicación de una aplicación que está en la lista de aplicaciones excluidas de la detección de modificaciones. Puede elegir entre una lista de aplicaciones en ejecución con comunicación de red abierta, para la que existe una regla del cortafuegos o cambiar la ubicación manualmente.

**Quitar**: quita entradas de la lista de aplicaciones excluidas de la detección de modificaciones.

# Protección contra los ataques de red (IDS)

La protección contra los ataques de red (IDS) mejora la detección de ataques de vulnerabilidades conocidas. Obtenga más información sobre la protección contra los ataques de red en el Glosario. Para configurar la protección contra los ataques de red, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red (IDS)**.

**Activar Protección contra ataques en la red (IDS)**: analiza el contenido del tráfico de red y le protege contra posibles ataques de red. Se bloqueará todo el tráfico que se considere dañino.

**Activar la protección contra botnets**: detecta y bloquea las comunicaciones con servidores de control y comando maliciosos basándose en patrones habituales cuando el ordenador está infectado y un bot intenta establecer comunicación. Lea más sobre la protección contra botnets en el glosario.

Reglas de IDS: esta opción le permite configurar opciones de filtro avanzadas para detectar varios tipos de ataques y exploits que se pueden usar para dañar el ordenador.

> **Instrucciones con ilustraciones**
> Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
> - Excluir una dirección IP del IDS en ESET Small Business Security

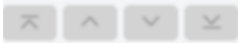
Todos los sucesos importantes detectados por la protección de la red se guardan en un archivo de registro. Consulte el registro de protección de la red para obtener más información.

# Reglas de IDS

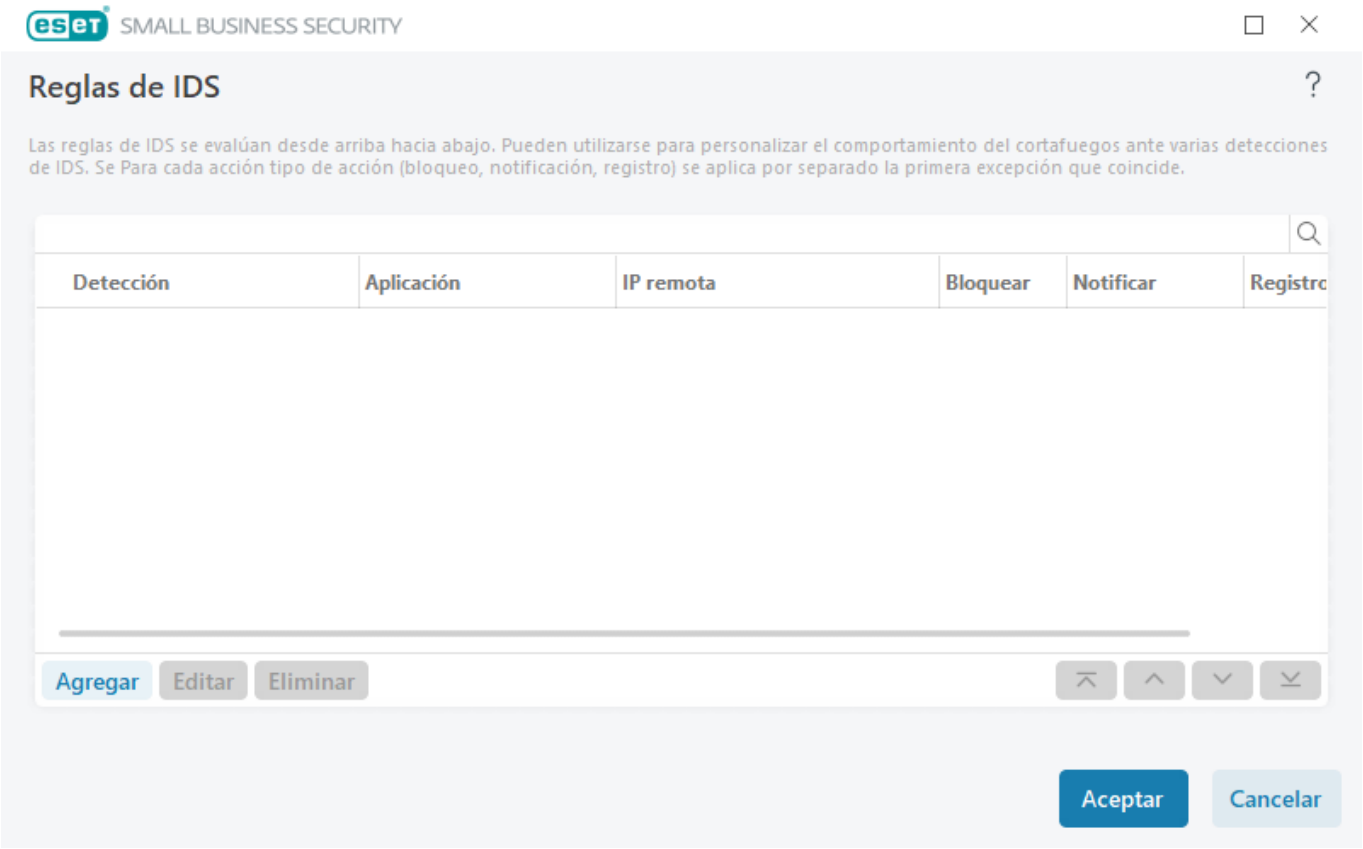
En algunas situaciones, el Servicio de detección de intrusiones (IDS) puede detectar la comunicación entre routers u otros dispositivos de red internos como un ataque potencial. Por ejemplo, puede agregar la dirección segura conocida a las Direcciones excluidas de la zona de IDS para ignorar el IDS.

> **Instrucciones con ilustraciones**
> Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
> - Excluir una dirección IP del IDS en ESET Small Business Security

## Administración de reglas de IDS

- **Agregar**: haga clic aquí para crear una nueva regla de IDS.
- **Modificar**: haga clic aquí para modificar una regla de IDS.
- **Quitar**: seleccione y haga clic aquí para quitar una regla de la lista de reglas de IDS.
-  **Superior/Arriba/Abajo/Inferior**: le permite ajustar el nivel de prioridad de las reglas

(las excepciones se evalúan de arriba abajo).




## Editor de reglas

**Detección**: tipo de detección.

**Nombre de amenaza**: puede especificar un nombre de amenaza para algunas de las detecciones disponibles.

**Aplicación**: para seleccionar la ruta de acceso del archivo de una aplicación que es una excepción, haga clic en … (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). No escriba el nombre de la aplicación.

**Dirección IP remota**: una lista de direcciones/rangos/subredes IPv4 o IPv6 remotos. Las direcciones deben separarse mediante comas.

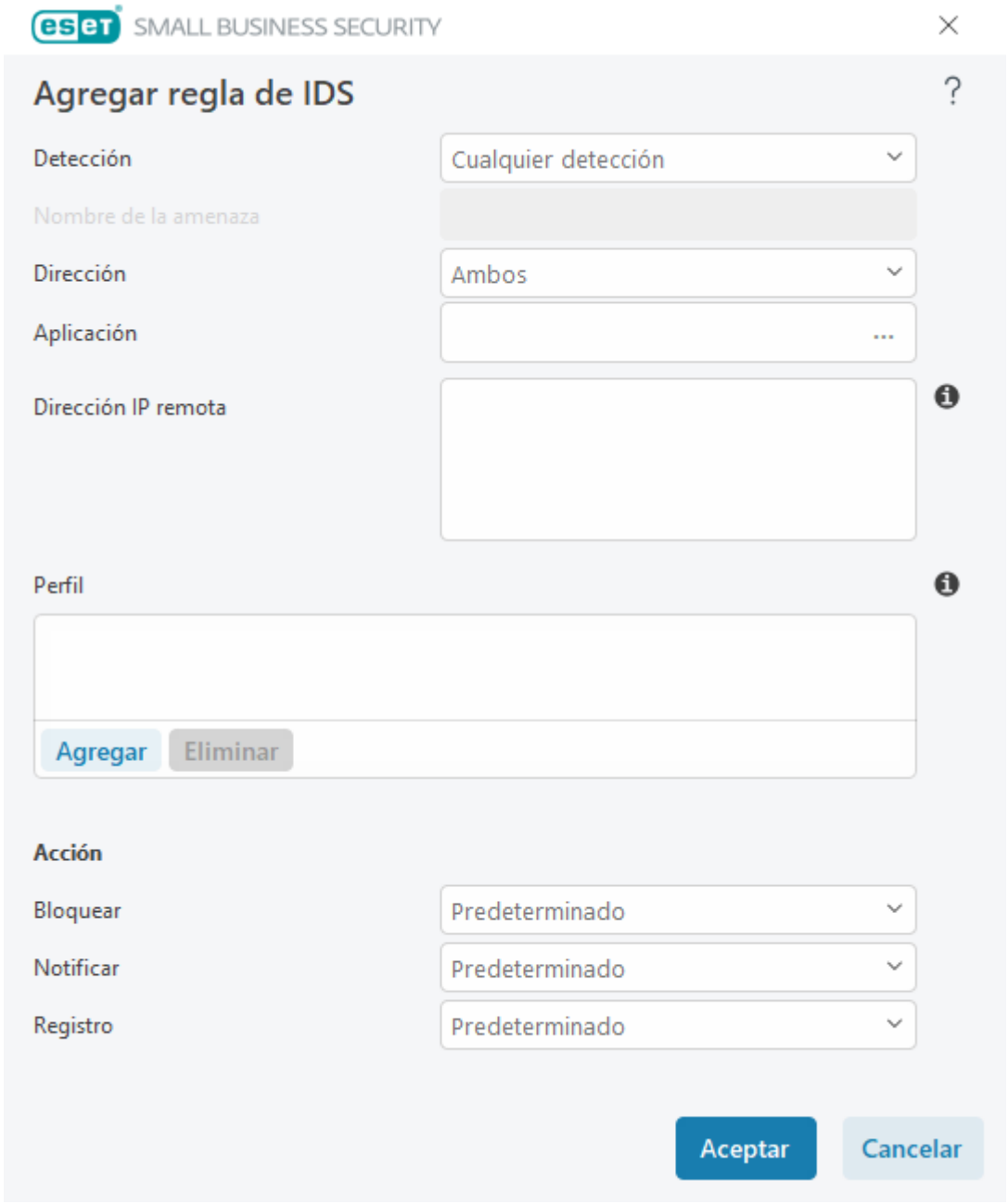
**Perfil**: puede elegir un perfil de conexión de red al que se aplicará esta regla.

### Acción

**Bloquear**: cada proceso del sistema tiene su propio comportamiento predeterminado y su propia acción asignada (bloquear o permitir). Si desea anular el comportamiento predeterminado de ESET Small Business Security, puede elegir la acción de bloquearlo o la acción de permitirlo en el menú desplegable.

**Notificar**: seleccione Sí para mostrar Notificaciones en el escritorio en su ordenador. Seleccione No si no desea notificaciones en el escritorio. Los valores disponibles son Predeterminado/Sí/No.

**Registrar**: seleccione **Sí** para registrar sucesos en los archivos de registro. Seleccione **No** si no desea registrar sucesos. Los valores disponibles son **Predeterminado**/**Sí**/**No**.




Si desea mostrar una notificación y recopilar un registro cada vez que se produzca el suceso:
1.Haga clic en **Agregar** para agregar una nueva regla de IDS.
2.Seleccione una detección específica en el menú desplegable **Detección**.
3.Haga clic en **...** para elegir la ruta de acceso de la aplicación para la que desea aplicar esta notificación.
4.Deje **Predeterminado** en el menú desplegable **Bloquear**. Se heredará la acción predeterminada aplicada por ESET Small Business Security.
5.Seleccione en el menú desplegable **Notificar** y en el menú desplegable **Registrar** la opción **Sí**.
6.Haga clic en **Aceptar** para guardar esta notificación.

Si no desea mostrar una notificación recurrente que no considera como una amenaza de un tipo concreto de **Detección**:

1.Haga clic en **Agregar** para agregar una nueva regla de IDS.

2.Seleccione una detección concreta en el menú desplegable **Detección**, por ejemplo, **Sesión SMB sin extensiones de seguridad** o **Ataque al puerto de exploración TCP**.

3.Seleccione **En** en el menú desplegable de dirección si el origen es una comunicación entrante.

4.En el menú desplegable **Notificar**, seleccione la opción **No**.

5.En el menú desplegable **Registrar**, seleccione la opción **Sí**.

6.Deje **Aplicación** en blanco.

7.Si la comunicación no procede de una dirección IP concreta, deje **Direcciones IP remotas** en blanco.

8.Haga clic en **Aceptar** para guardar esta notificación.

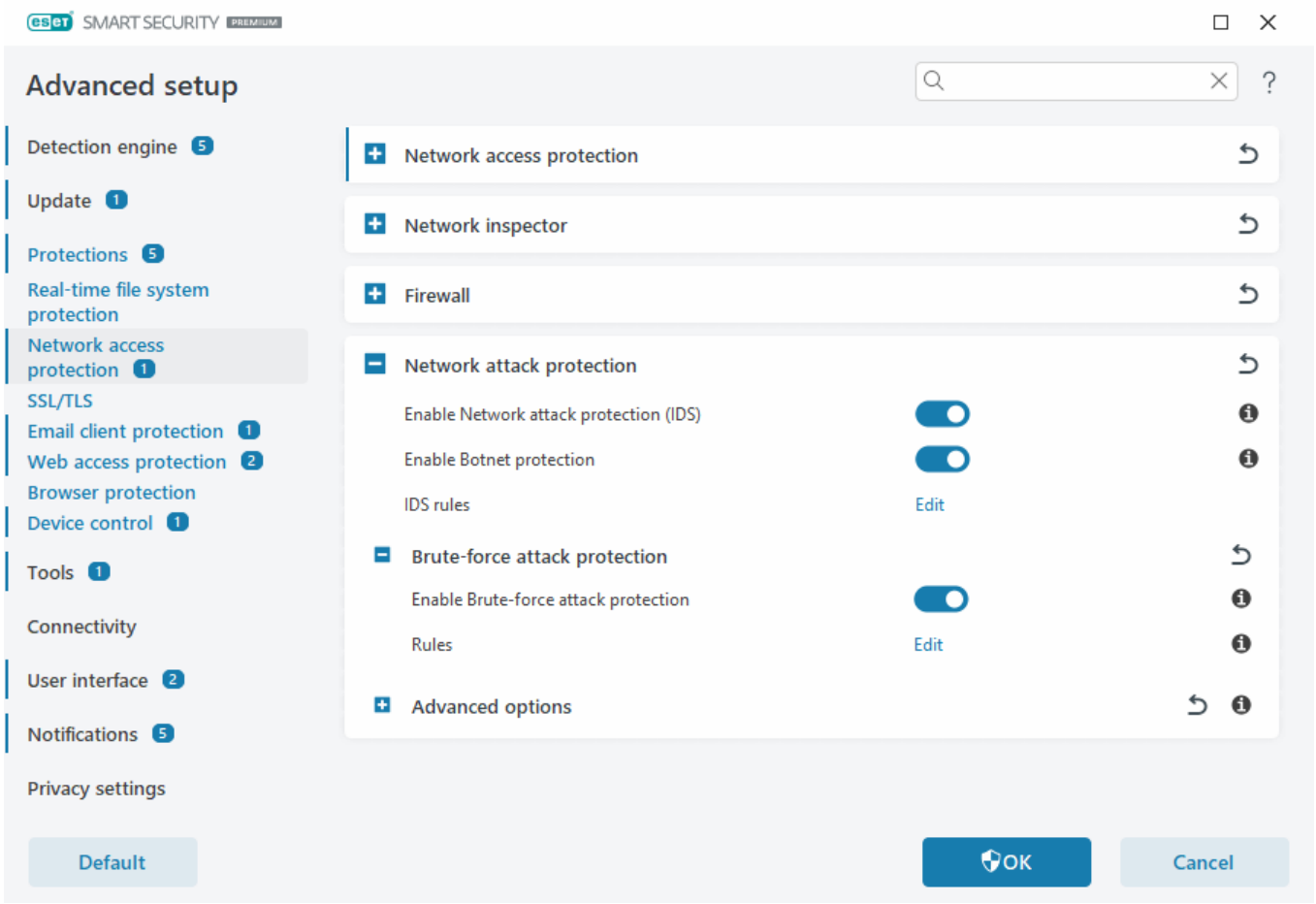
# Protección contra ataques de fuerza bruta

La protección contra ataques con fuerza bruta bloquea los ataques para adivinar contraseñas en los servicios RDP y SMB. Un ataque con fuerza es un método para descubrir una contraseña objetivo que consiste en probar de forma sistemática todas las combinaciones de letras, números y símbolos.

Para configurar la protección contra ataques de fuerza bruta, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red (IDS)** > **Protección contra ataques de fuerza bruta**.

**Activar la protección contra ataques de fuerza bruta**: ESET Small Business Security inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas.

**Reglas**: permiten crear, editar y ver reglas para las conexiones de red entrantes y salientes. Para obtener más información, consulte el capítulo Reglas.




# Reglas

Las reglas de protección contra ataques de fuerza bruta le permiten crear, editar y ver reglas para las conexiones de red entrantes y salientes. Las reglas predefinidas no se pueden editar ni eliminar.

## Administración de reglas de protección contra ataques de fuerza bruta

**Agregar**: crea una nueva regla.

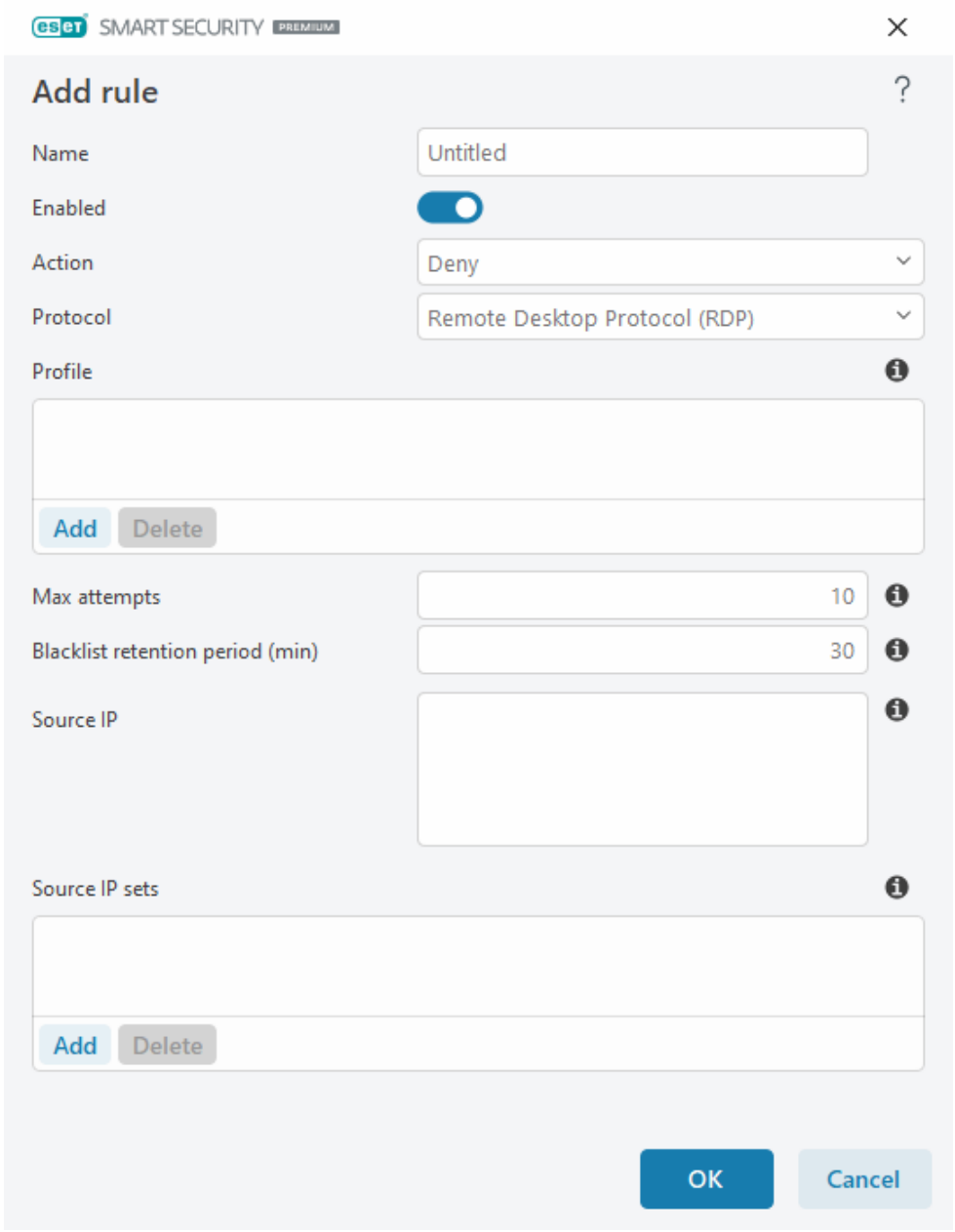
**Modificar**: modifique una regla existente.

**Eliminar**: quita una regla existente de la lista de reglas.

**Superior/Arriba/Abajo/Inferior:** ajusta el nivel de prioridad de las reglas.

> Para garantizar la máxima protección posible, se aplica la regla de bloqueo con el valor de **Número máximo de intentos** más bajo, aunque la regla esté situada más abajo en la lista de reglas cuando varias reglas de bloqueo cumplen las condiciones de detección.

## Editor de reglas




**Nombre**: nombre de la regla.

**Activado**: desactive el interruptor si desea conservar la regla en la lista, pero no aplicarla.

**Acción**: elija si desea **denegar** o **permitir** la conexión si se cumple la configuración de regla.

**Protocolo**: el protocolo de comunicación que inspeccionará esta regla.

**Perfil**: es posible definir reglas personalizadas y aplicarlas a perfiles concretos.

**Número máximo de intentos** – El número máximo de intentos permitidos de repetición de ataque hasta que la dirección IP se bloquea y se agrega a la lista negra.

**Periodo de retención de la lista negra (min)**: establece el tiempo para que la dirección caduque en la lista negra.

**IP de origen**: una lista de direcciones IP, rangos o subredes. Las direcciones deben separarse mediante comas.

**Conjuntos de IP de origen**: conjunto de direcciones IP que ya ha definido en Conjuntos de IP.

# Opciones avanzadas

En Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques de red (IDS)** > **Opciones avanzadas**, puede activar o desactivar la detección de varios tipos de ataques y vulnerabilidades que pueden dañar el ordenador.

En algunos casos no recibirá una notificación de amenaza sobre las comunicaciones bloqueadas. En la sección Registro y creación de reglas o excepciones del registro encontrará instrucciones para ver todas las comunicaciones bloqueadas en el registro del cortafuegos.

La disponibilidad de determinadas opciones de esta ventana puede variar en función del tipo o la versión de su producto de ESET y el módulo Cortafuegos, así como de la versión de su sistema operativo.

## Detección de intrusiones

La detección de intrusiones supervisa la comunicación de red del dispositivo en busca de actividades maliciosas.

- **Protocolo SMB**: detecta y bloquea los siguientes problemas de seguridad del protocolo SMB.
- **Protocolo RPC**: detecta y bloquea varios identificadores de CVE en el sistema de llamadas de procedimiento remoto desarrollado para el Entorno de computación distribuida (DCE).
- **Protocolo RDP**: detecta y bloquea distintos identificadores de CVE en el protocolo RDP (consulte la información previa).
- **Detección del ataque por envenenamiento ARP**: detección de ataques por envenenamiento ARP provocados por ataques de interceptación o detección por rastreo en el conmutador de red. La aplicación de red o el dispositivo utiliza ARP (Protocolo de resolución de direcciones) para determinar la dirección Ethernet.
- **Detección del ataque de exploración de puerto TCP/UDP**: detecta ataques de software de análisis de puertos; aplicación diseñada para detectar si existen puertos abiertos en un host enviando al cliente solicitudes para un intervalo de direcciones de puertos, con el objetivo de encontrar puertos activos y aprovechar la vulnerabilidad del servicio. Puede obtener más información sobre este tipo de ataque en el glosario.
- **Bloquear la dirección no segura una vez detectado el ataque**: las direcciones IP que se han detectado como fuentes de ataques se agregan a la lista negra para evitar la conexión durante un determinado periodo de tiempo. Puede definir el **Período de retención de la lista negra**, que establece el tiempo durante el que se bloqueará la dirección después de la detección del ataque.
- **Mostrar notificación tras la detección de un ataque**: activa el área de notificación de Windows en la esquina inferior derecha de la pantalla.
- **Mostrar notificaciones al recibir ataques que aprovechen de fallos de seguridad**: le avisa si se detectan ataques contra vulnerabilidades de seguridad o si una amenaza intenta acceder al sistema a través de este método.

## Comprobación de paquetes

Un tipo de análisis de paquetes que filtra los datos que se transfieren a través de la red.

- **Permitir una conexión entrante para intercambio de admin en el protocolo de SMB**: los recursos

compartidos administrativos (recursos compartidos del administrador) son los recursos compartidos de red predeterminados que comparten particiones del disco duro (*C$*, *D$*, etc.) en el sistema con la carpeta del sistema (*ADMIN$*). La desactivación de la conexión a los recursos compartidos del administrador debería mitigar muchos riesgos de seguridad. Por ejemplo, el gusano Conficker realiza ataques por diccionario para conectarse a recursos compartidos del administrador.

- **Denegar dialectos SMB anteriores (no compatibles)**: permite denegar sesiones SMB que utilicen un dialecto SMB anterior incompatible con IDS. Los sistemas operativos Windows modernos son compatibles con dialectos SMB anteriores gracias a la compatibilidad con sistemas operativos anteriores como Windows 95. El atacante puede utilizar un dialecto anterior en una sesión SMB para evadir la inspección de tráfico. Deniegue dialectos SMB anteriores si su ordenador no necesita compartir archivos (o utilizar la comunicación SMB en general) con un ordenador con una versión anterior de Windows.

- **Denegar la seguridad de SMB sin extensiones de seguridad**: la seguridad ampliada se puede utilizar durante la negociación de la sesión de SMB para proporcionar un mecanismo de autenticación más seguro que la autenticación de desafío o respuesta de LAN Manager (LM). El esquema de LM se considera débil, por lo que no se recomienda su uso.

- **Denegar apertura de archivos ejecutables en un servidor fuera de la zona de confianza en el protocolo SMB**: finaliza la conexión cuando se intenta abrir un archivo ejecutable (.exe, .dll, ...) desde una carpeta compartida en el servidor que no se encuentra en la zona de confianza del cortafuegos. Tenga en cuenta que copiar archivos ejecutables desde orígenes de confianza puede ser legítimo. Tenga en cuenta que la copia de archivos ejecutables desde fuentes de confianza puede ser legítima; no obstante, esta detección debería mitigar el riesgo de abrir accidentalmente un archivo de un servidor malicioso (por ejemplo, un archivo abierto al hacer clic en un enlace a un archivo ejecutable malicioso compartido).

- **Denegar la autenticación de NTLM en el protocolo de SMB para conectarse al servidor en la Zona de confianza/fuera de la Zona de confianza**: los protocolos que utilizan los esquemas de autenticación de NTLM (ambas versiones) pueden verse afectados por un ataque de envío de credenciales (conocido como ataque de retransmisión SMB en el caso del protocolo de SMB). La denegación de la autenticación de NTLM con un servidor fuera de la zona de confianza debería mitigar los riesgos de envío de credenciales por parte de un servidor malicioso fuera de la zona de confianza. Asimismo, puede denegar la autenticación de NTLM con servidores de la zona de confianza.

- **Permitir la comunicación con el servicio Security Account Manager**: para obtener más información sobre este servicio, consulte [MS-SAMR].

- **Permitir la comunicación con el servicio Local Security Authority**: para obtener más información sobre este servicio, consulte [MS-LSAD] y [MS-LSAT].

- **Permitir la comunicación con el servicio Remote Registry**: para obtener más información sobre este servicio, consulte [MS-RRP].

- **Permitir la comunicación con el servicio Services Control Manager**: para obtener más información sobre este servicio, consulte [MS-SCMR].

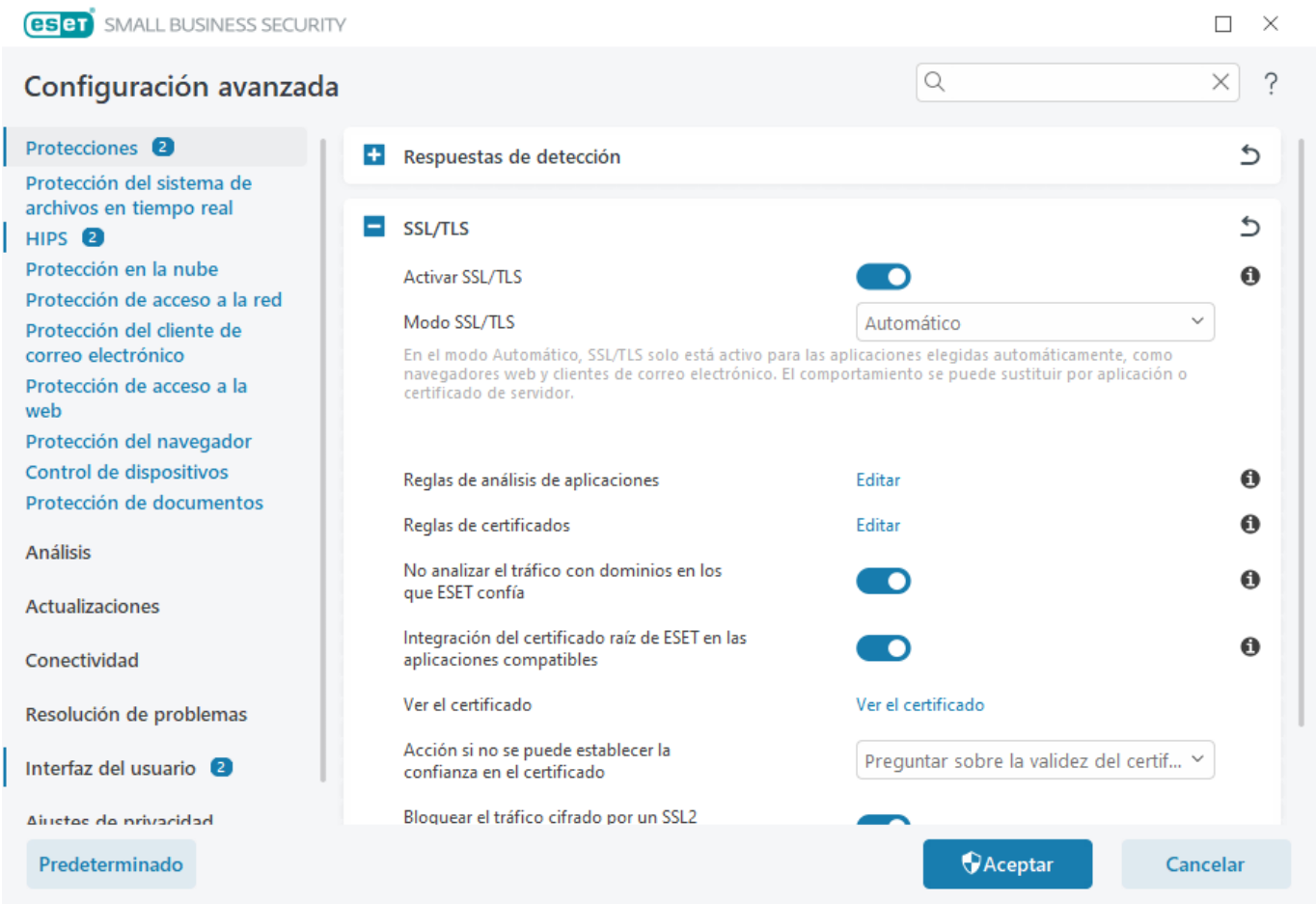
- **Permitir la comunicación con el Server Service**: para obtener más información sobre este servicio, consulte [MS-SRVS].

- **Permitir la comunicación con los otros servicios**: otros servicios de MSRPC. MSRPC es la implementación de Microsoft del mecanismo DCE RPC. Además, MSRPC puede utilizar aperturas de acceso con nombre en el protocolo SMB (intercambio de archivos en la red) para el transporte (transporte ncacn_np). Los servicios de

MSRPC proporcionan interfaces para acceder a sistemas Windows y administrarlos de forma remota. Se han detectado y aprovechado varias vulnerabilidades de seguridad en estado salvaje en el sistema MSRPC de Windows (gusano Conficker, gusano Sasser…). Desactive la comunicación con los servicios de MSRPC que no necesite proporcionar para mitigar muchos riesgos de seguridad (como la ejecución de código remoto o los ataques por fallo del servicio).

# SSL/TLS

ESET Small Business Security puede comprobar si hay amenazas de comunicación que utilizan el protocolo SSL. Puede utilizar varios modos de filtrado para examinar las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos del análisis de comunicaciones protegidas mediante el protocolo SSL. Para editar la configuración de SSL/TLS, abra Configuración avanzada > **Protecciones** > **SSL/TLS**.




**Activar SSL/TLS**: si esta opción está desactivada, ESET Small Business Security no analizará la comunicación a través de SSL/TLS.

**El modo SSL/TLS** ofrece las siguientes opciones:

| Modo de filtrado | Descripción |
|---|---|
| **Automático** | El modo predeterminado solo analizará las aplicaciones correspondientes, como navegadores de Internet y clientes de correo. Puede anularlo seleccionando las aplicaciones donde se analiza la comunicación. |
| **Interactivo** | Si entra en un sitio nuevo protegido mediante SSL (con un certificado desconocido), se muestra un cuadro de diálogo con las acciones posibles. Este modo le permite crear una lista de aplicaciones o certificados SSL que se excluirán del análisis. |

| Modo de filtrado | Descripción |
| --- | --- |
| **Modo basado en políticas** | Seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL, excepto las protegidas por certificados excluidos del análisis. Si se establece una comunicación nueva que utiliza un certificado firmado desconocido, no se le informará y la comunicación se filtrará automáticamente. Si accede a un servidor con un certificado que no sea de confianza pero que usted ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación. |

**Reglas de análisis de aplicaciones**: permite personalizar el comportamiento ESET Small Business Security de aplicaciones específicas.

**Reglas de certificados**: permite personalizar el comportamiento de ESET Small Business Security para certificados SSL específicos.

**No analizar el tráfico con dominios en los que ESET confía**: cuando esta opción está activada, la comunicación con dominios de confianza se excluye del análisis. Una lista blanca integrada administrada por ESET determina la fiabilidad de un dominio.

**Integración del certificado raíz de ESET en las aplicaciones compatibles**: para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). Cuando esté activada, ESET Small Business Security agregará el certificado ESET SSL Filter CA a los navegadores conocidos (por ejemplo, Opera) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente. Por ejemplo, Firefox está configurado automáticamente para confiar en entidades de certificación raíz del almacén de certificados del sistema.

Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

**Acción si no se puede establecer la confianza en el certificado**: en algunos casos, un certificado de sitio web no se puede comprobar mediante el almacén de entidades de certificación raíz de confianza (TRCA) (por ejemplo, un certificado caducado, un certificado que no es de confianza, un certificado no válido para el dominio específico o una firma que se puede analizar pero no firma el certificado correctamente). Los sitios web legítimos siempre utilizarán certificados de confianza. Si no proporcionan uno, podría significar que un atacante está descifrando la comunicación o que el sitio web está experimentando dificultades técnicas.

Si se ha seleccionado la opción **Preguntar sobre la validez del certificado** (seleccionada de forma predeterminada), se le pedirá que seleccione la acción cuando se establezca la comunicación cifrada. Se mostrará un cuadro de diálogo de selección que le permite marcar el certificado como de confianza o excluirlo. Si el certificado no se encuentra en la lista de TRCA, la ventana se mostrará en rojo. Si el certificado se encuentra en la lista de TRCA, la ventana se mostrará en verde.

**Bloquear las comunicaciones que usan el certificado** se puede seleccionar para cerrar siempre las conexiones cifradas con los sitios que utilicen un certificado sin verificar.

**Bloquear tráfico cifrado por SSL2 obsoleto**: la comunicación que utiliza la versión anterior del protocolo SSL se bloqueará automáticamente.

**Acción para certificados dañados**: un certificado dañado es un certificado que utiliza un formato no reconocido por ESET Small Business Security o que se ha dañado (por ejemplo, sobrescrito por datos aleatorios). En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**. Si se selecciona **Preguntar sobre la validez del certificado**, se solicita al usuario que elija la acción que desea cuando se establezca la comunicación cifrada.

Ejemplos ilustrados.

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- Notificaciones de certificados en productos para oficina pequeña de ESET para Windows
- «Tráfico de red cifrado certificado no de confianza» se muestra al visitar páginas web

# Reglas de análisis de aplicaciones

Las **reglas de análisis de aplicaciones** se pueden utilizar para personalizar el comportamiento de ESET Small Business Security para determinadas aplicaciones, así como para recordar las acciones elegidas cuando el **Modo SSL/TLS** está en el **Modo interactivo**. La lista se puede ver y editar en Configuración avanzada > **Protecciones** > **SSL/TLS** > **Reglas de análisis de aplicaciones** > **Editar**.

La ventana **Reglas de análisis de aplicaciones** consta de:

## Columnas

**Aplicación**: seleccione un archivo ejecutable en el árbol de directorios y haga clic en la opción **...**, o introduzca la ruta manualmente.

**Acción de análisis**: seleccione **Analizar** o **Ignorar** para analizar o ignorar la comunicación. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

## Elementos de control

**Agregar**: agregue la aplicación filtrada.

**Editar**: seleccione la aplicación que desea configurar y haga clic en **Editar**.

**Eliminar**: seleccione la aplicación que desea eliminar y haga clic en **Eliminar**.

**Importar**/**Exportar**: importe aplicaciones desde un archivo o guarde la lista actual de aplicaciones en un archivo.

**Aceptar**/**Cancelar**: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

# Reglas de certificados

**Las reglas de certificados** se pueden usar para personalizar el comportamiento de ESET Small Business Security para certificados SSL específicos y para recordar las acciones elegidas cuando el **modo SSL/TLS** está en **modo interactivo**. La lista se puede ver y editar en Configuración avanzada > **Protecciones** > **SSL/TLS** > **Reglas de certificados** > **Editar**.

La ventana **Reglas de certificados** consta de:

## Columnas

**Nombre**: nombre del certificado.

**Emisor del certificado**: nombre del creador del certificado.

**Sujeto del certificado**: en este campo se identifica a la entidad asociada a la clave pública almacenada en el campo de clave pública del asunto.

**Acceso**: seleccione **Permitir** o **Bloquear** como **Acción del acceso** para permitir o bloquear la comunicación que protege este certificado, independientemente de su fiabilidad. Seleccione **Auto** para permitir los certificados de confianza y preguntar cuando uno no sea de confianza. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

**Analizar**: seleccione **Analizar** o **Ignorar** como **Acción de análisis** para analizar o ignorar la comunicación que protege este certificado. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

## Elementos de control

**Agregar** – agrega un certificado nuevo y ajusta su configuración de opciones de análisis y acceso.

**Editar**: seleccione el certificado que desea configurar y haga clic en **Editar**.

**Eliminar**: seleccione el certificado que desea eliminar y haga clic en **Quitar**.

**Aceptar/Cancelar**: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

# Tráfico de red cifrado

Si el sistema está configurado para utilizar el análisis SSL/TLS, se mostrará un cuadro de diálogo para solicitarle que seleccione una acción en dos situaciones diferentes:

En primer lugar, si un sitio web utiliza un certificado no válido o que no se puede verificar y ESET Small Business Security está configurado para preguntar al usuario en estos casos (la opción predeterminada es sí para los certificados que no se pueden verificar y no para los que no son válidos), se abre un cuadro de diálogo para preguntarle si desea **Permitir** o **Bloquear** la conexión. Si el certificado no está en el Trusted Root Certification Authorities store (TRCA), se considera no fiable.

En segundo lugar, si el **modo SSL/TLS** está establecido en **Modo interactivo**, se mostrará un cuadro de diálogo para cada sitio web para preguntarle si desea **Analizar** o **Ignorar** el tráfico. Algunas aplicaciones comprueban que nadie haya modificado ni inspeccionado su tráfico SSL en estos casos, ESET Small Business Security debe **Ignorar** el tráfico para que la aplicación siga funcionando.

> **Ejemplos ilustrados.**
> Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:
> - Notificaciones de certificados en productos para oficina pequeña de ESET para Windows
> - «Tráfico de red cifrado certificado no de confianza» se muestra al visitar páginas web

En ambos casos, el usuario tiene la opción de recordar la acción seleccionada. Las acciones guardadas se almacenan en las Reglas de certificados.

# Protección del cliente de correo electrónico

Para configurar la protección del cliente de correo electrónico, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** y elija una de las siguientes opciones de configuración:

- Protección del correo electrónico
- Protección del buzón de correo
- ThreatSense

# Protección del correo electrónico

Los protocolos IMAP(S) y POP3(S) son los más utilizados para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. El Protocolo de acceso a mensajes de Internet (IMAP) es otro protocolo de Internet para la recuperación de mensajes de correo electrónico. IMAP presenta algunas ventajas sobre POP3; por ejemplo, permite la conexión simultánea de varios clientes al mismo buzón de correo y conserva la información de estado (si el mensaje se ha leído, contestado o eliminado). El módulo de protección que ofrece este control se inicia automáticamente al iniciar el sistema y, a continuación, está activo en la memoria.

ESET Small Business Security proporciona protección para estos protocolos, independientemente del cliente de correo electrónico utilizado, y sin necesidad de volver a configurar el cliente de correo electrónico. De forma predeterminada, se analiza toda la comunicación a través de los protocolos POP3 e IMAP, independientemente de los números de puerto POP3/IMAP predeterminados.
El protocolo MAPI no se analiza. Sin embargo, la comunicación con el servidor de Microsoft Exchange se puede analizar con el módulo de integración de clientes de correo electrónico como Microsoft Outlook.

ESET Small Business Security también admite el análisis de los protocolos IMAPS (585, 993) y POP3S (995), que utilizan un canal cifrado para transferir información entre el servidor y el cliente. ESET Small Business Security comprueba la comunicación con los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte).
La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, abra Configuración avanzada > **Protecciones** SSL/TLS.

Para configurar Protección del transporte de correo electrónico, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del transporte de correo electrónico**.

**Activar Protección del transporte de correo electrónico**: cuando está activada, la comunicación de transporte de correo está analizada por ESET Small Business Security.

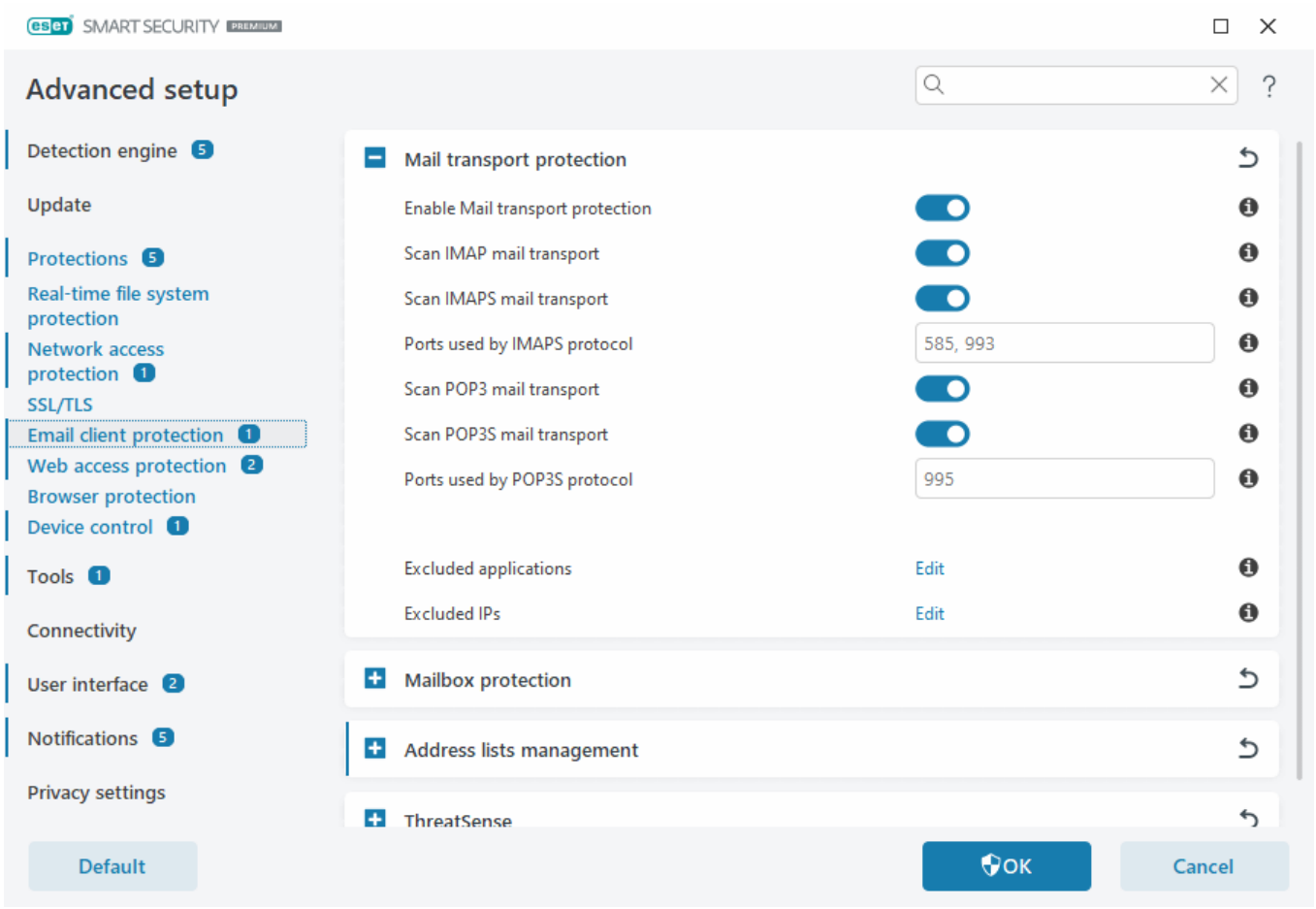
Puede elegir qué protocolos de transporte de correo se analizarán haciendo clic en el interruptor situado junto a las siguientes opciones (de forma predeterminada, está activado el análisis de todos los protocolos):

- **Analizar el transporte de correo IMAP**
- **Analizar el transporte de correo IMAPS**
- **Analizar el transporte de correo POP3**
- **Analizar el transporte de correo POP3S**

De forma predeterminada, ESET Small Business Security analizará la comunicación IMAPS y POP3S en los puertos estándar. Para agregar puertos personalizados para los protocolos IMAPS y POP3S, agréguelos al campo de texto junto a **Puertos usados por el protocolo IMAPS** o **Puertos usados por el protocolo POP3S**. Cuando haya varios números de puerto, deben delimitarse con una coma.

Aplicaciones excluidas: permite excluir aplicaciones específicas del análisis de Protección del transporte de correo electrónico. Útil cuando Protección de acceso a la web causa problemas de compatibilidad.

IP excluidas: permite excluir direcciones remotas específicas del análisis de Protección del transporte de correo electrónico. Útil cuando Protección de acceso a la web causa problemas de compatibilidad.



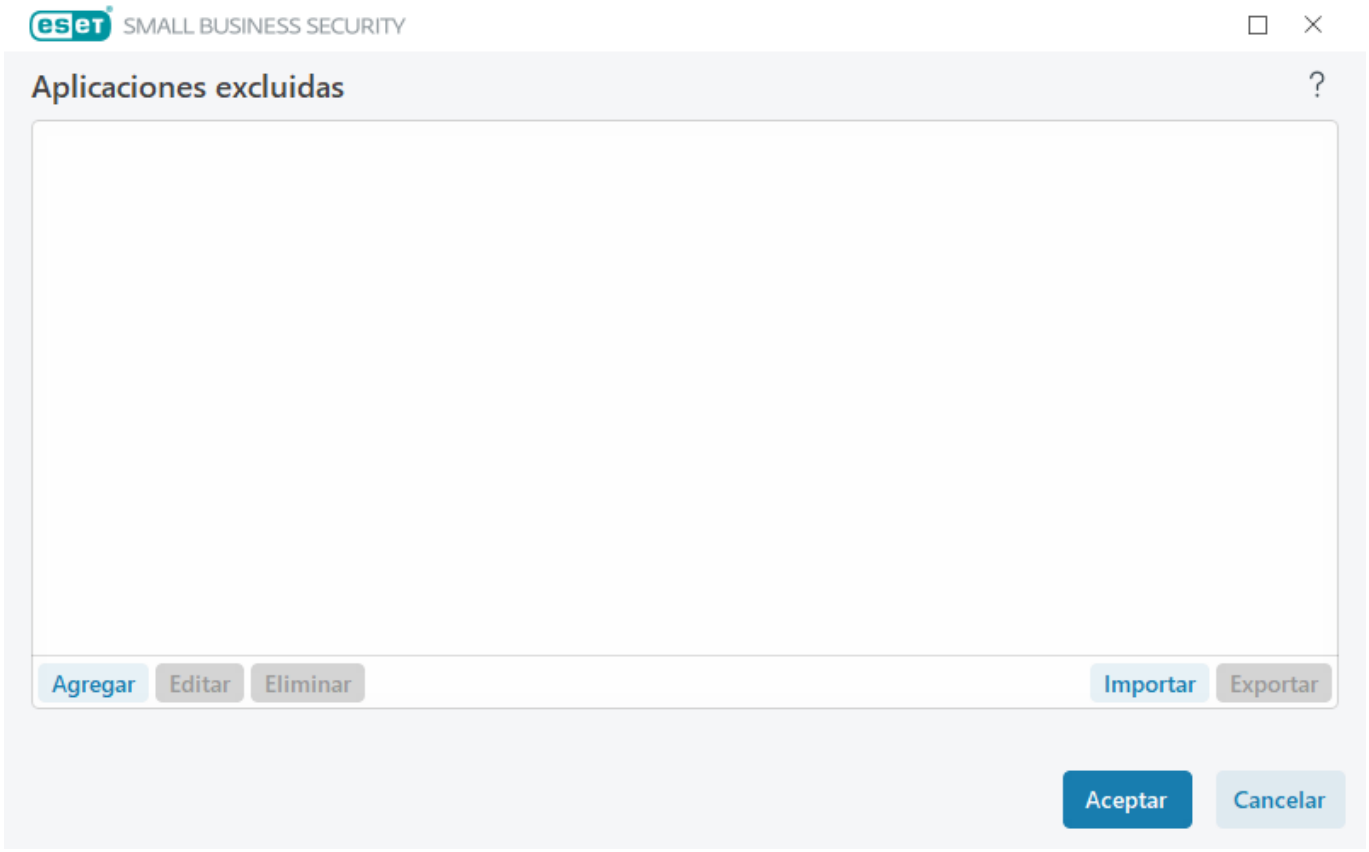

# Aplicaciones excluidas

Para excluir el análisis de la comunicación para aplicaciones específicas, añádalas a la lista. No se comprobará la presencia de amenazas en la comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas. Se recomienda su uso únicamente en aplicaciones que no funcionen correctamente cuando se compruebe su comunicación.

Las aplicaciones y los servicios en ejecución estarán disponibles aquí de forma automática cuando haga clic en **Agregar**. Haga clic en **...** y navegue hasta una aplicación para agregar la exclusión manualmente.

**Modificar**: modifique las entradas seleccionadas de la lista.

**Eliminado**: elimina las entradas seleccionadas de la lista.



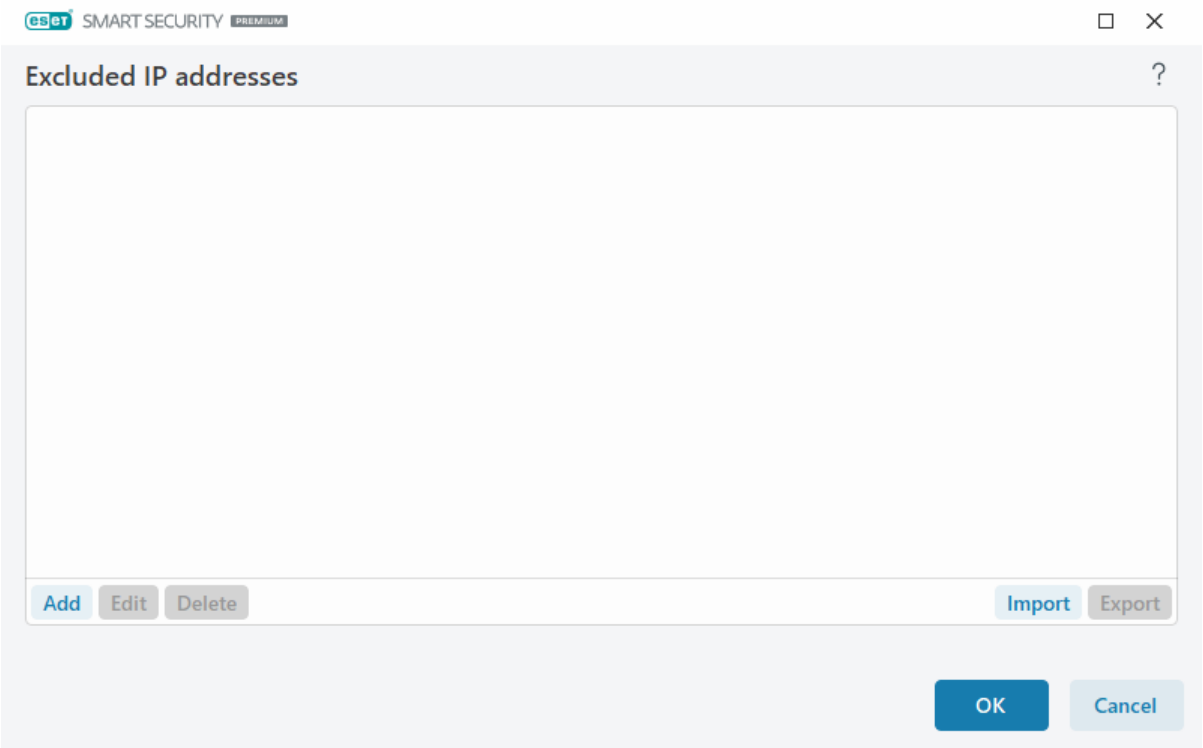

# IP excluidas

Las entradas de la lista se excluirán del análisis. No se comprobará la presencia de amenazas en las comunicaciones HTTP(S)/POP3(S)/IMAP(S) entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Haga clic en **Agregar** para excluir una dirección IP, un rango de direcciones o una subred de un punto remoto.

Haga clic en **Editar** para cambiar la dirección IP seleccionada.

Haga clic en **Eliminar** para quitar las entradas seleccionadas de la lista.




### Ejemplos de direcciones IP

Agregar dirección IPv4:
**Dirección única**: agrega la dirección IP de un ordenador concreto (por ejemplo, *192.168.0.10*).
**Rango de direcciones**: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones de varios ordenadores (por ejemplo, *192.168.0.1-192.168.0.99*).
**Subred**: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red de la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.
Agregar dirección IPv6:
**Dirección única**: agrega la dirección IP de un ordenador concreto (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
**Subred**: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

# Protección del buzón de correo

La integración de ESET Small Business Security con el buzón de correo aumenta el nivel de protección activa contra código malicioso en los mensajes de correo electrónico.

Para configurar la protección del buzón, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón de correo**.

**Activar protección del correo electrónico mediante complementos del cliente**: cuando esta opción está desactivada, la protección mediante complementos del cliente de correo electrónico está desactivada.

Seleccione los mensajes de correo electrónico que desea analizar:

- **Correo electrónico recibido**
- **Correo electrónico enviado**
- **Correo electrónico leído**

- **Correo electrónico modificado**

Se recomienda mantener la opción **Activar protección del correo electrónico mediante complementos del cliente** activada. Aunque la integración no esté activada o no funcione, la comunicación por correo electrónico sigue estando protegida por Protección del transporte de correo electrónico (IMAP/IMAPS y POP3/POP3S).

## Analizar en busca de spam

El correo electrónico no solicitado, llamado spam, es uno de los problemas más graves de la comunicación electrónica. Representa hasta el 30 % de todas las comunicaciones por correo electrónico. Antispam del cliente de correo electrónico sirve para proteger contra este problema. Antispam del cliente de correo electrónico, que combina varios principios de seguridad del correo electrónico, ofrece un filtrado superior para que la bandeja de entrada siga siempre limpia. En la detección de spam, un principio importante es reconocer los mensajes de correo electrónico no solicitados a partir de direcciones de confianza predefinidas (permitidas) y direcciones de spam (bloqueadas).

El principal método utilizado para detectar spam es el análisis de las propiedades de los mensajes de correo electrónico. Los mensajes recibidos se analizan con criterios básicos contra correo no deseado (definiciones de mensajes, heurística estadística, algoritmos reconocidos y otros métodos únicos) y el valor del índice resultante determina si un mensaje es deseado o no deseado.

**Activar Antispam del cliente de correo electrónico**: cuando está activado, los mensajes recibidos se analizan en busca de spam.

**Utilizar análisis avanzado de spam**: periódicamente se descargarán datos antispam adicionales, lo que aumentará las capacidades antispam y producirá mejores resultados.

**Registro del nivel de spam**: el motor antispam de ESET Small Business Security asigna un nivel de spam a cada uno de los mensajes analizados. El mensaje se anotará en el Registro de protección antispam (ventana principal del programa > **Herramientas** > **Archivos de registro** > **Antispam del cliente de correo electrónico**).

- **Ninguno**: no se registrará el nivel obtenido en el análisis de correo no deseado.
- **Reclasificado y marcado como SPAM**: seleccione esta opción si desea registrar un nivel de SPAM a los mensajes marcados como correo no deseado.
- **Todos**: todos los mensajes se anotarán en el registro con un nivel de spam.

Cuando hace clic en un mensaje de la carpeta de correo no deseado puede elegir **Reclasificar como correo deseado** y el mensaje se enviará a la bandeja de entrada. Si hace clic en un mensaje de la bandeja de entrada que considera como correo no deseado, seleccione **Reclasificar mensajes como correo no deseado** y el mensaje se enviará a la carpeta de correo no deseado. Puede seleccionar varios mensajes y actuar en todos ellos simultáneamente.

**Optimización de la gestión de los archivos adjuntos**: si la optimización está desactivada, todos los archivos adjuntos se analizan inmediatamente. Puede que el rendimiento del cliente de correo electrónico se ralentice.

**Integraciones**: le permite integrar la protección del buzón de correo en el cliente de correo electrónico. Consulte Integraciones para obtener más información.

**Respuesta**: le permite personalizar la gestión de los mensajes de spam. Consulte Respuesta para obtener más información.

# Integraciones

La integración de ESET Small Business Security con su cliente de correo electrónico aumenta el nivel de protección activa contra código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, puede activar la integración en ESET Small Business Security. Cuando se integra en el cliente de correo electrónico, la barra de herramientas de ESET Small Business Security se inserta directamente en el cliente de correo electrónico, aumentando así la eficacia de la protección del correo electrónico.

Para editar la configuración de integración, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón de correo** > **Integración**.

**Integrar con Microsoft Outlook**: actualmente, Microsoft Outlook es el único cliente de correo electrónico compatible. La protección de correo electrónico funciona como un plugin. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus. Para ver una lista completa de versiones de Microsoft Outlook compatibles, consulte este artículo de la base de conocimiento de ESET.

**Procesamiento avanzado del cliente de correo electrónico**: procesa eventos de Outlook Messaging API (MAPI) adicionales: Objeto modificado (`fnevObjectModified`) y Objeto creado (`fnevObjectCreated`). Si el sistema funciona más lento de lo normal cuando trabaja con el cliente de correo electrónico, desactive esta opción.

# Barra de herramientas de Microsoft Outlook

La protección de Microsoft Outlook funciona como un módulo de plugin. Una vez instalado ESET Small Business Security, esta barra de herramientas que contiene las opciones de la protección antivirus y el Antispam del cliente de correo electrónico se agrega a Microsoft Outlook:

**Correo no deseado**: marca los mensajes seleccionados como correo no deseado. Después de marcar, se envía una “huella” del mensaje a un servidor central que almacena firmas de correo no deseado. Si el servidor recibe más "huellas" similares de varios usuarios, el mensaje se clasificará como correo no deseado en el futuro.

**Correo deseado**: marca los mensajes seleccionados como correo deseado.

**Direcciones de spam** (bloqueadas; lista de direcciones de spam): agrega una nueva dirección de remitente a la lista de direcciones como Bloqueada. Todos los mensajes recibidos de la lista se clasifican automáticamente como correo no deseado.

Tenga cuidado con el spoofing (o falsificación de la dirección de un remitente en mensajes de correo electrónico), que se utiliza para engañar a los receptores de los mensajes para que los lean y los contesten.

**Direcciones de confianza** (permitidas; lista de direcciones de confianza): agrega una nueva dirección de remitente a la lista de direcciones como Permitida. Los mensajes recibidos de direcciones permitidas no se clasificarán nunca como spam de forma automática.

**ESET Small Business Security**: Haga doble clic en el icono para abrir la ventana principal de ESET Small Business Security.

**Analizar de nuevo los mensajes**: le permite iniciar la comprobación del correo electrónico de forma manual. Puede especificar los mensajes que se comprobarán y activar un nuevo análisis del correo recibido. Para obtener más información, consulte Protección del buzón de correo.

**Configuración del análisis**: muestra las opciones de configuración de Protección del buzón de correo.

**Configuración del Correo no deseado**: muestra las opciones de configuración de Protección del buzón de correo.

**Libretas de direcciones**: abre la ventana Administración de listas de direcciones, en la que puede acceder a las listas de direcciones de correo no deseado, de confianza y excluidas.

# Cuadro de diálogo de confirmación

Esta notificación sirve para comprobar que el usuario realmente desea realizar la acción seleccionada, de forma que se deberían eliminar los posibles errores.

Por otra parte, el cuadro de diálogo también ofrece la posibilidad de desactivar las confirmaciones.

# Analizar de nuevo los mensajes

La barra de herramientas de ESET Small Business Security integrada en los clientes de correo electrónico permite a los usuarios especificar varias opciones de análisis del correo electrónico. La opción **Analizar de nuevo los mensajes** ofrece dos modos de análisis:

**Todos los mensajes de la carpeta actual**: analiza los mensajes de la carpeta que se muestra en ese momento.

**Solo los mensajes seleccionados**: analiza únicamente los mensajes marcados por el usuario.

La casilla de verificación **Volver a analizar los mensajes ya analizados** proporciona una opción para ejecutar otro análisis en mensajes ya analizados.

# Respuesta

Según los resultados del análisis de mensajes, ESET Small Business Security puede mover los mensajes analizados o agregar texto personalizado al asunto. Puede configurar estas opciones en Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Protección del buzón de correo** > **Respuesta**.

Antispam del cliente de correo electrónico en ESET Small Business Security le permite configurar los siguientes parámetros para los mensajes:

**Agregar texto al asunto del mensaje**: le permite agregar un prefijo personalizado a la línea de asunto de los mensajes que se han clasificado como correo electrónico no deseado. El **texto** predeterminado es "[SPAM]".

**Mover a carpeta de spam**: si esta opción está activada, los mensajes no deseados se moverán a la carpeta predeterminada de correo basura, y los mensajes reclasificados como correo deseado se moverán a la bandeja de entrada. Cuando hace clic con el botón derecho del ratón en un mensaje de correo electrónico y selecciona ESET

Small Business Security en el menú contextual puede elegir entre las opciones aplicables.

**Mover a carpeta personalizada**: cuando esta opción está activada, los mensajes de spam se mueven a una carpeta especificada a continuación.

**Carpeta**: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Si hay un mensaje que contiene detección, de forma predeterminada, ESET Small Business Security intenta desinfectar el mensaje. Si el mensaje no se puede desinfectar, puede elegir una **Acción a emprender si no es posible la desinfección**:

- **Sin acciones**: si esta opción está activada, el programa identificará los archivos adjuntos infectados, pero dejará los mensajes sin realizar ninguna acción.
- **Eliminar mensajes**: el programa informará al usuario sobre las amenazas y eliminará el mensaje.
- **Mover el correo electrónico a la carpeta de elementos eliminados**: los mensajes infectados se moverán automáticamente a la carpeta Elementos eliminados.
- **Mover mensajes a la carpeta** (acción predeterminada): los mensajes de correo electrónico infectados se moverán automáticamente a la carpeta especificada.

**Carpeta**: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

**Marcar los mensajes de spam como leídos**: active esta opción para marcar el correo no deseado como leído de forma automática. Esto le ayudará a centrar su atención en los mensajes "desinfectados".

**Marcar los mensajes reclasificados como no leídos**: se mostrarán como no leídos los mensajes que originalmente se clasificaron como correo no deseado, pero que después se marcaron como "desinfectados".

Después de analizar un mensaje de correo electrónico, se puede adjuntar al mensaje una notificación del análisis. Puede elegir entre las opciones **Notificar en los mensajes recibidos y leídos** o **Notificar en los mensajes enviados**.

Tenga en cuenta que en ocasiones puntuales es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o que hayan sido falsificados por código malicioso. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Están disponibles las opciones siguientes:

- **Nunca**: no se agregará ningún mensaje de etiqueta.
- **Cuando se produce una detección**: únicamente se marcarán como analizados los mensajes que contengan software malicioso (opción predeterminada).
- **A todo el correo electrónico cuando se analiza**: el programa agregará un mensaje a todo el correo analizado.

**Actualizar asunto de los correos electrónicos recibidos y leídos/Actualizar asunto de los correos electrónicos enviados**: active esta opción para agregar texto personalizado especificado a continuación al mensaje.

**Texto que se agrega al asunto de los correos electrónicos detectados**: edite esta plantilla si desea modificar el formato de prefijo del asunto de un mensaje de correo electrónico infectado. Esta función sustituye el asunto del mensaje "Hello" por el siguiente formato: "[detection %DETECTIONNAME%] Hello". La variable %DETECTIONNAME% representa la amenaza detectada.

# ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor de ThreatSense le permiten especificar varios parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

## Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

**Memoria operativa**: busca amenazas que ataquen a la memoria operativa del sistema.

**Sectores de inicio/UEFI**: analiza los sectores de inicio para detectar malware en el registro de inicio principal. Lea más sobre la UEFI en el glosario.

**Archivos de correo**: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

**Archivos comprimidos**: el programa es compatible con las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

**Archivos comprimidos autoextraíbles**: los archivos comprimidos autoextraíbles (SFX) son archivos comprimidos que pueden extraerse por sí solos.

**Empaquetadores en tiempo de ejecución**: después de su ejecución, los empaquetadores en tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

## Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

**Heurística**: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

**Heurística avanzada/ADN inteligentes**: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

## Desinfección

Las opciones de desinfección determinan el comportamiento de ESET Small Business Security durante la desinfección de objetos. Hay 4 niveles de desinfección:

ThreatSense tiene los siguientes niveles de corrección (es decir, desinfección).

## Corrección en ESET Small Business Security

| Nivel de desinfección | Descripción |
|---|---|
| **Reparar la detección siempre** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos raros (por ejemplo, archivos del sistema), si no se puede corregir la detección, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, mantener de otro modo** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la detección no se puede corregir, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, preguntar de otro modo** | Intentar corregir la detección durante la desinfección de objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este ajuste se recomienda en la mayoría de los casos. |
| **Preguntar siempre al usuario final** | El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción correctiva (por ejemplo, eliminar u omitir). Este nivel se ha diseñado para usuarios más avanzados que conocen los pasos necesarios en caso de detección. |

## Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

## Otros

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

**Analizar secuencias de datos alternativas (ADS)**: las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

**Realizar análisis en segundo plano con baja prioridad**: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

**Registrar todos los objetos**: el registro del análisis mostrará todos los archivos analizados en archivos comprimidos de autoextracción, incluso los no infectados (puede generar muchos datos de registro del análisis y aumentar el tamaño del archivo de registro del análisis).

**Activar la optimización inteligente**: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

**Preservar el último acceso con su fecha y hora**: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

## Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

## Configuración de los objetos

**Tamaño máximo del objeto**: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado.

**Tiempo máximo de análisis para el objeto (s)**: define el valor de tiempo máximo para el análisis de los archivos de un objeto contenedor (por ejemplo, un archivo comprimido RAR/ZIP o un mensaje de correo electrónico con varios archivos adjuntos). Este ajuste no se aplica a los archivos independientes. Si se ha introducido un valor definido por el usuario y ha transcurrido el tiempo, el análisis se detendrá lo antes posible, independientemente

de si ha finalizado el análisis de cada archivo del objeto contenedor.
En el caso de un archivo comprimido con archivos grandes, el análisis se detendrá en cuanto se extraiga un archivo del archivo comprimido (por ejemplo, si la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo tarda 5 segundos). El resto de archivos del archivo comprimido no se analizarán una vez transcurrido el tiempo.
Para limitar el tiempo de análisis, incluido el de los archivos comprimidos más grandes, utilice los ajustes **Tamaño máximo del objeto** y **Tamaño máx. de archivo en el archivo comprimido** (no se recomienda debido a posibles riesgos de seguridad).
Valor predeterminado: ilimitado.

### Configuración del análisis de archivos comprimidos

**Nivel de anidamiento de archivos**: especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10.

**Tamaño máx. de archivo en el archivo comprimido**: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. El valor máximo es **3 GB**.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

## Protección del acceso a la Web

La protección de acceso a la web le permite configurar opciones avanzadas del módulo Protección de internet. Las siguientes opciones están disponibles en Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Protección de acceso a la web**:

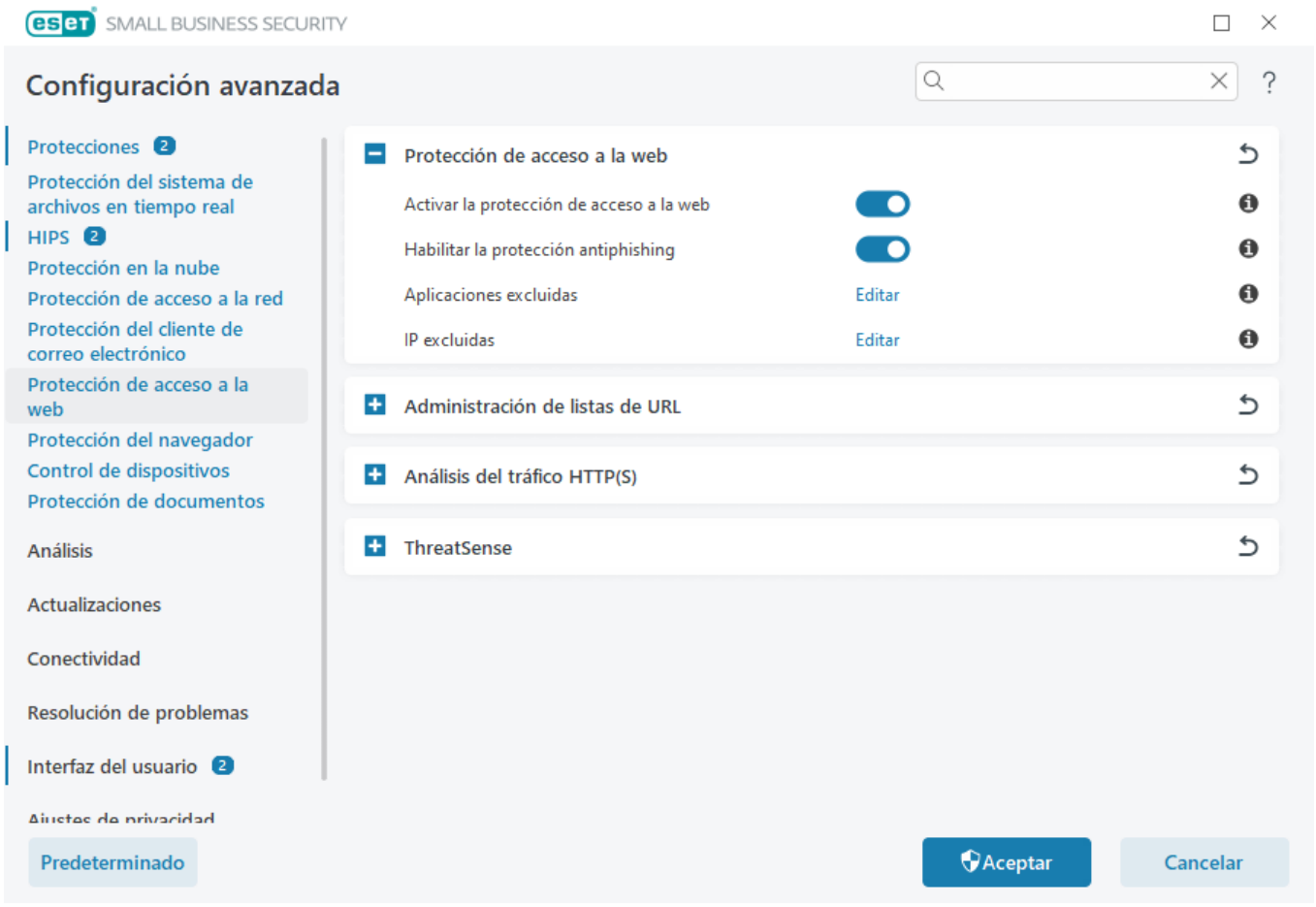
**Activar la protección de acceso a la web**: cuando esta opción está desactivada, no se ejecutan Protección de acceso a la web ni Protección antiphishing.

> Le recomendamos encarecidamente que deje activada la Protección de acceso a la web y no excluya ninguna aplicación o dirección IP de forma predeterminada.

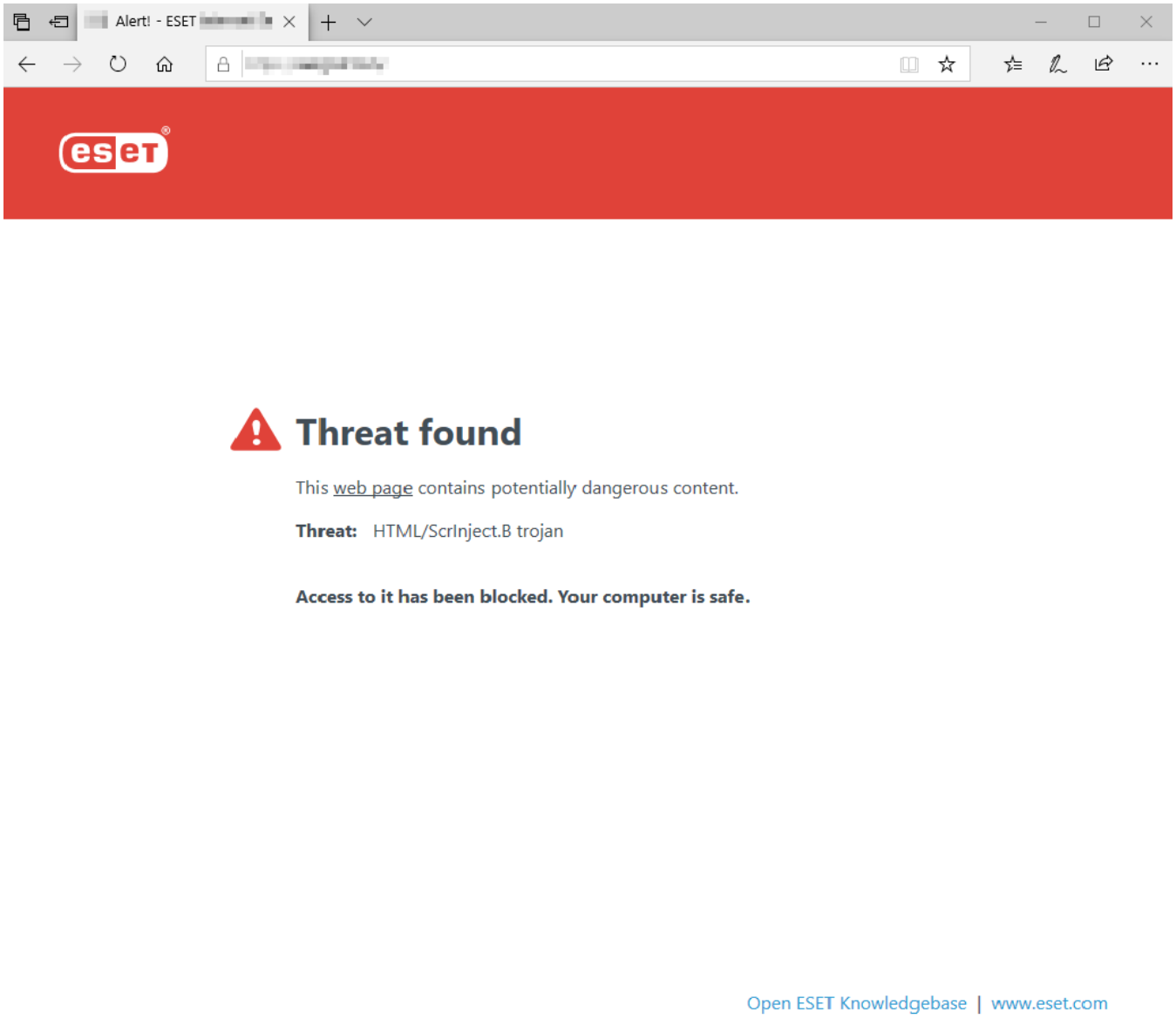
**Activar protección anti-phishing**: cuando esta opción activada, las páginas web de phishing se bloquean. Consulte Protección antiphishing para obtener más información.

Aplicaciones excluidas: permite excluir aplicaciones específicas del análisis de Protección de acceso a la web. Útil cuando Protección de acceso a la web causa problemas de compatibilidad.

IP excluidas: permite excluir direcciones remotas específicas del análisis de la protección de acceso a la Web. Útil cuando Protección de acceso a la web causa problemas de compatibilidad.




Protección de acceso a la web mostrará el siguiente mensaje en su navegador cuando el sitio web esté bloqueado:




Instrucciones con ilustraciones

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- Evitar que la protección de acceso a la web bloquee un sitio web seguro
- Bloquear un sitio web usando ESET Small Business Security

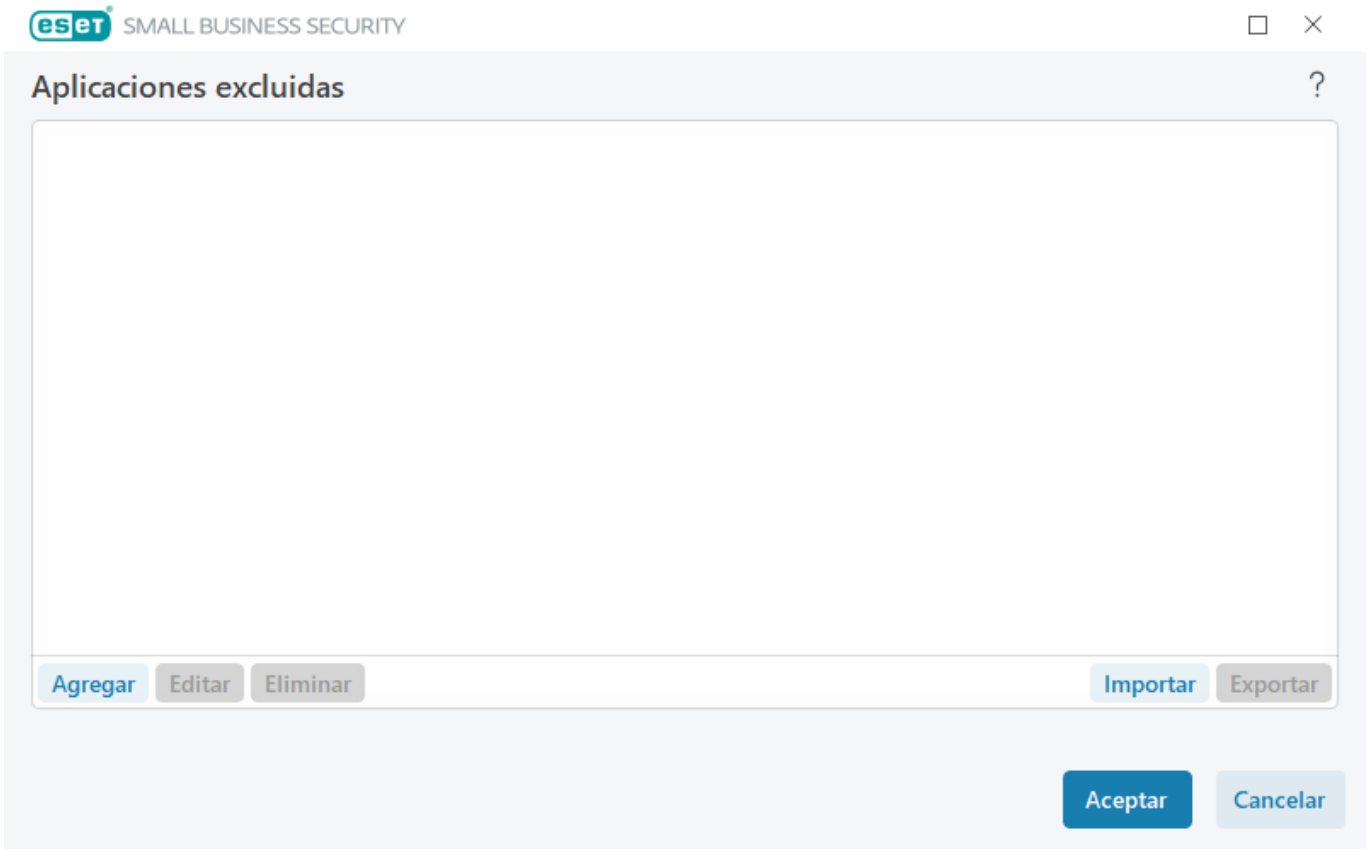
# Aplicaciones excluidas

Para excluir el análisis de la comunicación para aplicaciones específicas, añádalas a la lista. No se comprobará la presencia de amenazas en la comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas. Se recomienda su uso únicamente en aplicaciones que no funcionen correctamente cuando se compruebe su comunicación.

Las aplicaciones y los servicios en ejecución estarán disponibles aquí de forma automática cuando haga clic en **Agregar**. Haga clic en **...** y navegue hasta una aplicación para agregar la exclusión manualmente.

**Modificar**: modifique las entradas seleccionadas de la lista.

**Eliminado**: elimina las entradas seleccionadas de la lista.



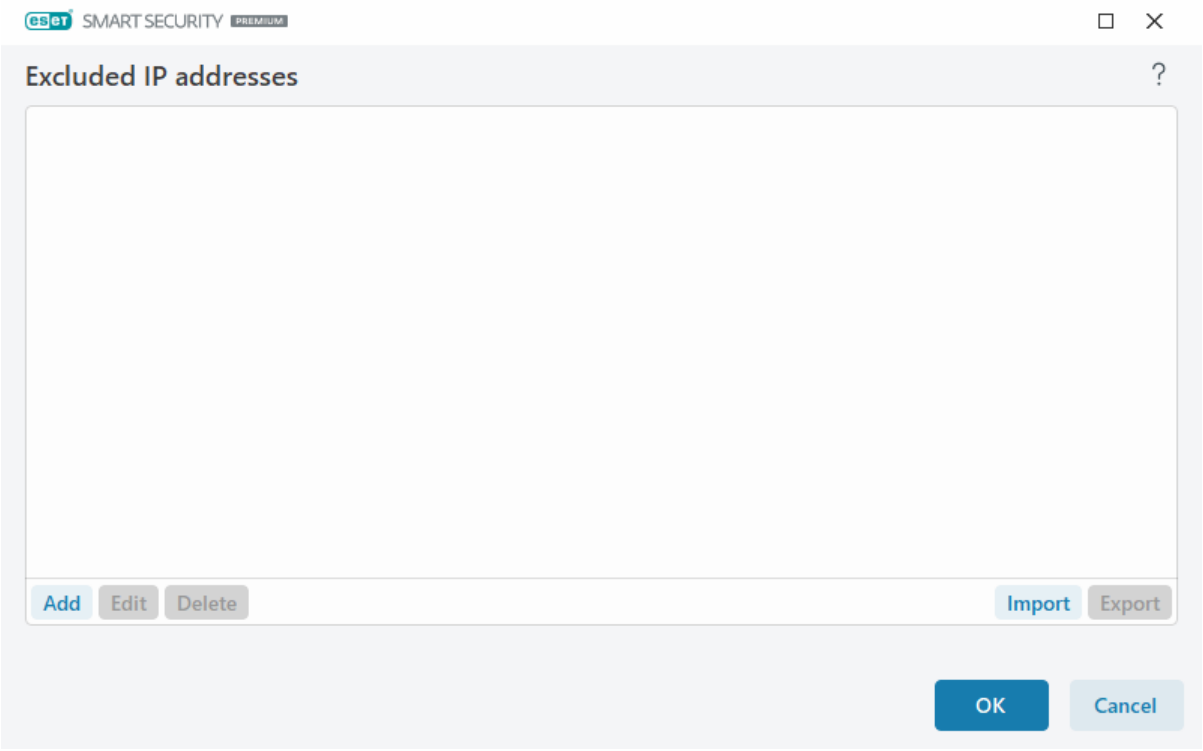

# IP excluidas

Las entradas de la lista se excluirán del análisis. No se comprobará la presencia de amenazas en las comunicaciones HTTP(S)/POP3(S)/IMAP(S) entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Haga clic en **Agregar** para excluir una dirección IP, un rango de direcciones o una subred de un punto remoto.

Haga clic en **Editar** para cambiar la dirección IP seleccionada.

Haga clic en **Eliminar** para quitar las entradas seleccionadas de la lista.




### Ejemplos de direcciones IP

Agregar dirección IPv4:
**Dirección única**: agrega la dirección IP de un ordenador concreto (por ejemplo, *192.168.0.10*).
**Rango de direcciones**: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones de varios ordenadores (por ejemplo, *192.168.0.1-192.168.0.99*).
**Subred**: grupo de ordenadores definido por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red de la subred 192.168.1.0. Para excluir todo el tipo de subred en *192.168.1.0/24*.
Agregar dirección IPv6:
**Dirección única**: agrega la dirección IP de un ordenador concreto (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
**Subred**: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

# Administración de listas de URL

La **administración de listas de URL** en Configuración avanzada > **Protecciones** > **Protección de acceso a la web** le permite especificar direcciones HTTP para bloquearlas, permitirlas o excluirlas del análisis de contenido.

SSL/TLS debe estar activado si desea filtrar direcciones HTTPS además de HTTP. Si no lo hace, solo se agregarán los dominios de los sitios HTTPS que haya visitado, pero no la URL completa.

No podrá acceder a los sitios web de **Lista de direcciones bloqueadas** a menos que también se incluyan en **Lista de direcciones permitidas**. Cuando se acceda a sitios web que se encuentran en **Lista de direcciones excluidas del análisis de contenido**, dichos sitios web no se analizarán en busca de código malicioso.

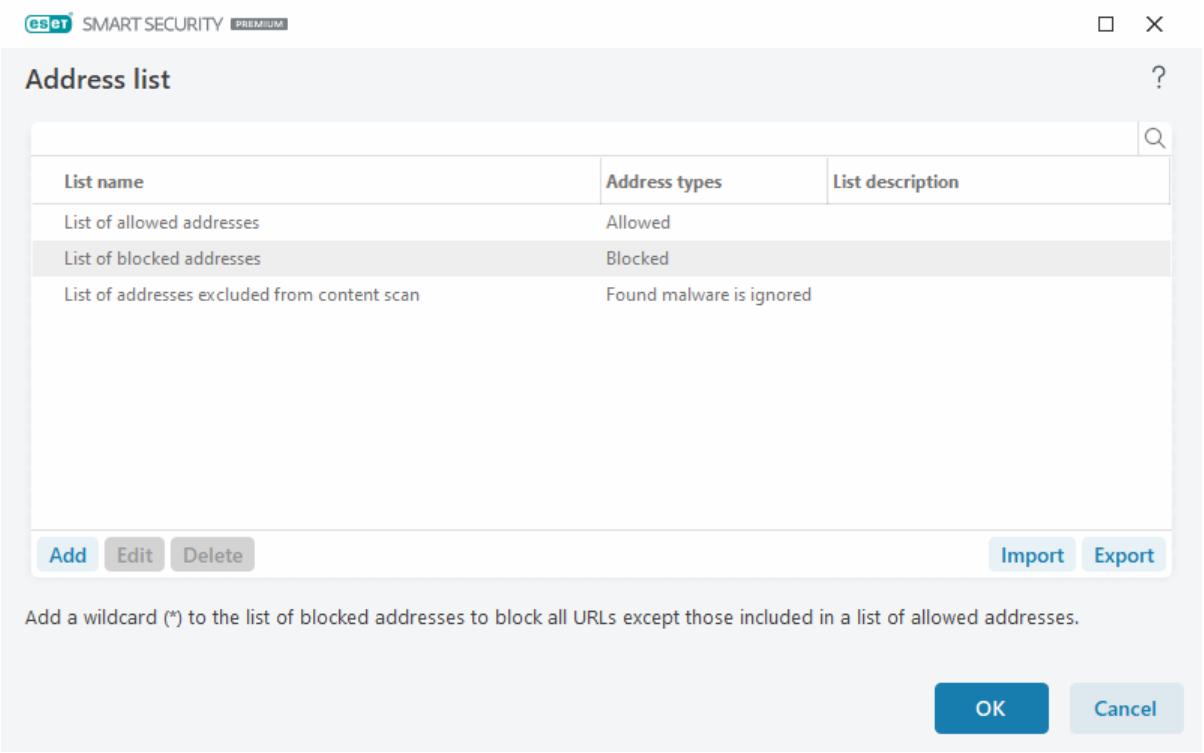
Si desea bloquear todas las direcciones HTTP menos las incluidas en la **Lista de direcciones permitidas** activa, agregue el símbolo * a la **Lista de direcciones bloqueadas** activa.

No se pueden utilizar los símbolos especiales * (asterisco) y ? (signo de interrogación) en listas. El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Preste atención al

especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista. Consulte Agregar dirección HTTP/máscara de dominio para obtener información sobre cómo detectar un dominio completo con todos sus subdominios de forma segura. Para activar una lista, seleccione **Lista activa**. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione **Notificar al aplicar**.

### Direcciones en las que confía ESET

Si la opción **No analizar el tráfico con dominios en los que ESET confía** está activada en SSL/TLS, los dominios de la lista blanca administrada por ESET no se verán afectados por la configuración de administración de la lista de URL.




## Elementos de control

**Agregar**: crea una lista nueva que se suma a las predefinidas. Esta opción puede ser útil si se desea dividir varios grupos de direcciones de forma lógica. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que otra contiene su propia lista negra. Esto facilita la actualización de la lista externa sin que la suya se vea afectada.

**Modificar**: modifica las listas existentes. Utilice esta opción para agregar o quitar direcciones.

**Eliminar**: elimina las listas existentes. Esta opción solo está disponible en listas creadas con **Agregar**, no en las listas predeterminadas.

# Lista de direcciones

En esta sección podrá indicar las listas de direcciones HTTP(S) que desea bloquear, permitir o excluir del análisis.

De forma predeterminada, están disponibles estas tres listas:

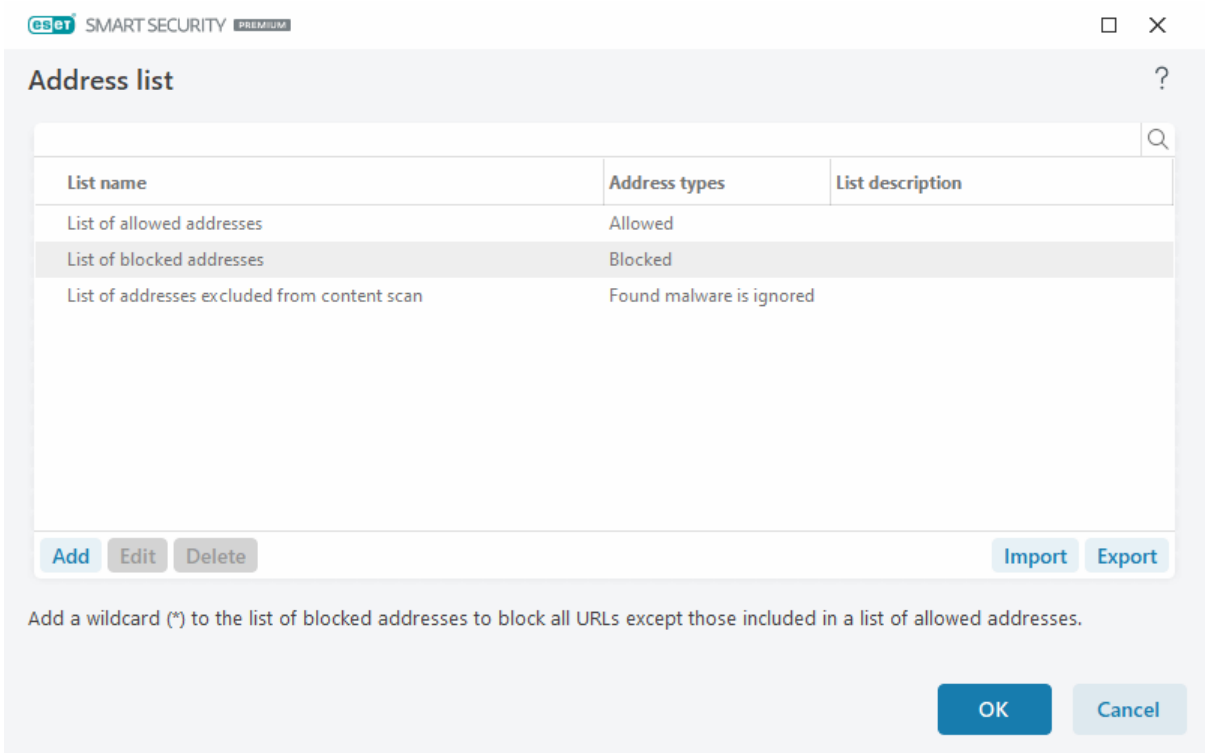
- **Lista de direcciones excluidas del análisis de contenido**: no se comprobará la existencia de código

malicioso en ninguna de las direcciones agregadas a esta lista.

• **Lista de direcciones permitidas**: si está activada la opción Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones especificadas en esta lista. Las direcciones de esta lista estarán autorizadas incluso si se incluyen en la lista de direcciones bloqueadas.

• **Lista de direcciones bloqueadas**: el usuario no tendrá acceso a las direcciones incluidas en esta lista a menos que aparezcan también en la lista de direcciones permitidas.

Haga clic en **Agregar** para crear una lista nueva. Para eliminar las listas seleccionadas, haga clic en **Eliminar**.




**Instrucciones con ilustraciones**

Es posible que los siguientes artículos de la base de conocimiento de ESET solo estén disponibles en inglés:

- Evitar que la protección de acceso a la web bloquee un sitio web seguro
- Bloquear un sitio web con los productos para oficina pequeña de ESET para Windows

Para obtener más información, consulte Administración de listas de URL.

# Creación de nueva lista de direcciones

Este cuadro de diálogo permite configurar una nueva lista de máscaras o direcciones URL que se bloquearán, permitirán o excluirán de la comprobación.

Puede configurar las siguientes opciones:

**Tipo de lista de direcciones**: están disponibles tres tipos de listas:

• **Excluido de la comprobación**: no se comprobará la existencia de código malicioso en ninguna de las direcciones agregadas a esta lista.

- **Bloqueado**: se bloqueará el acceso a las direcciones especificadas en esta lista.

- **Permitido**: se permitirá el acceso a las direcciones especificadas en esta lista. Las direcciones de esta lista se permitirán aunque estén incluidas en la lista de direcciones bloqueadas.

**Nombre de la lista**: especifique el nombre de la lista. Este campo no está disponible cuando se edita una única lista predefinida.

**Descripción de la lista**: escriba una breve descripción de la lista (opcional). Este campo no está disponible cuando se edita una única lista predefinida.

Para activar una lista, seleccione **Lista activa** junto a ella. Si desea recibir una notificación cuando se utilice una lista específica al acceder a sitios web, seleccione **Notificar al aplicar**. Por ejemplo, recibirá una notificación si un sitio web se bloquea o se permite por estar incluido en la lista de direcciones bloqueadas o permitidas. La notificación contendrá el nombre de la lista.

**Registro de severidad:** la información sobre la lista específica que se utiliza al acceder a sitios web se puede escribir en los archivos de registro.

## Elementos de control

**Agregar**: agregue a la lista una dirección URL nueva (introduzca varios valores con un separador).

**Modificar**: modifica la dirección existente en la lista. Esta opción solo estará disponible para las direcciones creadas con **Agregar**.

**Quitar**: elimina las direcciones existentes de la lista. Esta opción solo estará disponible para las direcciones creadas con **Agregar**.

**Importar**: importe un archivo con direcciones URL separadas por un salto de línea (por ejemplo, un archivo *.txt con codificación UTF-8).

# Cómo agregar una máscara URL

Consulte las instrucciones de este cuadro de diálogo antes de especificar la dirección/máscara de dominio que desea.

ESET Small Business Security permite al usuario bloquear el acceso a determinados sitios web para evitar que el navegador de Internet muestre su contenido. Además, permite especificar las direcciones que no se deben comprobar.

Si no se conoce el nombre completo del servidor remoto o si el usuario desea especificar un grupo completo de servidores remotos, se pueden utilizar máscaras para identificar dicho grupo. Las máscaras incluyen los símbolos "?" y "*":

- Utilice ? para sustituir un símbolo.

- Utilice * para sustituir una cadena de texto.

Por ejemplo, *.c?m sirve para todas las direcciones cuya última parte comienza con la letra c, termina con la letra m y contiene un símbolo desconocido entre ellas (.com, .cam, etc.).

Las secuencias que empiezan con "*." reciben un trato especial si se utilizan al principio de un nombre de dominio. En primer lugar, el comodín * no coincide con el carácter de barra ("/") en este caso. Con esto se pretende evitar que se burle la máscara, por ejemplo, la máscara **.dominio.com* no coincidirá con *http://cualquierdominio.com/cualquierruta#.dominio.com* (este sufijo se puede añadir a cualquier URL sin que la descarga se vea afectada). En segundo lugar, la secuencia "*." también se corresponde con una cadena vacía en este caso especial. El objetivo es permitir la detección de un dominio completo, incluidos todos sus subdominios, con una sola máscara.

Por ejemplo, la máscara **.dominio.com* también coincide con *http://dominio.com*. No sería correcto utilizar **dominio.com*, ya que esta cadena también detectaría *http://otrodominio.com*.

# Análisis del tráfico HTTP(S)

De forma predeterminada, ESET Small Business Security está configurado para analizar el tráfico HTTP y HTTPS que utilizan los navegadores de Internet y otras aplicaciones. Debe desactivar el análisis de tráfico solo si tiene problemas con un software de terceros y desea saber si el problema lo causa ESET Small Business Security.

**Activar análisis del tráfico HTTP**: El tráfico HTTP se supervisa siempre en todos los puertos y para todas las aplicaciones.

**Activar análisis del tráfico HTTPS**: el tráfico de HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Small Business Security comprueba la comunicación mediante los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo (puede agregar puertos a los predefinidos 443 y 0-65535).

# ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor de ThreatSense le permiten especificar varios parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real

- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

## Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

**Memoria operativa**: busca amenazas que ataquen a la memoria operativa del sistema.

**Sectores de inicio/UEFI**: analiza los sectores de inicio para detectar malware en el registro de inicio principal. Lea más sobre la UEFI en el glosario.

**Archivos de correo**: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

**Archivos comprimidos**: el programa es compatible con las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

**Archivos comprimidos autoextraíbles**: los archivos comprimidos autoextraíbles (SFX) son archivos comprimidos que pueden extraerse por sí solos.

**Empaquetadores en tiempo de ejecución**: después de su ejecución, los empaquetadores en tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

## Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

**Heurística**: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

**Heurística avanzada/ADN inteligentes**: la heurística avanzada es un algoritmo heurístico único desarrollado por

ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

## Desinfección

Las opciones de desinfección determinan el comportamiento de ESET Small Business Security durante la desinfección de objetos. Hay 4 niveles de desinfección:

ThreatSense tiene los siguientes niveles de corrección (es decir, desinfección).

## Corrección en ESET Small Business Security

| Nivel de desinfección | Descripción |
|---|---|
| **Reparar la detección siempre** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos raros (por ejemplo, archivos del sistema), si no se puede corregir la detección, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, mantener de otro modo** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la detección no se puede corregir, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, preguntar de otro modo** | Intentar corregir la detección durante la desinfección de objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este ajuste se recomienda en la mayoría de los casos. |
| **Preguntar siempre al usuario final** | El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción correctiva (por ejemplo, eliminar u omitir). Este nivel se ha diseñado para usuarios más avanzados que conocen los pasos necesarios en caso de detección. |

## Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

## Otros

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

**Analizar secuencias de datos alternativas (ADS)**: las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

**Realizar análisis en segundo plano con baja prioridad**: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

**Registrar todos los objetos**: el registro del análisis mostrará todos los archivos analizados en archivos comprimidos de autoextracción, incluso los no infectados (puede generar muchos datos de registro del análisis y aumentar el tamaño del archivo de registro del análisis).

**Activar la optimización inteligente**: si la opción Optimización inteligente está activada, se utiliza la configuración

más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

**Preservar el último acceso con su fecha y hora**: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

## Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

## Configuración de los objetos

**Tamaño máximo del objeto**: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado.

**Tiempo máximo de análisis para el objeto (s)**: define el valor de tiempo máximo para el análisis de los archivos de un objeto contenedor (por ejemplo, un archivo comprimido RAR/ZIP o un mensaje de correo electrónico con varios archivos adjuntos). Este ajuste no se aplica a los archivos independientes. Si se ha introducido un valor definido por el usuario y ha transcurrido el tiempo, el análisis se detendrá lo antes posible, independientemente de si ha finalizado el análisis de cada archivo del objeto contenedor.
En el caso de un archivo comprimido con archivos grandes, el análisis se detendrá en cuanto se extraiga un archivo del archivo comprimido (por ejemplo, si la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo tarda 5 segundos). El resto de archivos del archivo comprimido no se analizarán una vez transcurrido el tiempo.
Para limitar el tiempo de análisis, incluido el de los archivos comprimidos más grandes, utilice los ajustes **Tamaño máximo del objeto** y **Tamaño máx. de archivo en el archivo comprimido** (no se recomienda debido a posibles riesgos de seguridad).
Valor predeterminado: ilimitado.

## Configuración del análisis de archivos comprimidos

**Nivel de anidamiento de archivos**: especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10.

**Tamaño máx. de archivo en el archivo comprimido**: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. El valor máximo es **3 GB**.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

# Protección del navegador

La protección del navegador es otra capa de protección para su seguridad y privacidad que protege la memoria del navegador para que otros procesos no la inspeccionen, aumenta la protección contra los registradores de pulsaciones e impide pegar datos relacionados con los pagos en línea modificados por el malware desde el portapapeles en el navegador seguro.

Para configurar la protección del navegador, abra Configuración avanzada > **Protecciones** > **Protección del navegador** y elija entre las siguientes opciones de configuración:

- Banca y navegación seguras
- Lista blanca de Protección del navegador
- Marco del navegador

# Banca y navegación seguras

Puede configurar la Banca y navegación seguras en Configuración avanzada > **Protecciones** > **Protección del navegador** > **Banca y navegación seguras**.

## Básico

**Activar Banca y navegación seguras**: cuando la función Banca y navegación seguras está activada, todos los navegadores web compatibles se iniciarán en modo seguro de forma predeterminada.

## Protección del navegador

Active **Proteger todos los navegadores** para iniciar todos los navegadores web compatibles en un modo seguro.

**Modo de instalación de extensiones**: en el menú desplegable, puede seleccionar qué extensiones podrán instalarse en un navegador protegido por ESET:

- **Extensiones esenciales**: solo las extensiones más importantes que ha desarrollado el editor de un navegador concreto.
- **Todas las extensiones**: todas las extensiones compatibles con un navegador concreto.

> Cambiar el modo de instalación de extensiones no afecta a las extensiones del navegador instaladas anteriormente.

### Navegador protegido

**Protección de memoria mejorada**: si se activa esta opción, se impedirá que otros procesos inspeccionen la memoria del navegador protegido.

**Protección del teclado**: si se activa esta opción, la información que se introduzca en el navegador protegido mediante el teclado se ocultará a otras aplicaciones. Esto aumenta la protección contra registradores de pulsaciones.

**Protección del portapapeles**: si está activada, ESET Small Business Security evitará pegar cualquier dato relacionado con los pagos en línea modificado por malware desde el portapapeles en el navegador protegido. Esto garantiza la protección contra posibles cambios realizados por software malicioso.

**Marco del navegador** – Personalice la configuración de pantalla del marco del navegador en navegadores protegidos.

**Lista blanca de Protección del navegador**: Administre los archivos y los ID de extensión agregados a la lista de permitidos de protección del navegador.

### Privacidad y seguridad del navegador

**Activar Privacidad y seguridad del navegador**: si se desactiva esta función, la extensión Privacidad y seguridad del navegador se desinstalará de todos los navegadores compatibles en todas las cuentas de Windows.

**Mostrar notificaciones de Privacidad y seguridad del navegador**: si se activa, ESET Small Business Security mostrará las notificaciones de Privacidad y seguridad del navegador.

### Análisis de scripts del navegador

**Activar análisis avanzado de los scripts del navegador**: si se activa, el análisis antivirus comprobará todos los programas JavaScript ejecutados por los navegadores de Internet.

## Lista blanca de Protección del navegador

Aparecerá la ventana de la **Lista blanca de Protección del navegador** y permitirá administrar los archivos agregados. La lista blanca se utiliza para crear exenciones para archivos que no son de confianza y, por lo tanto, no se cargan en los navegadores, pero son necesarios para ciertas funcionalidades. Se pueden realizar las siguientes acciones desde **Configuración** > **Configuración avanzada** > **Protecciones** > **Protección del navegador** > **Lista blanca de Protección del navegador** > **Editar**:

**Agregar**: agrega a la lista la ruta de acceso del archivo .

> Los archivos bloqueados que no son de confianza también quedan registrados en el registro de los **Archivos de registro** > **Protección del navegador**, y puede agregarlos a la lista blanca directamente al hacer clic con el botón derecho en el archivo.

**Modificar**: le permite modificar las entradas seleccionadas.

**Eliminar**: quita el elemento de la lista.

**Importar**: importa la lista en formato XML.

**Exportar**: exporta la lista en formato XML.

## Marco del navegador

El navegador protegido le informa de su estado actual con las notificaciones del navegador y el color de la ventana del navegador.

Las notificaciones del navegador se muestran en la ficha del lado derecho.

Para expandir la notificación en el navegador, haga clic en el icono de ESET. Para minimizar la notificación, haga clic en el texto de la notificación. Para descartar la notificación y el marco verde del navegador, haga clic en el icono de cerrar.

Solo pueden descartarse la notificación informativa y el marco verde del navegador.

## Notificaciones del navegador

| Tipo de la notificación | Estado |
|---|---|
| Notificación informativa y marco verde en el navegador | Se garantiza la máxima protección y se minimiza la notificación del navegador de forma predeterminada. Expanda la notificación en el navegador y haga clic en **Configuración** para abrir la configuración de Herramientas de seguridad. |
| Advertencia y marco amarillo para aplicaciones de acceso remoto, Wi-Fi no protegida y extensiones que no sean de confianza | El navegador protegido requiere su atención para los problemas que no sean críticos. Para obtener más información sobre un problema o una solución, siga las instrucciones de la notificación del navegador. |

Para permanecer protegido, no se conecte a redes Wi-Fi no seguras con una contraseña débil o sin contraseña.

Si se detecta una extensión de navegador que no es de confianza en su navegador, es posible que no sea suficientemente seguro para acceder a la banca por Internet o realizar pagos en línea. Si confía en esta extensión, puede agregarla a su lista de permitidos.

# Control del dispositivo

ESET Small Business Security proporciona control automático del dispositivo (CD/DVD/USB/etc.). Este módulo le permite bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

## Dispositivos externos admitidos:

- Almacenamiento en disco (unidad de disco duro, disco USB extraíble)
- CD/DVD
- USB Impresora
- FireWire Almacenamiento
- Bluetooth Dispositivo
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- LPT/COM puerto

- Dispositivo portátil (dispositivos con batería, como reproductores multimedia, smartphones, dispositivos plug-and-play, etc.)
- Todos los tipos de dispositivos

Las opciones de configuración del control del dispositivo se pueden modificar en Configuración avanzada > **Protecciones** > **Control del dispositivo**.

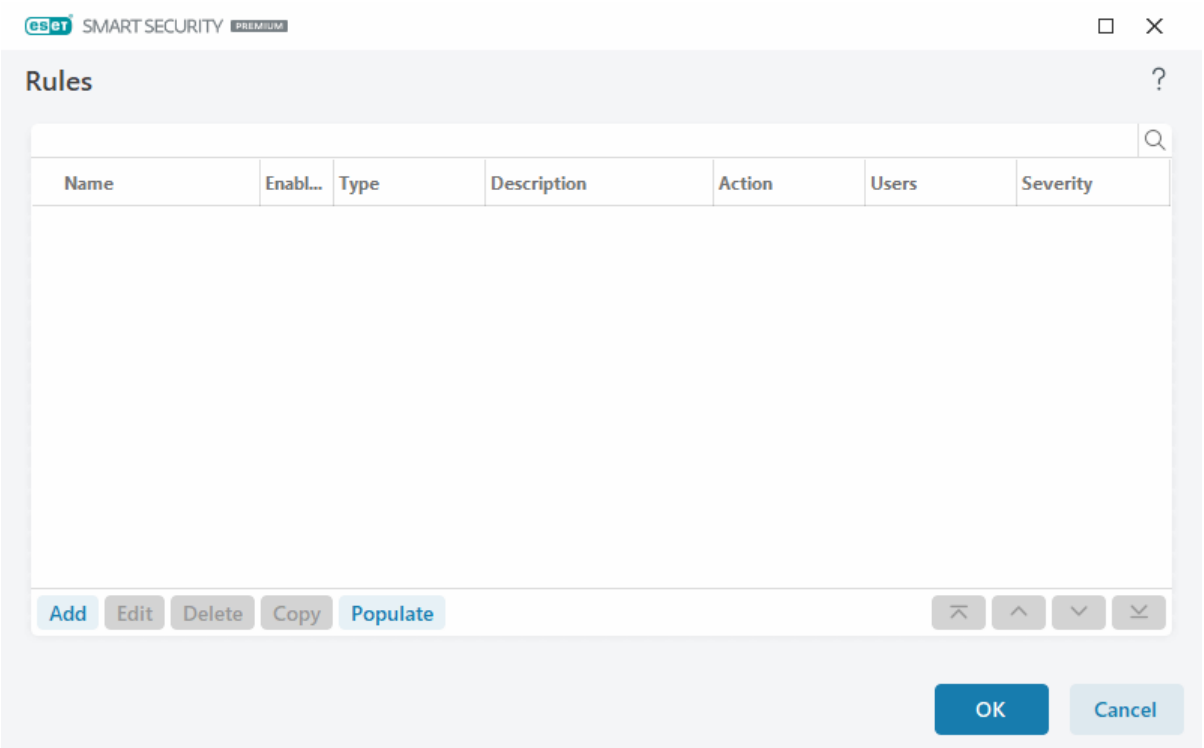
Haga clic en el botón **Activar el control de dispositivos** para activar la función Control de dispositivos en ESET Small Business Security; debe reiniciar el ordenador para que este cambio se aplique. Una vez activado Control de dispositivos, puede definir las **Reglas** en la ventana Editor de reglas.

> Puede crear varios grupos de dispositivos a los que se aplicarán reglas distintas. También puede crear solo un grupo de dispositivos al que se aplicará la regla con la acción **Permitir** o **Bloquear escritura**. Esto garantiza el bloqueo de dispositivos no reconocidos por el control de dispositivos pero conectados al ordenador.

Si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación y se prohíbe el acceso a dicho dispositivo.

# Editor de reglas de control de dispositivos

La ventana **Editor de reglas de control de dispositivos** muestra las reglas existentes y permite controlar con precisión los dispositivos externos que los usuarios conectan al equipo.

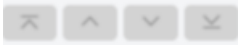



Determinados dispositivos se pueden permitir o bloquear por usuario o por grupo de usuarios y según parámetros adicionales del dispositivo que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro. Consulte también Adición de reglas de control de dispositivos

Haga clic en **Agregar** o en **Modificar** para administrar una regla. **Haga clic en Copiar** para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML que se muestran al hacer clic en una regla se pueden copiar en el portapapeles para ayudar a administradores de sistemas a exportar o importar datos y utilizarlos.

Al mantener pulsado **CTRL** y hacer clic, puede seleccionar varias reglas y aplicar acciones, como eliminarlas o moverlas hacia arriba o hacia abajo en la lista, a todas las reglas seleccionadas. La casilla de verificación **Activado** desactiva o activa una regla; esto puede ser útil si desea conservar la regla.

Haga clic en **Llenar** para rellenar automáticamente los parámetros del medio extraíble conectado a su ordenador.

Las reglas se muestran en orden de prioridad; las que tienen más prioridad se muestran más arriba en la lista. Las reglas pueden moverse haciendo clic en  **Superior/Arriba/Abajo/Inferior** tanto por separado como en grupo.

Las entradas del registro se pueden ver en la ventana principal del programa > **Herramientas** > Archivos de registro.

El Registro de control de dispositivos anota todas las ocasiones en las que se activa el Control de dispositivos.

# Dispositivos detectados

El botón **Llenar** contiene una visión general de todos los dispositivos conectados actualmente con información sobre los aspectos siguientes: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible). Si desea ver todos los dispositivos ocultos, seleccione **Mostrar dispositivos ocultos**.

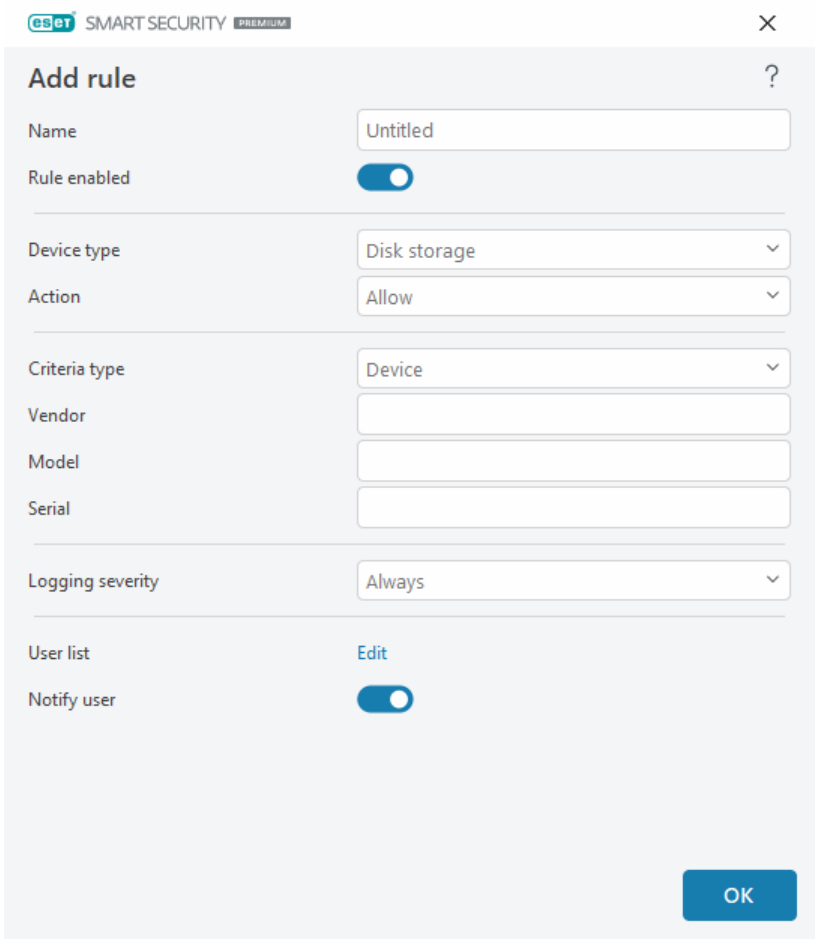
Seleccione un dispositivo en la lista de dispositivos detectados y haga clic en **Aceptar** para agregar una regla de control de dispositivos con información predefinida (se puede ajustar toda la configuración).

Los dispositivos que estén en el modo de bajo consumo (suspensión) están marcados con un icono de advertencia . Para activar el botón **Aceptar** y agregar una regla para este dispositivo:

- Vuelva a conectar el dispositivo.
- Utilice el dispositivo (por ejemplo, inicie la aplicación Cámara en Windows para activar una cámara web).

# Adición de reglas de control de dispositivos

Una regla de control de dispositivos define la acción que se realizará al conectar al ordenador un dispositivo que cumple los criterios de la regla.




Introduzca una descripción de la regla en el campo **Nombre** para mejorar la identificación. Haga clic en el interruptor situado junto a **Regla activada** para activar o desactivar esta regla. Esto puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

## Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (Almacenamiento en disco, Dispositivo portátil, Bluetooth, FireWire…). La información sobre el tipo de dispositivo se recopila del sistema operativo y se puede ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Los lectores de tarjetas inteligentes abarcan todos los lectores que tienen incrustado un circuito integrado, como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras. Como estos dispositivos solo proporcionan información sobre sus acciones y no sobre los usuarios, solo pueden bloquearse a nivel global.

## Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Permitir**: se permitirá el acceso completo al dispositivo.
- **Bloquear**: se bloqueará el acceso al dispositivo.
- **Bloquear escritura**: solo se permitirá el acceso de lectura al dispositivo.
- **Advertir**: cada vez que se conecte un dispositivo se informará al usuario de si está permitido o bloqueado, y se efectuará una entrada de registro. Los dispositivos no se recuerdan, y se seguirá mostrando una notificación en las siguientes conexiones del mismo dispositivo.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. Si se trata de un dispositivo de tipo almacenamiento, las cuatro acciones estarán disponibles. En el caso de los dispositivos que no son de almacenamiento solo hay tres disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

## Tipo de criterios

Seleccione **Grupo de dispositivos** o **Dispositivo**.

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas según el dispositivo. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

Si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado en todos los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines. El signo de interrogación (?) representa un carácter único, y el asterisco (*) una cadena variable de cero o más caracteres.

Si desea ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo en el Registro de control de dispositivos.

## Nivel de registro

ESET Small Business Security guarda todos los sucesos importantes en un archivo de registro que se puede ver directamente en el menú principal. Haga clic en **Herramientas** > **Archivos de registro** y, a continuación, seleccione **Control de dispositivos** en el menú desplegable **Registrar**.

- **Siempre**: registra todos los sucesos.
- **Diagnóstico**: registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta.
- **Ninguno**: no se registra nada.

## Lista de usuarios

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios si se agregan a la lista de usuarios al hacer clic en **Editar** junto a **Lista de usuarios**.

- **Agregar**: abre el cuadro de diálogo **Tipos de objeto: Usuarios o grupos**, que le permite seleccionar los

usuarios que desee.

- **Quitar**: elimina del filtro al usuario seleccionado.

> **Limitaciones de la lista de usuarios**
> La lista de usuarios no se puede definir para reglas con tipos de dispositivo específicos:
> - Impresora USB
> - Dispositivo Bluetooth
> - Lector de tarjetas inteligentes
> - Dispositivo de imagen
> - Módem
> - Puerto LPT/COM

**Notificar al usuario**: si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación.

# Grupos de dispositivos

> La conexión de un dispositivo al ordenador puede presentar un riesgo para la seguridad.

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo correspondiente, mientras que la parte izquierda contiene los grupos creados. Seleccione un grupo para mostrar los dispositivos en el panel de la derecha.

Cuando abre la ventana Grupos de dispositivos y selecciona uno de los grupos, puede agregar o quitar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo. También puede hacer clic en el botón **Llenar** y se mostrarán en la ventana **Dispositivos detectados** todos aquellos dispositivos que estén conectados a su ordenador. Seleccione dispositivos de la lista para agregarlos al grupo haciendo clic en **Aceptar**.

## Elementos de control

**Agregar**: puede agregar un grupo escribiendo su nombre o un dispositivo a un grupo existente en función del punto de la ventana en el que hiciera clic en el botón.

**Modificar**: le permite modificar el nombre del grupo seleccionado o los parámetros (proveedor, modelo, número de serie) del dispositivo.

**Eliminar**: elimina el grupo o el dispositivo seleccionados, según la parte de la ventana en la que hiciera clic.

**Importar**: importa una lista de dispositivos desde un archivo de texto. La importación de dispositivos desde un archivo de texto requiere el formato correcto:

- Cada dispositivo se inicia en una línea nueva.

- El **Proveedor**, el **Modelo** y el **Número de serie** deben estar presentes en cada dispositivo y separados con una coma.

> A continuación se muestra un ejemplo del contenido del archivo de texto:
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

**Exportar**: exporta una lista de dispositivos a un archivo.

El botón **Llenar** contiene una visión general de todos los dispositivos conectados actualmente con información sobre los aspectos siguientes: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible).

## Agregar dispositivo

Haga clic en **Agregar** la ventana de la derecha para agregar un dispositivo a un grupo existente. Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas según el dispositivo. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor**: filtrar por nombre o ID de proveedor.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.
- **Descripción**: descripción del dispositivo para una mejor organización.

> Si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado en todos los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines. El signo de interrogación (?) representa un carácter único, y el asterisco (*) una cadena variable de cero o más caracteres.

Haga clic en **Aceptar** para guardar los cambios. Haga clic en **Cancelar** para cerrar la ventana **Grupos de dispositivos** sin guardar los cambios.

> Tras crear un grupo de dispositivos, tendrá que agregar una nueva regla de control de dispositivos y elegir la acción que desea realizar.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. Las cuatro acciones estarán disponibles si se trata de un dispositivo de tipo almacenamiento. En el caso de los dispositivos que no son de almacenamiento, solo hay tres disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

# Protección de cámara web

**Protección de cámara web** le informa sobre los procesos y las aplicaciones que acceden a la cámara web del ordenador. Si una aplicación intenta acceder a la cámara, recibirá una notificación para **permitir** o **bloquear** ese acceso. El color de la ventana de alerta depende de la reputación de la aplicación.

Las opciones de configuración de Protección de la cámara web se pueden modificar en Configuración avanzada > **Protecciones** > **Control de dispositivos** > **Protección de la cámara web**.

Para activar la función de protección de la cámara web en ESET Small Business Security, active el interruptor situado junto a **Activar protección de la cámara web**.

Cuando se active la protección de la cámara web, se activarán las **Reglas**, lo que le permitirá abrir la ventana

Editor de reglas.

Para desactivar las alertas de aplicaciones que tengan una regla y se hayan modificado, pero aún tengan una firma digital válida (por ejemplo, una actualización de la aplicación), active el interruptor situado junto a **Desactivar las alertas de acceso a la cámara web para aplicaciones modificadas**.

# Editor de reglas de protección de cámara web

En esta ventana se muestran las reglas existentes y se pueden controlar las aplicaciones y los procesos que acceden a la cámara web del ordenador en función de la acción que haya tomado.

Están disponibles las siguientes acciones:

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

- **Preguntar**: pregunta al usuario cada vez que una aplicación intenta acceder a la cámara web.

Desmarque la casilla de verificación de la columna **Notificar** para dejar de recibir notificaciones cuando una aplicación acceda a la cámara web.

> **Instrucciones con ilustraciones**
> Cómo crear y modificar reglas de cámara web en ESET Small Business Security.

# ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor de ThreatSense le permiten especificar varios parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar

- La combinación de diferentes métodos de detección.

- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real

- Análisis de estado inactivo

- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

## Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

**Memoria operativa**: busca amenazas que ataquen a la memoria operativa del sistema.

**Sectores de inicio/UEFI**: analiza los sectores de inicio para detectar malware en el registro de inicio principal. Lea más sobre la UEFI en el glosario.

**Archivos de correo**: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

**Archivos comprimidos**: el programa es compatible con las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

**Archivos comprimidos autoextraíbles**: los archivos comprimidos autoextraíbles (SFX) son archivos comprimidos que pueden extraerse por sí solos.

**Empaquetadores en tiempo de ejecución**: después de su ejecución, los empaquetadores en tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

## Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

**Heurística**: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que el motor de detección anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

**Heurística avanzada/ADN inteligentes**: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los

productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

## Desinfección

Las opciones de desinfección determinan el comportamiento de ESET Small Business Security durante la desinfección de objetos. Hay 4 niveles de desinfección:

ThreatSense tiene los siguientes niveles de corrección (es decir, desinfección).

## Corrección en ESET Small Business Security

| Nivel de desinfección | Descripción |
|---|---|
| **Reparar la detección siempre** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos raros (por ejemplo, archivos del sistema), si no se puede corregir la detección, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, mantener de otro modo** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la detección no se puede corregir, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, preguntar de otro modo** | Intentar corregir la detección durante la desinfección de objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este ajuste se recomienda en la mayoría de los casos. |
| **Preguntar siempre al usuario final** | El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción correctiva (por ejemplo, eliminar u omitir). Este nivel se ha diseñado para usuarios más avanzados que conocen los pasos necesarios en caso de detección. |

## Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

## Otros

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

**Analizar secuencias de datos alternativas (ADS)**: las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

**Realizar análisis en segundo plano con baja prioridad**: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

**Registrar todos los objetos**: el registro del análisis mostrará todos los archivos analizados en archivos comprimidos de autoextracción, incluso los no infectados (puede generar muchos datos de registro del análisis y aumentar el tamaño del archivo de registro del análisis).

**Activar la optimización inteligente**: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis

distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

**Preservar el último acceso con su fecha y hora**: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

## Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

### Configuración de los objetos

**Tamaño máximo del objeto**: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: ilimitado.

**Tiempo máximo de análisis para el objeto (s)**: define el valor de tiempo máximo para el análisis de los archivos de un objeto contenedor (por ejemplo, un archivo comprimido RAR/ZIP o un mensaje de correo electrónico con varios archivos adjuntos). Este ajuste no se aplica a los archivos independientes. Si se ha introducido un valor definido por el usuario y ha transcurrido el tiempo, el análisis se detendrá lo antes posible, independientemente de si ha finalizado el análisis de cada archivo del objeto contenedor.
En el caso de un archivo comprimido con archivos grandes, el análisis se detendrá en cuanto se extraiga un archivo del archivo comprimido (por ejemplo, si la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo tarda 5 segundos). El resto de archivos del archivo comprimido no se analizarán una vez transcurrido el tiempo.
Para limitar el tiempo de análisis, incluido el de los archivos comprimidos más grandes, utilice los ajustes **Tamaño máximo del objeto** y **Tamaño máx. de archivo en el archivo comprimido** (no se recomienda debido a posibles riesgos de seguridad).
Valor predeterminado: ilimitado.

### Configuración del análisis de archivos comprimidos

**Nivel de anidamiento de archivos**: especifica el nivel máximo de análisis de archivos. Valor predeterminado: 10.

**Tamaño máx. de archivo en el archivo comprimido**: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. El valor máximo es **3 GB**.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

# Niveles de desinfección

Para cambiar la configuración del nivel de desinfección de un módulo de protección, expanda **ThreatSense** (por ejemplo, **Protección del sistema de archivos en tiempo real**) y, a continuación, elija un **Nivel de desinfección** en

el menú desplegable.

ThreatSense tiene los siguientes niveles de corrección (es decir, desinfección).

### Corrección en ESET Small Business Security

| Nivel de desinfección | Descripción |
|---|---|
| **Reparar la detección siempre** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos raros (por ejemplo, archivos del sistema), si no se puede corregir la detección, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, mantener de otro modo** | Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la detección no se puede corregir, el objeto del que se informa se deja en su ubicación original. |
| **Reparar la detección si es seguro, preguntar de otro modo** | Intentar corregir la detección durante la desinfección de objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este ajuste se recomienda en la mayoría de los casos. |
| **Preguntar siempre al usuario final** | El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción correctiva (por ejemplo, eliminar u omitir). Este nivel se ha diseñado para usuarios más avanzados que conocen los pasos necesarios en caso de detección. |

# Extensiones de archivo excluidas del análisis

Las extensiones de archivo excluidas forman parte de ThreatSense. Para configurar las extensiones de archivo excluidas, haga clic en **ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense.

Una extensión es una parte del nombre de archivo delimitada por un punto. Una extensión define el tipo y el contenido de un archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

> No se confunda con Exclusiones de procesos, Exclusiones del HIPS ni Exclusiones de archivo/carpeta.

De forma predeterminada, se analizan todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis.

A veces es necesario excluir archivos del análisis si, por ejemplo, el análisis de determinados tipos de archivo impide la correcta ejecución del programa que utiliza determinadas extensiones. Por ejemplo, quizás sea aconsejable excluir las extensiones `.edb`, `.eml` y `.tmp` cuando se utilizan servidores Microsoft Exchange.

> Para agregar una nueva extensión a la lista, haga clic en **Agregar**. Escriba la extensión en el campo en blanco (por ejemplo, tmp) y haga clic en **Aceptar**. Cuando selecciona **Introduzca múltiples valores**, puede agregar varias extensiones de archivo delimitadas por líneas, comas o punto y coma (por ejemplo, elija **Punto y coma** en el menú desplegable como separador y escriba `edb;eml;tmp`).
> Puede utilizar un símbolo especial ? (signo de interrogación). El signo de interrogación representa cualquier símbolo (por ejemplo, `?db`).

> Para ver la extensión exacta (si la hubiera) de un archivo en un sistema operativo Windows, debe marcar la casilla de verificación **Extensiones de nombre de archivo** en **Explorador de Windows** > **Ver** (pestaña).

# Parámetros adicionales de ThreatSense

Para modificar esta configuración, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Parámetros adicionales de ThreatSense**.

## Parámetros adicionales de ThreatSense para archivos nuevos y modificados

La probabilidad de infección en los archivos recién creados o modificados es superior a la de los archivos existentes. Por eso el programa comprueba estos archivos con parámetros de análisis adicionales. ESET Small Business Security utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización del motor de detección en combinación con métodos de análisis basados en firmas.

Además de en los archivos nuevos, el análisis se realiza también en los **archivos comprimidos de autoextracción** (.sfx) y **empaquetadores en tiempo real** (archivos ejecutables comprimidos internamente). De forma predeterminada, los archivos comprimidos se analizan hasta el 10.º nivel de anidamiento y se comprueban independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, anule la selección de la opción **Configuración predeterminada para el análisis de archivos comprimidos**.

## Parámetros adicionales de ThreatSense para los archivos ejecutados

**Heurística avanzada para los archivos ejecutados**: de forma predeterminada, se utiliza la Heurística avanzada al ejecutar archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET LiveGrid® con el fin de mitigar su repercusión en el rendimiento del sistema.

**Heurística avanzada al ejecutar archivos desde las unidades extraíbles**: la heurística avanzada emula el código en un entorno virtual y evalúa su comportamiento antes de permitir la ejecución del código desde soportes extraíbles.

# Conectividad

En redes específicas, un servidor proxy puede mediar en la comunicación entre el ordenador e Internet. Si utiliza un servidor proxy, debe definir la siguiente configuración. De lo contrario, ESET Small Business Security y sus módulos no se pueden actualizar automáticamente. En ESET Small Business Security, la configuración del servidor proxy está disponible en dos secciones diferentes de Configuración avanzada.

En primer lugar, se puede configurar en Configuración avanzada > **Conectividad** > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para ESET Small Business Security. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar la configuración global del servidor proxy, active **Usar servidor proxy** y escriba la dirección del **Servidor proxy** junto con el número de **Puerto** del servidor proxy.

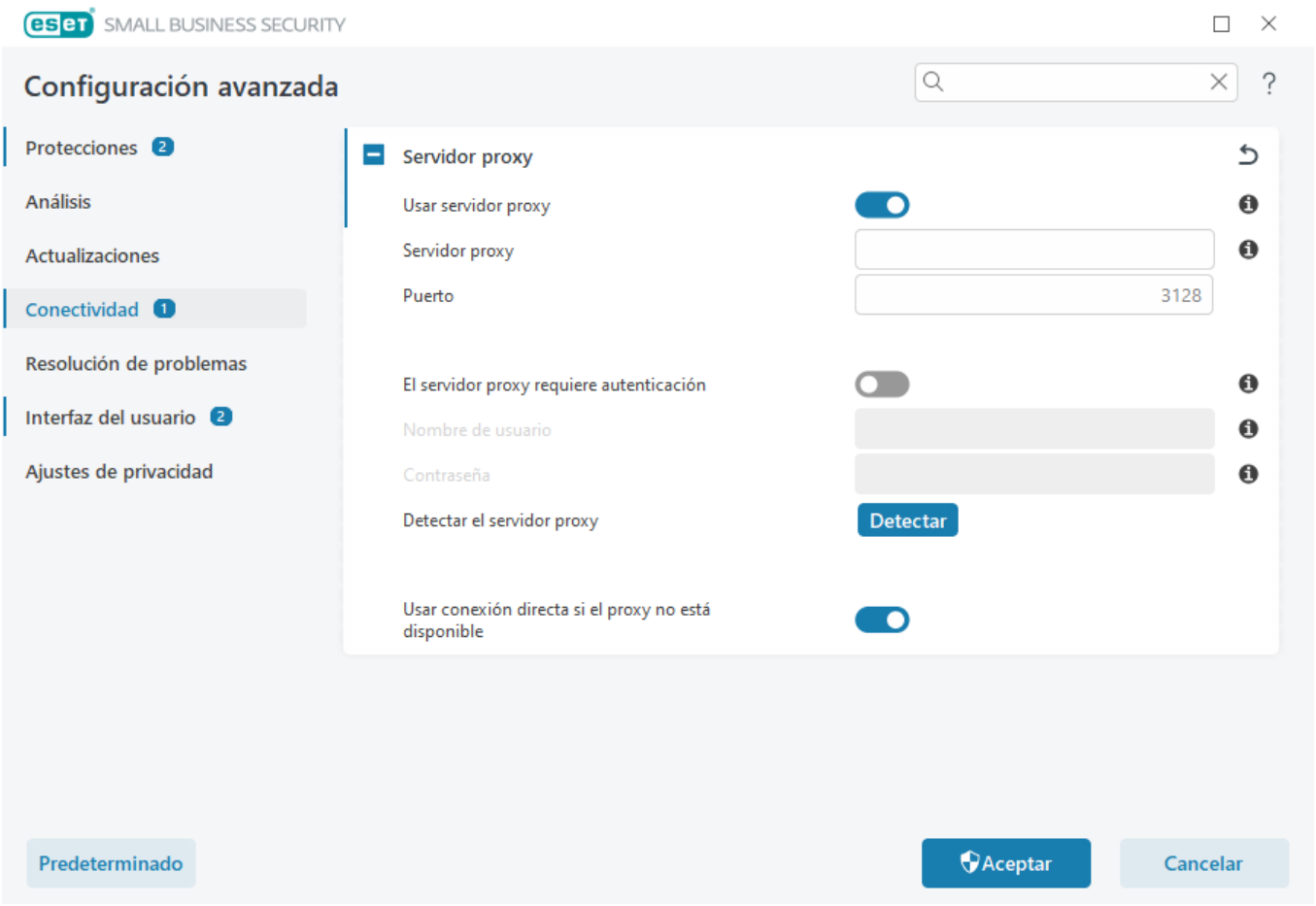
Si la comunicación con el servidor proxy requiere autenticación, seleccione **El servidor proxy requiere autenticación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes. Haga clic en **Detectar servidor proxy** para detectar y rellenar la configuración del servidor proxy automáticamente. ESET Small Business Security copiará los parámetros especificados en Opciones de Internet para Internet Explorer o Google Chrome.

> Debe especificar el nombre de usuario y la contraseña manualmente en la configuración del **Servidor proxy**.

**Usar conexión directa si el proxy no está disponible**: si ESET Small Business Security está configurado para conectarse mediante proxy y es imposible conectar con el proxy, ESET Small Business Security omitirá el proxy y

se conectará directamente con los servidores de ESET.

La configuración del servidor proxy también se puede definir en Configuración avanzada > **Actualizaciones** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** seleccionando **Conexión a través de un servidor proxy** en el menú desplegable **Modo proxy**. Esta configuración se aplica solo para las actualizaciones y se recomienda para los ordenadores portátiles que reciben actualizaciones de módulos desde ubicaciones remotas. Para obtener más información, consulte Configuración avanzada de actualizaciones.




# Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, ekrn). Cuando una aplicación se bloquea, se genera un volcado de memoria. Puede ayudar a los desarrolladores a depurar y arreglar ESET Small Business Security problemas diversos.

Haga clic en el menú desplegable situado junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Desactivar** para desactivar esta característica.

- **Mini** (predeterminado): registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado. Pero dada la poca información que contiene, es posible que el análisis de este archivo no detecte los errores que no estén relacionados directamente con el subproceso que se estaba ejecutando cuando se produjo el problema.

- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma

inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.

**Directorio de destino**: directorio en el que se genera el volcado durante el bloqueo.

**Abrir la carpeta de diagnóstico**: haga clic en **Abrir** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

**Crear volcado de diagnóstico**: haga clic en **Crear** para crear archivos de volcado de diagnóstico en el **Directorio de destino**.

## Registro avanzado

**Activar el registro avanzado en los mensajes de marketing**: registra todos los sucesos relacionados con los mensajes de marketing en el producto.

**Activar registro avanzado del motor antispam**: registrar todos los sucesos que tienen lugar durante el análisis antispam. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el motor antispam de ESET.

**Activar registro avanzado del motor antirrobo**: registrar todos los sucesos que se produzcan en Antirrobo para permitir diagnosticar y resolver problemas.

**Activar registro avanzado de Protección del navegador**: registre todos los eventos que se producen en Banca y navegación seguras.

**Activar registro avanzado del análisis del ordenador**: registrar todos los sucesos que tienen lugar durante el análisis de archivos y carpetas del análisis del ordenador.

**Activar registro avanzado de Control de dispositivos**: registrar todos los sucesos que tienen lugar en Control de dispositivos. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con Control de dispositivos.

**Activar el registro avanzado de Direct Cloud**: registrar todos los sucesos que tienen lugar en ESET LiveGrid®. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con ESET LiveGrid®.

**Activar registro avanzado de la Protección de documentos**: registre todos los sucesos que se produzcan en la Protección de documentos para permitir el diagnóstico y la resolución de problemas.

**Activar registro avanzado de la protección del cliente de correo electrónico**: registra todos los sucesos que tienen lugar en la Protección del cliente de correo electrónico y el complemento del cliente de correo electrónico para permitir diagnosticar y resolver problemas.

**Activar el registro avanzado de ESET LiveGuard**: registrar todos los sucesos que tienen lugar en ESET LiveGuard para permitir diagnosticar y resolver problemas.

**Activar registro avanzado del núcleo**: registra todos los sucesos que se produzcan en el núcleo de ESET (ekrn).

**Activar registro avanzado de licencias**: registrar toda la comunicación del producto con los servidores de activación de ESET o ESET License Manager.

**Activar seguimiento de memoria**: registra todos los eventos que ayudarán a los desarrolladores a diagnosticar

fugas de memoria.

**Activar registro avanzado de la protección de la red**: registrar los datos de red que pasan a través del cortafuegos en formato PCAP. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el cortafuegos.

**Activar registro avanzado de análisis de tráfico de red**: registre todos los datos que pasan por el análisis de tráfico de red en formato PCAP para ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el análisis de tráfico de red.

**Activar registro avanzado del sistema operativo**: registra información sobre el sistema operativo, tal como los procesos en ejecución, la actividad de la CPU, las operaciones del disco, etc. Estos datos pueden ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el producto de ESET que se ejecuta en su sistema operativo.

**Activar registro avanzado de mensajes push**: registra todos los sucesos que se produzcan durante los mensajes push.

**Activar registro avanzado del Protección del sistema de archivos en tiempo real**: registra todos los sucesos que tienen lugar durante el análisis de archivos y carpetas con la protección del sistema de archivos en tiempo real.

**Activar registro avanzado del motor de actualización**: registrar todos los eventos que se producen durante el proceso de actualización. Esto puede ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el motor de actualización.

**Activar registro avanzado de la interfaz del usuario**: Se registran todos los sucesos que se produzcan en la interfaz de usuario para permitir el diagnóstico y la resolución de problemas.

Los archivos de registro se encuentran en *C:\ProgramData\ESET\ESET Security\Diagnostics*.

# Soporte técnico

Cuando se pondrá en contacto con el servicio de soporte técnico de ESET desde ESET Small Business Security, puede enviar datos de configuración del sistema. Seleccione **Enviar siempre** en el menú desplegable **Enviar datos de configuración del sistema** para enviar los datos automáticamente, o seleccione **Preguntar antes de enviar** antes de que se envíen los datos.

# Archivos de registro

Puede encontrar la configuración de registro de ESET Small Business Security en Configuración avanzada > **Herramientas** > **Archivos de registro**. La sección de registros se utiliza para definir cómo se gestionarán los registros. El programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro. Puede especificar las siguientes opciones para los archivos de registro:

**Nivel mínimo de detalle al registrar**: especifica el nivel de contenido mínimo de los sucesos que se van a registrar:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.

- **Advertencias**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores críticos (errores al iniciar la protección antivirus, el cortafuegos, etc...).

> Al seleccionar el nivel de detalle de diagnóstico se registrarán todas las conexiones bloqueadas.

Las entradas de registro anteriores al número de días especificado en el campo **Eliminar automáticamente los registros con una antigüedad de más de (días)** se eliminarán de manera automática.

**Optimizar archivos de registro automáticamente**: si se marca esta opción, los archivos de registro se desfragmentarán automáticamente si el porcentaje es superior al valor especificado en **Si la cantidad de registros no usados supera el (%)**.

Haga clic en **Optimizar** para empezar la desfragmentación de los archivos de registro. Todas las entradas de registro vacías se eliminan durante este proceso, lo cual aumenta el rendimiento y la velocidad del proceso de registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

Active **Habilitar formato del texto** para activar el almacenamiento de registros en otro formato de archivo, independiente de Archivos de registro:

- **Directorio de destino**: el directorio donde se almacenarán los archivos de registro (solo se aplica a los formatos de texto y CSV). Cada sección de registros tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, virlog.txt para la sección **Amenazas detectadas** de los archivos de registro, si se utiliza el formato de archivo de texto plano para almacenar los registros).
- **Tipo**: si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto y los datos se separarán mediante tabuladores. El comportamiento es el mismo para el formato de archivo **CSV** con datos separados por comas. Si selecciona **Suceso**, los registros se almacenarán en el registro de eventos de Windows (que se puede ver en el Visor de eventos del Panel de control), en vez de en un archivo.
- **Eliminar todos los archivos de registro**: borra todos los registros almacenados que se seleccionen en el menú desplegable **Tipo**. Se mostrará una notificación sobre la correcta eliminación de los archivos de registro.

> ESET podría solicitarle los registros de su ordenador para agilizar la solución de problemas. ESET Log Collector facilita la recopilación de los datos necesarios. Para obtener más información sobre ESET Log Collector, consulte el artículo de la base de conocimientos de ESET.

# Interfaz del usuario

Para configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa, abra Configuración avanzada > **Interfaz de usuario**.

Puede ajustar el aspecto visual del programa y los efectos utilizados en la pantalla Configuración avanzada de elementos de la interfaz del usuario.

Si desea disponer del máximo nivel de seguridad del software de seguridad, proteja la configuración mediante

una contraseña para impedir la desinstalación o los cambios no autorizados con la herramienta Configuración de acceso.

Consulte el apartado Notificaciones para configurar el comportamiento de las notificaciones del sistema, las alertas de detección y los estados de la aplicación.

# Modo de presentación

El modo de presentación es una función para usuarios que exigen un uso del software sin interrupciones y sin ventanas de notificación o alerta, así como un menor uso de la CPU. Este modo también se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Al activar esta característica se desactivan todas las ventanas emergentes y la actividad del planificador de tareas se detiene por completo. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Puede activar o desactivar el modo de presentación en la ventana principal del programa, dentro de **Configuración** > **Protección del ordenador**. Para ello, haga clic en  o en  junto a **Modo de presentación**. Activar el modo de presentación constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección disponible en la barra de tareas se volverá naranja y mostrará un signo de alerta. Esta alerta también se puede ver en la ventana principal del programa donde verá el mensaje **Modo de presentación activo** en naranja.

Agregue o edite **Aplicaciones excluidas** para las que no se iniciará el modo de presentación. Consulte Aplicaciones excluidas del modo de presentación.

Active la opción **Activar el modo de presentación automáticamente al ejecutar aplicaciones en pantalla completa** en Configuración avanzada > **Herramientas** > **Modo de presentación** para que el Modo de presentación se active cuando inicie una aplicación a pantalla completa y se detenga cuando cierre dicha aplicación.

Deje habilitada la opción **No mostrar ventanas que requieran la interacción del usuario mientras el modo de presentación esté activo** y las ventanas interactivas no se mostrarán incluso cuando el modo de presentación esté activo.

Active **Desactivar el modo de presentación automáticamente después de** para definir la cantidad de tiempo que tardará en desactivarse el modo de presentación automáticamente.

Si el cortafuegos está en modo interactivo y el modo de presentación está activado, podría tener problemas para conectarse a Internet. Esto puede ser un problema si el juego necesita conexión a Internet. Por lo general, se le solicita que confirme dicha acción (si no se ha definido ninguna regla o excepción de comunicación), pero en el modo de presentación la intervención del usuario está desactivada. Para permitir la comunicación, defina una regla de comunicación para cualquier aplicación que pueda encontrar este problema, o utilice un Modo de filtrado en el cortafuegos. Recuerde que, si el modo de presentación está activado y accede a una página web o aplicación que presente un riesgo de seguridad potencial, esta podría bloquearse sin ninguna explicación o alerta, ya que la intervención del usuario está desactivada.

# Aplicaciones excluidas del modo de presentación

Puede seleccionar aplicaciones que no se ejecutarán en modo de presentación agregando el nombre o la ruta de acceso de una aplicación. Al ejecutar una aplicación excluida en modo de pantalla completa, no se utilizará el modo de presentación.

## Elementos de control

**Agregar**: agregue una aplicación excluida.

**Editar**: seleccione la aplicación que desea configurar y haga clic en **Editar**.

**Eliminar**: seleccione la aplicación que desea eliminar y haga clic en **Eliminar**.

**Importar/Exportar**: importe aplicaciones desde un archivo o guarde la lista actual de aplicaciones en un archivo.

# Elementos de la interfaz del usuario

Puede ajustar el entorno de trabajo (interfaz gráfica de usuario) de ESET Small Business Security según sus necesidades en Configuración avanzada > **Interfaz de usuario** > **Elementos de la interfaz de usuario**.

**Modo de color**: seleccione el esquema de colores de la interfaz gráfica de usuario de ESET Small Business Security en el menú desplegable:

- **Igual que el color del sistema**: define el esquema de colores de ESET Small Business Security según la configuración del sistema operativo.
- **Oscuro**: ESET Small Business Security tendrá un esquema de colores oscuros (modo oscuro).
- **Claro**: ESET Small Business Security tendrá un esquema de colores estándar y claro.

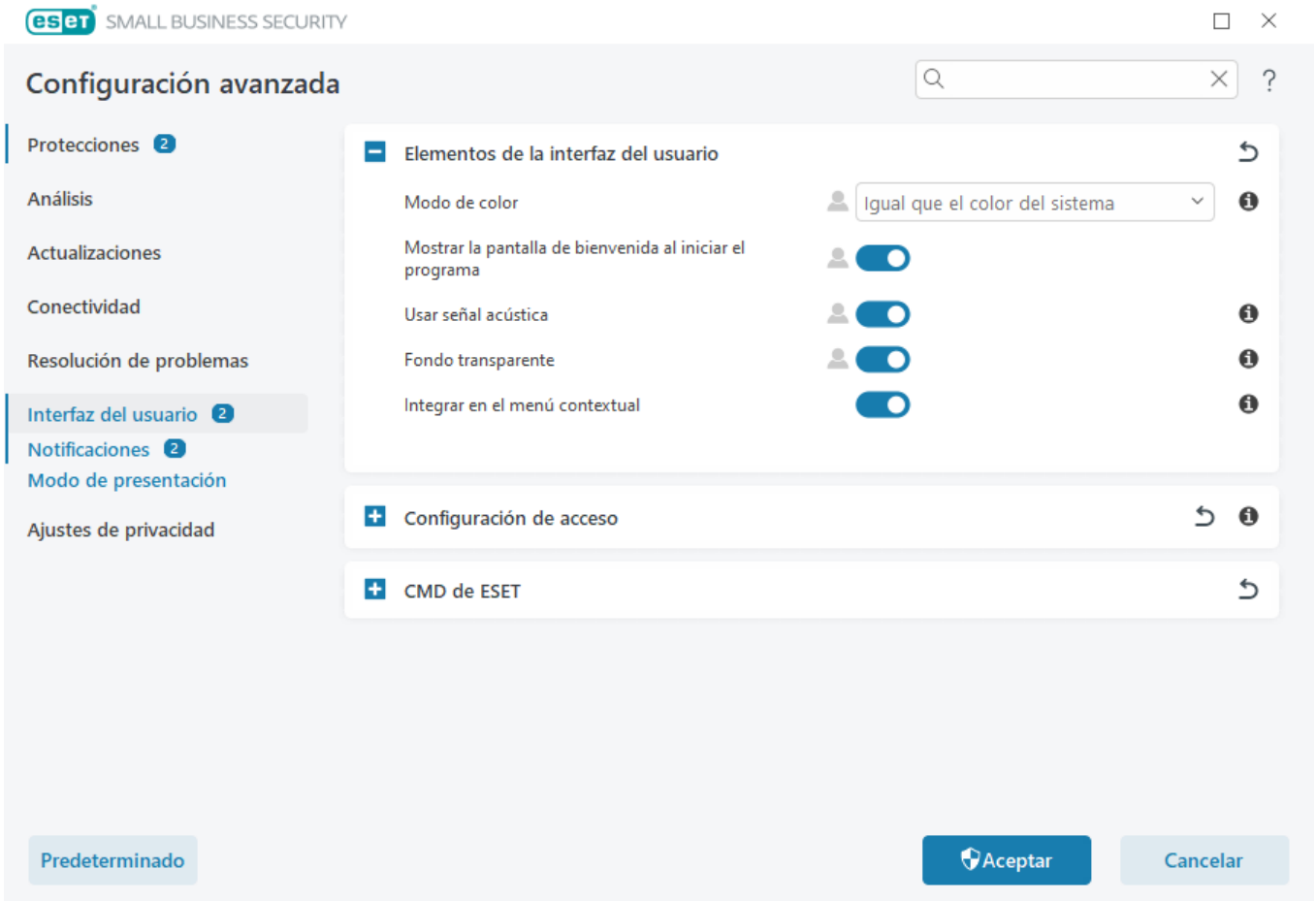
> También puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET Small Business Security en la esquina superior derecha de la ventana principal del programa.

**Mostrar la pantalla de bienvenida al iniciar el programa**: muestra la pantalla de bienvenida de ESET Small Business Security durante el inicio.

**Usar señal acústica**: reproduce un sonido cuando se producen sucesos importantes durante un análisis (por ejemplo al detectar una amenaza o al finalizar el análisis).

**Fondo transparente**: activa un efecto de fondo transparente para la ventana principal del programa. El fondo transparente solo está disponible para las versiones más recientes de Windows (RS4 y posteriores).

**Integrar en el menú contextual**: integra los elementos de control de ESET Small Business Security en el menú contextual.




# Configuración de acceso

La configuración de ESET Small Business Security es una parte crucial de la política de seguridad. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Para evitar modificaciones no autorizadas, los parámetros de configuración y la desinstalación de ESET Small Business Security se pueden proteger mediante contraseña. La configuración de acceso se puede configurar en Configuración avanzada > **Interfaz de usuario** > **Configuración de acceso**.

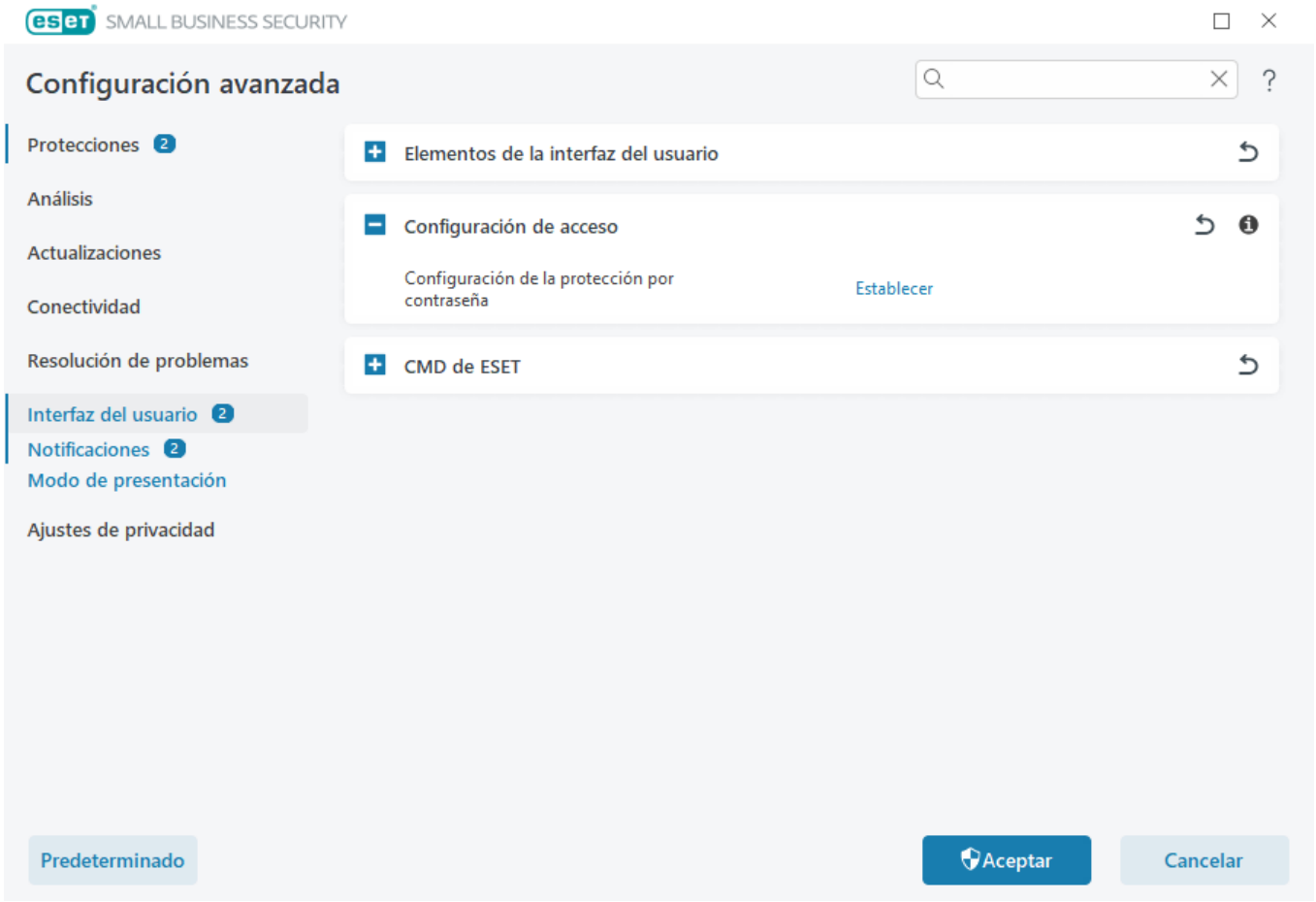
Para establecer una contraseña para proteger los parámetros de configuración y la desinstalación de ESET Small Business Security, haga clic en el botón **Establecer** junto a **Configuración de protección de contraseña**.

Cuando intenta acceder a la Configuración avanzada protegida , se muestra la ventana de introducción de contraseña. Si olvida o pierde la contraseña, haga clic en la opción **Restaurar contraseña** que aparece a continuación e introduzca la dirección de correo electrónico que utilizó para registrar la suscripción. ESET le enviará un mensaje de correo electrónico con el código de verificación e instrucciones sobre cómo restablecer la contraseña.

- Cómo desbloquear la Configuración avanzada

Para cambiar la contraseña, haga clic en **Cambiar contraseña** junto a **Configuración de protección de contraseña**.

Para quitar la contraseña, haga clic en **Quitar** junto a **Configuración de protección de contraseña**.




# Contraseña de Configuración avanzada

Para proteger la configuración avanzada de ESET Small Business Security y evitar modificaciones no autorizadas, escriba la nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**. Haga clic en **Aceptar**.

Si desea cambiar una contraseña:

1. Escriba la contraseña anterior en el campo **Contraseña anterior**.
2. Escriba la nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**.
3. Haga clic en **Aceptar**.

Esta contraseña será necesaria para acceder a la configuración avanzada.

Si olvida su contraseña, consulte Desbloquear contraseña de configuración en los productos domésticos de ESET.

Para recuperar la clave de activación de ESET perdida, la fecha de caducidad de su suscripción u otra información de suscripción a ESET Small Business Security, consulte He perdido mi clave de activación.

# CMD DE ESET

Se trata de una función que activa comandos de ecmd avanzados. Le permite exportar e importar la configuración utilizando la línea de comandos (ecmd.exe). Hasta ahora, solo era posible exportar la configuración utilizando la interfaz gráfica de usuario. La configuración de ESET Small Business Security puede exportarse a un archivo *.xml*.

Si tiene activado ESET CMD, dispone de dos métodos de autorización:

- **Ninguno**: sin autorización. No le recomendamos este método, ya que permite importar configuraciones no firmadas, lo que supone un riesgo.

- **Configuración avanzada de contraseña**: se requiere contraseña para importar una configuración de un archivo .xml. Este archivo debe estar firmado (consulte cómo se firma un archivo de configuración .xml más adelante). Debe introducirse la contraseña especificada en Configuración de acceso para poder importar una nueva configuración. Si no ha activado la configuración de acceso, la contraseña no coincide o el archivo de configuración .xml no está firmado, la configuración no se importará.

Una vez que ESET CMD esté activado, podrá utilizar la línea de comandos para importar o exportar configuraciones de ESET Small Business Security. Podrá hacerlo manualmente o crear un script con fines de automatización.

Para poder utilizar comandos de ecmd avanzados, deberá ejecutarlos con privilegios de administrador, o abrir el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**. De lo contrario, se mostrará el mensaje **Error executing command**. Asimismo, a la hora de exportar una configuración, deberá existir una carpeta de destino. El comando de exportación sigue funcionando cuando se desactiva el ajuste ESET CMD.

Comando para exportar configuración:
`ecmd /getcfg c:\config\settings.xml`

Comando para importar configuración:
`ecmd /setcfg c:\config\settings.xml`

Los comandos ecmd avanzados solo pueden ejecutarse de forma local.

Cómo firmar un archivo de configuración *.xml*:

1. Descargue el archivo ejecutable XmlSignTool.

2. Abra el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**.

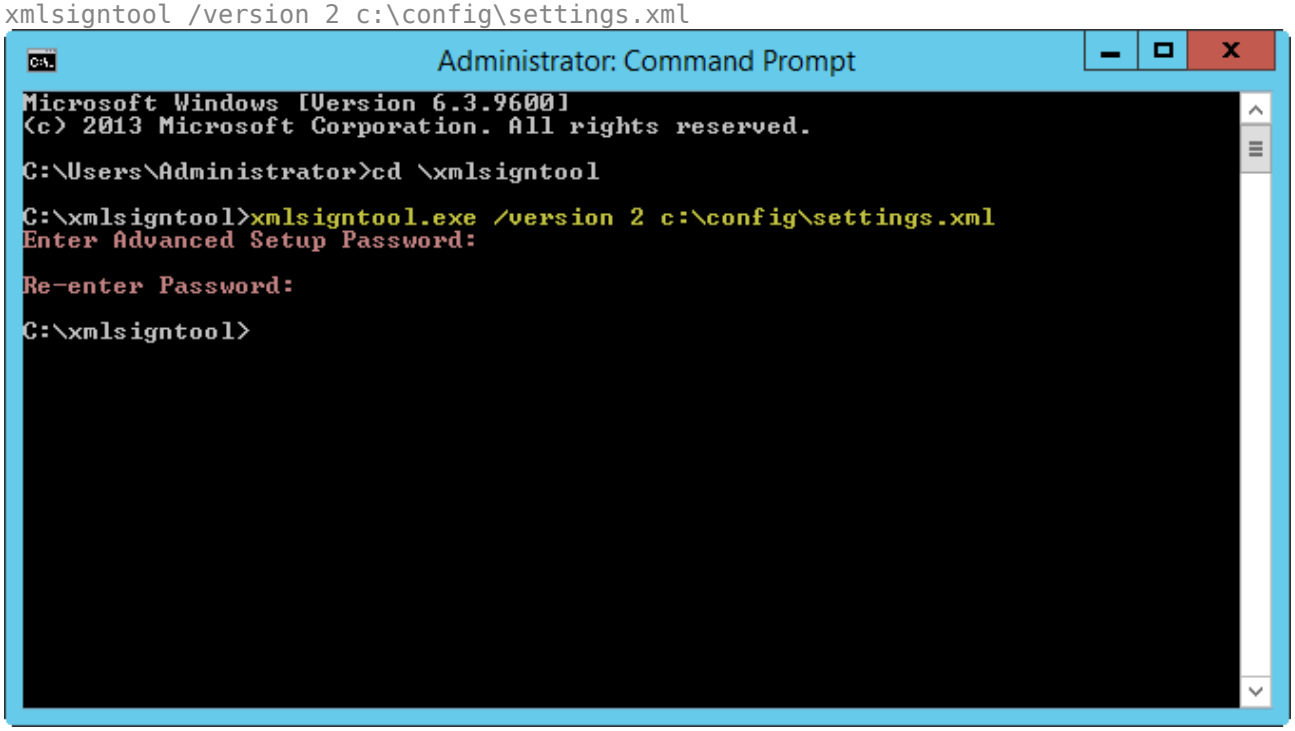
3. Vaya a la ubicación en la que se ha guardado `xmlsigntool.exe`.

4. Ejecute un comando para firmar el archivo de configuración *.xml*; uso: `xmlsigntool /version 1|2 <xml_file_path>`.

El valor del parámetro `/version` depende de su versión de ESET Small Business Security. Utilice `/version 1` para versiones de ESET Small Business Security anteriores a 11.1. Utilice `/version 2` para la versión actual de ESET Small Business Security.

5. Introduzca y vuelva a introducir la contraseña de Configuración avanzada cuando se lo solicite XmlSignTool. Su archivo de configuración *.xml* ya estará firmado y podrá utilizarse para importar otra instancia de ESET Small Business Security con ESET CMD utilizando el método de autorización de contraseña.

Comando para firmar un archivo de configuración exportado:
`xmlsigntool /version 2 c:\config\settings.xml`




Si la contraseña de Configuración de acceso cambia y desea importar una configuración firmada anteriormente con una contraseña antigua, tendrá que volver a firmar el archivo de configuración *.xml* utilizando la contraseña actual. Esto le permitirá utilizar un archivo de configuración más antiguo sin necesidad de exportarlo a otro equipo que ejecute ESET Small Business Security antes de la importación.

No se recomienda activar el CMD de ESET sin autorización, ya que hacerlo permitirá importar configuraciones no firmadas. Configure la contraseña en Configuración avanzada > **Interfaz de usuario** > **Configuración de acceso** para evitar que los usuarios realicen modificaciones no autorizadas.

# Compatibilidad con lectores de pantalla

ESET Small Business Security se puede usar con lectores de pantalla para permitir que los usuarios de ESET discapacitados visuales puedan navegar por el producto o configurar los ajustes. Se admiten los siguientes lectores de pantalla: (JAWS, NVDA, Narrator).

Para asegurarse de que el software de lector de pantalla pueda acceder a la interfaz gráfica de usuario de ESET Small Business Security correctamente, siga las instrucciones del artículo de la base de conocimiento.

# Notificaciones

Para administrar las notificaciones de ESET Small Business Security, abra Configuración avanzada > **Notificaciones**. Puede definir los tipos de notificaciones siguientes:

- Estados de la aplicación: notificaciones que se muestran en la ventana principal del programa > **Información general**.
- Notificaciones en el escritorio: pequeñas ventanas de notificación junto a la barra de tareas del sistema.
- Alertas interactivas: ventanas de alerta y cuadros de mensajes que requieren la intervención del usuario.

• Reenvío (Notificaciones por correo electrónico): las notificaciones por correo electrónico se envían a la dirección de correo electrónico especificada.

---


### Estados de la aplicación

**Estados de la aplicación**: haga clic en **Editar** para seleccionar los estados de la aplicación que se muestran en la sección de inicio de la ventana principal del programa > **Información general**.

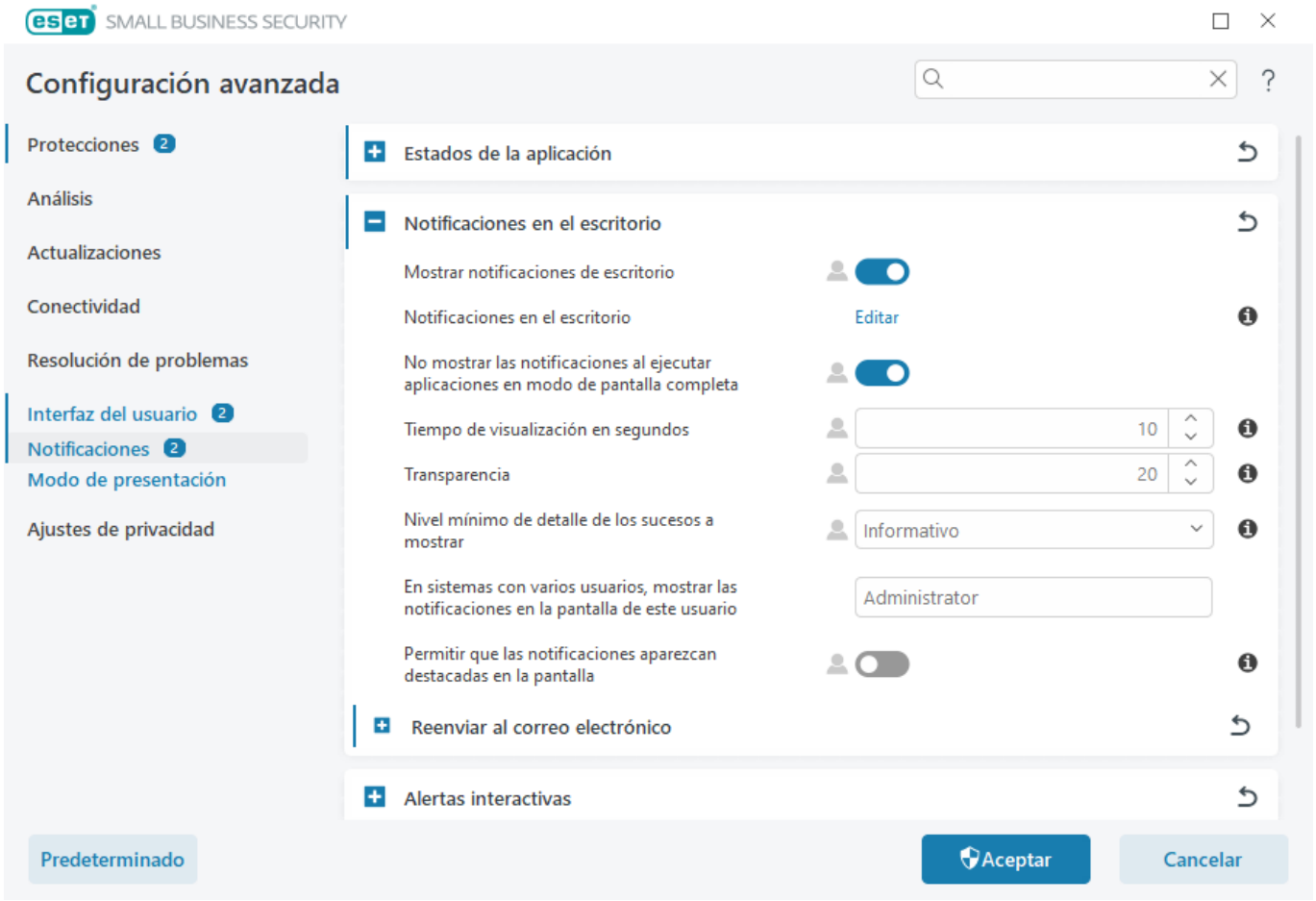
# Ventana de diálogo: estados de la aplicación

En este cuadro de diálogo puede seleccionar los estados de aplicación que se mostrarán. Por ejemplo, cuando pone en pausa la protección antivirus y antiespía o cuando activa el modo de presentación.

El estado de la aplicación también se mostrará si su producto no está activado o la suscripción ha caducado.

# Notificaciones en el escritorio

Las notificaciones en el escritorio se representan mediante una pequeña ventana notificación situada junto a la barra de tareas del sistema. De forma predeterminada, se muestra durante 10 segundos y, a continuación, desaparece lentamente. Entre las notificaciones se incluyen actualizaciones correctas del producto, nuevos dispositivos conectados, finalización de tareas de análisis de virus o nuevas amenazas encontradas.




**Mostrar notificaciones en el escritorio:** se recomienda mantener esta opción activada, para que el producto pueda informarle cuando se produce un suceso nuevo.

**Notificaciones en el escritorio**: haga clic en **Editar** para activar o desactivar las notificaciones en el escritorio.

**No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa**: suprime todas las notificaciones que no son interactivas al ejecutar aplicaciones en modo de pantalla completa.

**Tiempo de visualización en segundos**: definir la duración de la visibilidad de la notificación. El valor debe estar entre 3 y 30 segundos.

**Transparencia**: definir el porcentaje de transparencia de la notificación. El intervalo admitido es de 0 (sin transparencia) a 80 (transparencia muy alta).

**Nivel mínimo de detalle de los suceso a mostrar**: definir el nivel de gravedad de la notificación inicial mostrado. Seleccione una de las siguientes opciones en el menú desplegable:

- **Diagnóstico**: muestra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: muestra los mensajes informativos, como los sucesos de red no convencionales, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Advertencias**: muestra mensajes de advertencia, errores y errores críticos (por ejemplo, si la actualización ha fallado).
- **Errores**: muestra errores (por ejemplo, si la protección de documentos no se ha iniciado) y errores críticos.

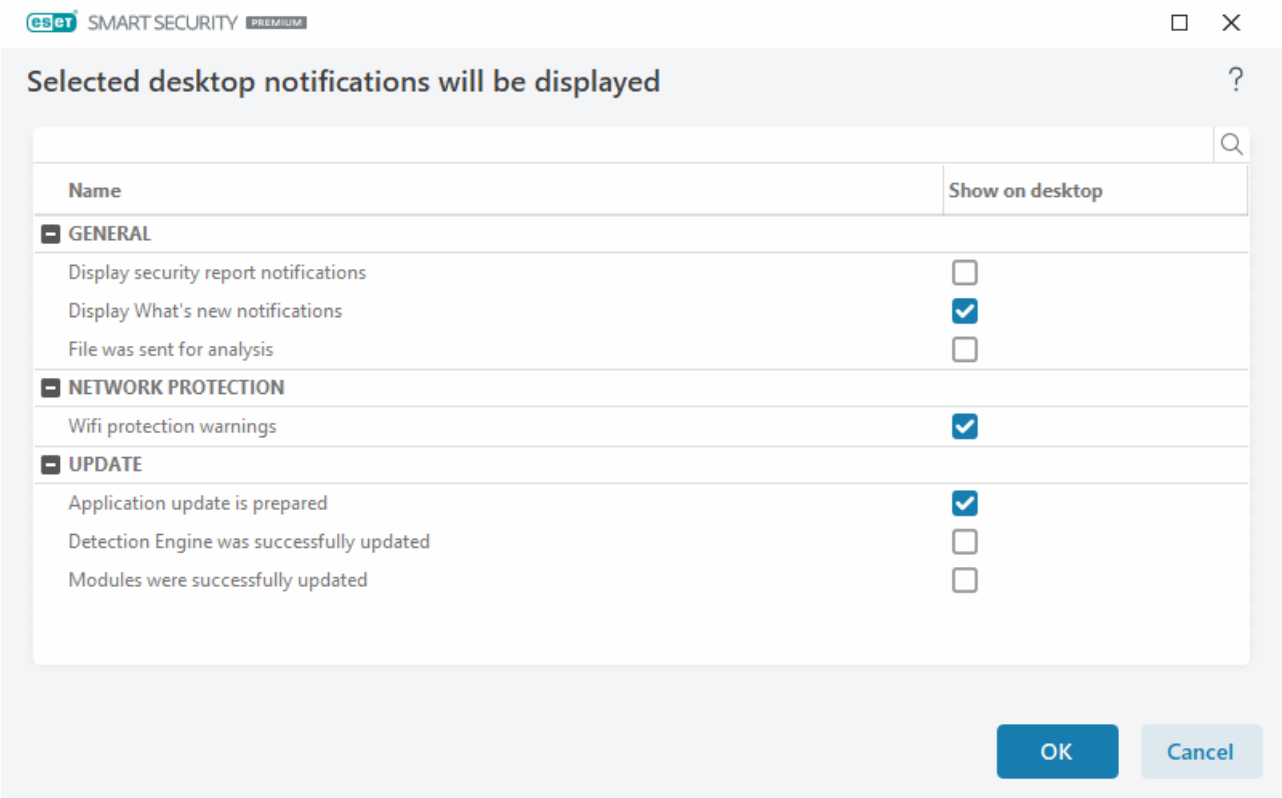
- **Críticos**: muestra solo errores críticos (error al iniciar la protección antivirus, sistema infectado, etc.).

**En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este usuario**: permite que la cuenta seleccionada reciban notificaciones en el escritorio. Por ejemplo, si no utiliza la cuenta de administrador, escriba el nombre completo de la cuenta para que se muestren las notificaciones en el escritorio relacionadas. Solo una cuenta de usuario puede recibir las notificaciones en el escritorio.

**Permitir que las notificaciones aparezcan destacadas en la pantalla**: permite que las notificaciones aparezcan destacadas en la pantalla y que se pueda acceder a ellas en el menú **ALT + Tab**.

# Lista de notificaciones en el escritorio

Para ajustar la visibilidad de las notificaciones en el escritorio (mostradas en la parte inferior derecha de la pantalla), abra Configuración avanzada > **Interfaz de usuario** > **Notificaciones** > **Notificaciones en el escritorio**. Haga clic en **Editar** junto a **Notificaciones en el escritorio** y marque la casilla **Mostrar**.




## General

**Mostrar notificaciones del informe de seguridad**: envía una notificación cuando se genera un nuevo Informe de seguridad.

**Mostrar notificaciones de novedades**: notificaciones sobre funciones nuevas y mejoradas de la versión más reciente del producto.

**El archivo se ha enviado para su análisis**: envía una notificación cada vez que ESET Small Business Security envía un archivo para su análisis.

## Inspector de red

**Notificaciones de dispositivos de red recién detectados**: reciba una notificación cuando se conecte un nuevo dispositivo a la red.

## Protección de la red

**Perfil de red cambiado**: reciba una notificación cuando se cambie el perfil de red.

**Advertencias de protección Wi-Fi**: reciba una notificación cuando intente conectarse a una red Wi-Fi con una contraseña débil o sin contraseña.

## Actualización

**La actualización de la aplicación está preparada**: envía una notificación cuando haya una actualización de una nueva versión de ESET Small Business Security preparada.

**El motor de detección se ha actualizado correctamente**: envía una notificación cuando el producto actualiza los módulos del Motor de detección.

**Los módulos se han actualizado correctamente**: recibe una notificación cuando el producto actualiza los componentes del programa.

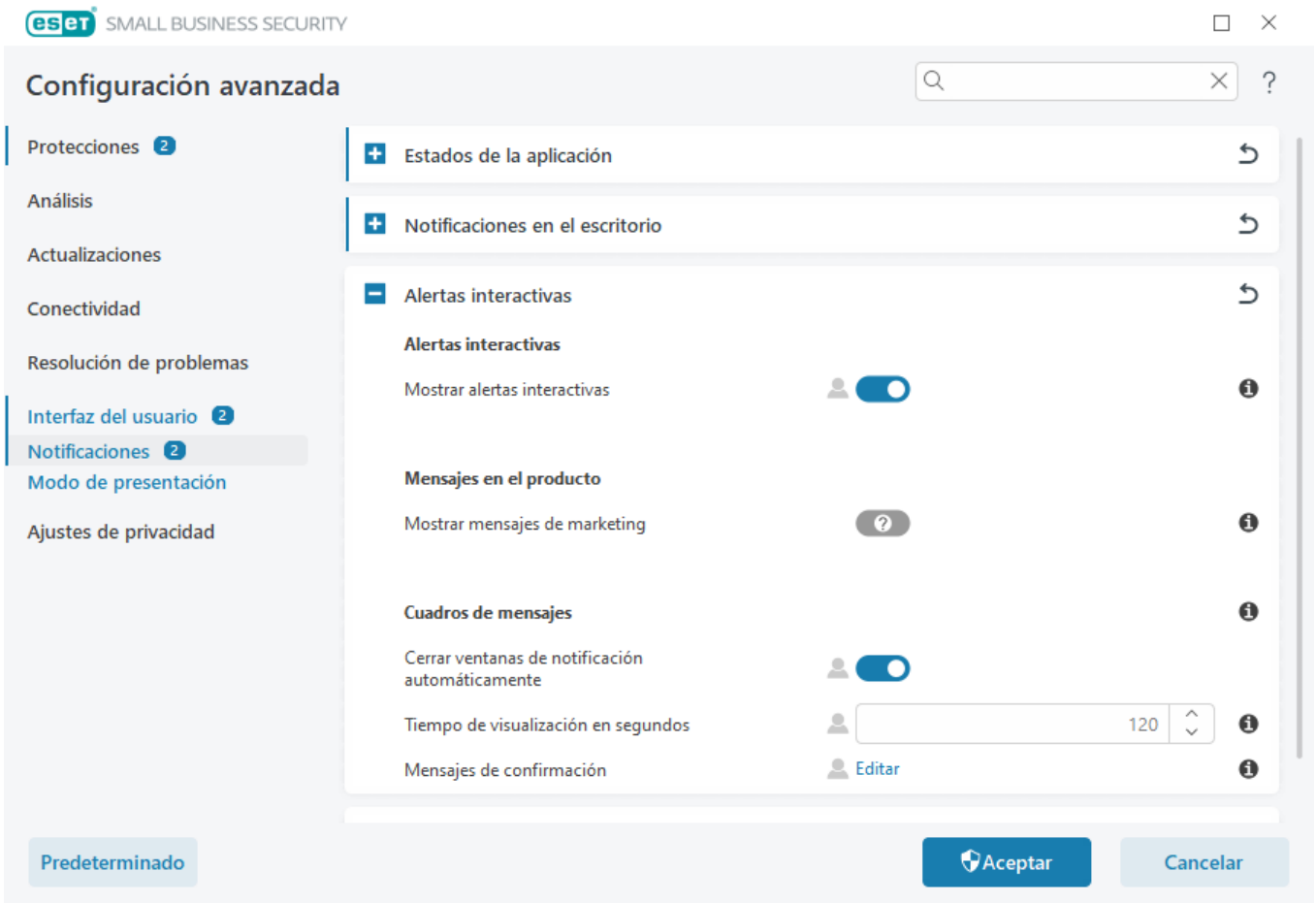
Para configurar los ajustes generales de las notificaciones en el escritorio (por ejemplo, cuánto tiempo se muestra un mensaje o el nivel de detalle mínimo de los sucesos que se debe mostrar), consulte Notificaciones en el escritorio en Configuración avanzada > **Interfaz del usuario** > **Notificaciones**.

# Alertas interactivas

¿Busca información sobre alertas y notificaciones habituales?

- Amenaza detectada
- La dirección se ha bloqueado.
- El producto no está activado
- Actualización disponible
- La información de actualización no es consistente
- Solución de problemas para el mensaje "Error de actualización de los módulos"
- Resolver errores de actualización de módulos
- Amenaza de red bloqueada
- El certificado del sitio web se ha revocado

La sección **Alertas interactivas** de Configuración avanzada > **Notificaciones** le permite configurar cómo gestiona ESET Small Business Security los cuadros de mensajes y las alertas interactivas de las detecciones cuando un usuario debe tomar una decisión (por ejemplo, sitios web que pueden ser de phishing).




## Alertas interactivas

Si desactiva la opción **Mostrar alertas interactivas**, se ocultarán todas las ventanas de alerta y los cuadros de diálogo del navegador. Solo resulta útil para una serie de situaciones muy específicas. Se recomienda mantener esta opción activada.

## Mensajes en el producto

Los mensajes en el producto están pensados para informar a los usuarios acerca de noticias de ESET y otras comunicaciones. Para que se envíen los mensajes de marketing, es necesario que el usuario dé su consentimiento. Los mensajes de marketing no se envían a los usuarios de forma predeterminada (se muestran como un signo de interrogación).
Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no le interesa recibir material de marketing de ESET, desactive la opción **Mostrar mensajes de marketing**.

## Cuadros de mensajes

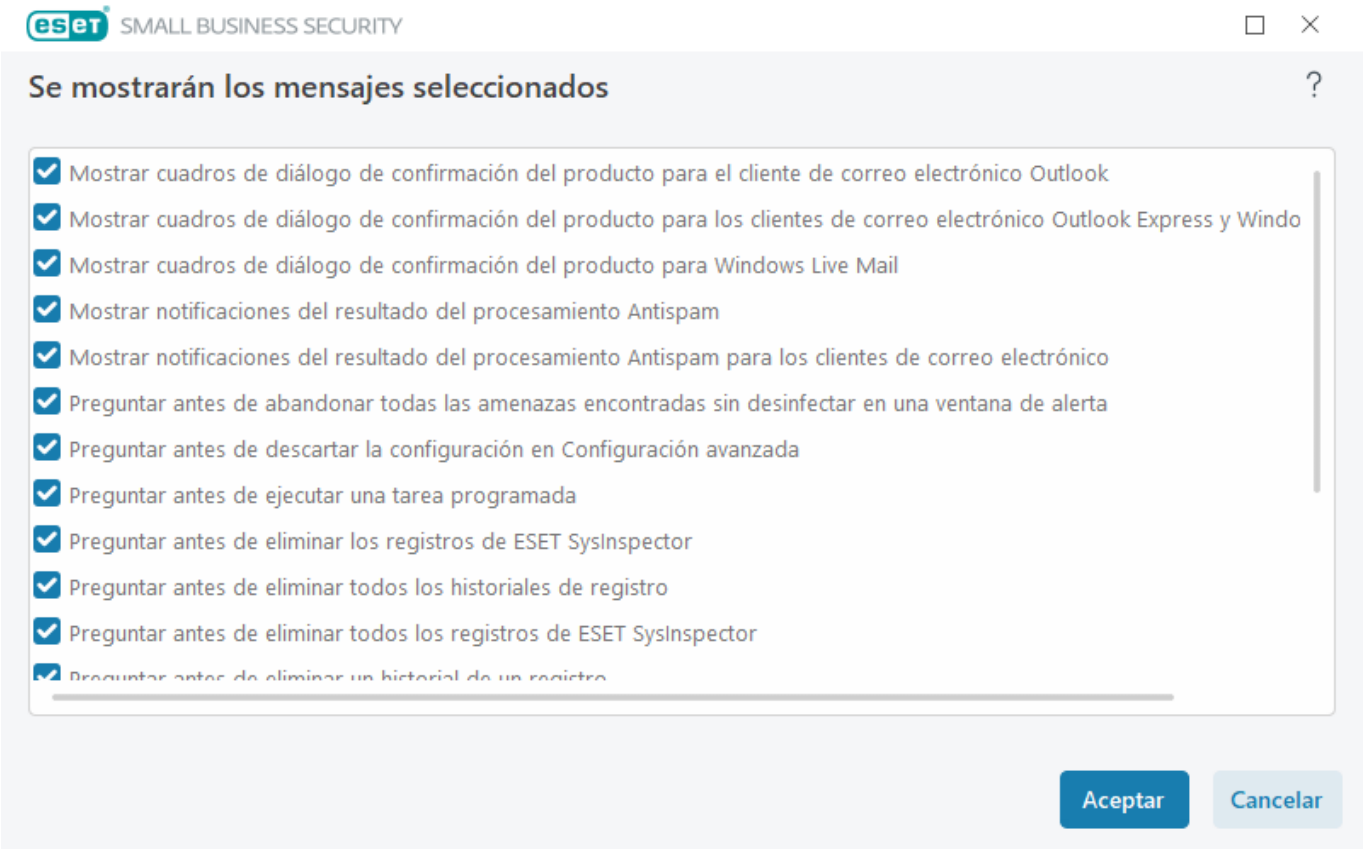
Para cerrar los cuadros de mensajes automáticamente después de un de tiempo determinado, seleccione la opción **Cerrar cuadros de mensajes automáticamente**. Si no se cierran de forma manual, las ventanas de alerta se cerrarán automáticamente cuando haya transcurrido el periodo de tiempo especificado.

**Tiempo de visualización en segundos**: define la duración de la visibilidad de la alerta. El valor debe estar entre 10 y 999 segundos.

**Mensajes de confirmación**: haga clic en **Editar** para ver una lista de mensajes de confirmación que se pueden seleccionar para que se muestren o no.

# Mensajes de confirmación

Para ajustar los mensajes de confirmación, abra Configuración avanzada > **Notificaciones** > **Alertas interactivas** y haga clic en **Editar** junto a **Mensajes de confirmación**.




En este cuadro de diálogo se muestran los mensajes de confirmación que mostrará ESET Small Business Security antes de que se realice cualquier acción. Seleccione o anule la selección de la casilla de verificación disponible junto a cada mensaje de confirmación para permitirlo o desactivarlo.

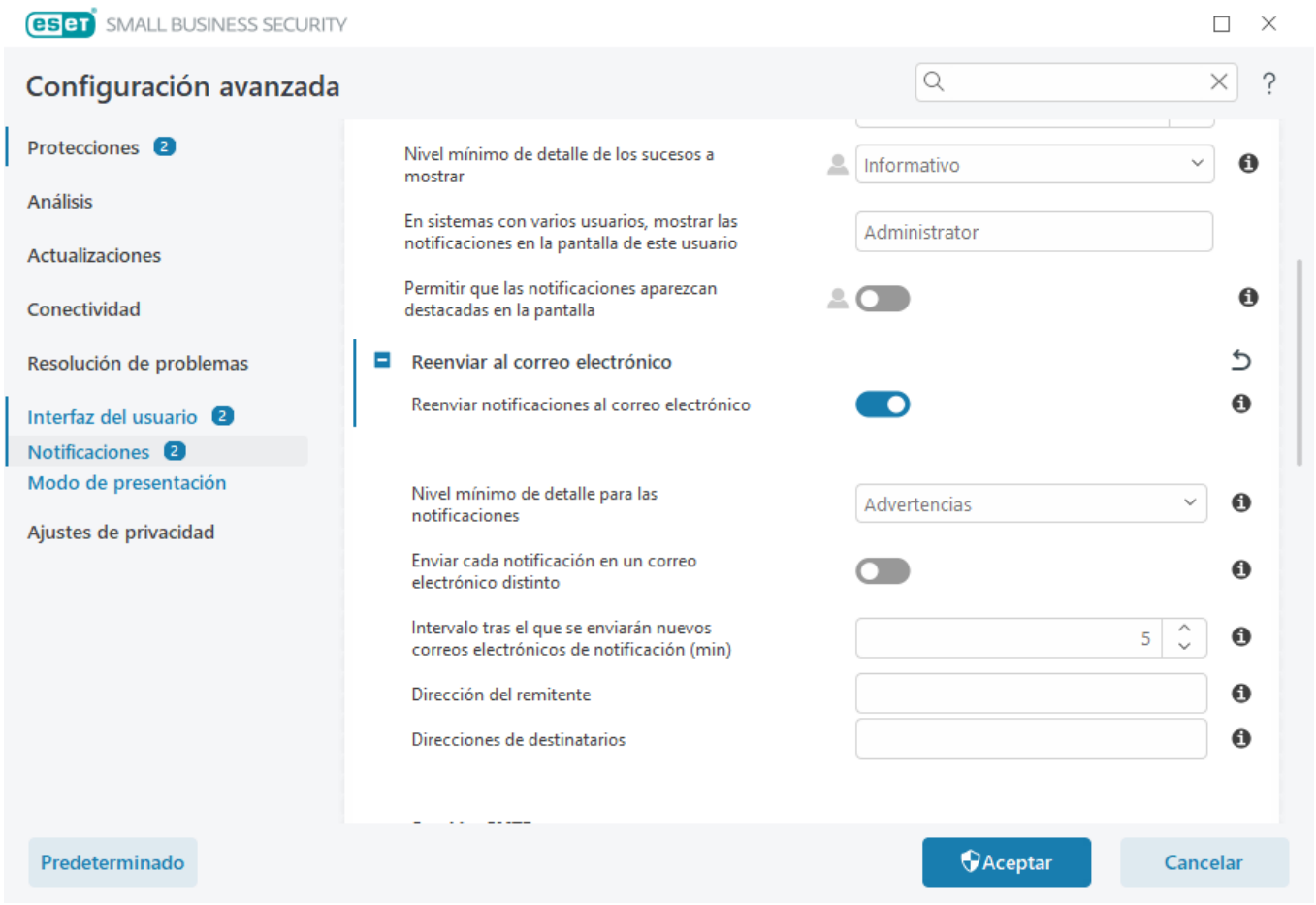
Obtenga más información sobre la función específica relacionada con los mensajes de confirmación:

- Preguntar antes de eliminar registros de ESET SysInspector
- Preguntar antes de eliminar todos los registros de ESET SysInspector
- Preguntar antes de eliminar un objeto de cuarentena
- Preguntar antes de descartar la configuración en Configuración avanzada
- Preguntar antes de abandonar todas las amenazas encontradas sin desinfectar en una ventana de alerta
- Preguntar antes de eliminar un historial de un registro
- Preguntar antes de eliminar una tarea programada
- Preguntar antes de eliminar todos los historiales de registro
- Preguntar antes de restablecer las estadísticas

- Preguntar antes de restaurar un objeto de cuarentena
- Preguntar antes de restaurar objetos de cuarentena y excluirlos del análisis
- Preguntar antes de ejecutar una tarea programada
- Mostrar notificaciones del resultado del procesamiento Antispam
- Mostrar notificaciones del resultado del procesamiento Antispam para los clientes de correo electrónico
- Mostrar cuadros de diálogo de confirmación del producto para los clientes de correo electrónico Outlook Express y Windows Mail
- Mostrar cuadros de diálogo de confirmación del producto para Windows Live Mail
- Mostrar cuadros de diálogo de confirmación del producto para el cliente de correo electrónico Outlook

# Reenvío

ESET Small Business Security puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Abra Configuración avanzada > **Notificaciones** > **Reenvío** y active **Reenviar notificaciones al correo electrónico** para permitir las notificaciones por correo electrónico.




En el menú desplegable **Nivel mínimo de detalle para las notificaciones** puede seleccionar el nivel de gravedad inicial de las notificaciones que desea enviar.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, como los sucesos de red no convencionales, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Advertencias**: registra errores graves y mensajes de alerta (por ejemplo, un fallo de actualización).
- **Errores**: se registran los errores (protección de documentos no iniciada) y los errores graves.
- **Crítico**: registra solo errores críticos (por ejemplo, Error al activar la protección antivirus o Amenaza detectada).

**Enviar cada notificación en un correo electrónico distinto**: si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría suponer la recepción de varios correos electrónicos en un breve periodo de tiempo.

**Intervalo tras el que se enviarán nuevos correos electrónicos de notificación (min)**: intervalo en minutos tras el cual se enviarán nuevas notificaciones al correo electrónico. Si define este valor en 0, las notificaciones se enviarán de forma inmediata.

**Dirección del remitente**: defina la dirección de correo del emisor que se mostrará en el encabezado de los mensajes de correo electrónico de notificación.

**Direcciones de destinatarios**: defina las direcciones de correo de los destinatarios que se muestran en el encabezado de los mensajes de correo electrónico de notificación. Es posible incluir varios valores. Utilice el punto y coma como separador.

## SMTPServidor

Servidor **SMTP**: el servidor SMTP que se utiliza para enviar notificaciones (por ejemplo, smtp.provider.com:587; el puerto predefinido es 25).

Los servidores SMTP con cifrado TLS son compatibles con ESET Small Business Security.

**Nombre de usuario** y **contraseña**: si el servidor SMTP requiere autenticación, estos campos deben cumplimentarse con un nombre de usuario y una contraseña válidos que faciliten el acceso al servidor SMTP.

**Habilitar TLS**: Secure Alert y notificaciones con cifrado TLS.

**Probar conexión SMTP**: se enviará un correo electrónico de prueba a la dirección de correo del destinatario. Es necesario rellenar los campos Servidor SMTP, Nombre de usuario, Contraseña, Dirección del remitente y Direcciones de destinatarios.

## Formato de mensajes

Las comunicaciones entre el programa y un usuario o administrador de sistemas remotos se realizan a través de mensajes de correo electrónico o mensajes de red local (mediante el servicio de mensajería de Windows). El **formato predeterminado de los mensajes** de alerta y las notificaciones será el óptimo para la mayoría de situaciones. En algunas circunstancias, tendrá que cambiar el formato de los mensajes de sucesos.

**Para notificar la ocurrencia de sucesos**: formato de los mensajes de suceso que se muestran en los ordenadores

remotos.

**Formato de mensajes de alerta de amenazas**: los mensajes de notificación y alerta de amenazas tienen un formato predefinido. Se recomienda mantener el formato predeterminado. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes.

**Conjunto de caracteres**: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI según la configuración regional de Windows (por ejemplo, windows-1250, Unicode (UTF-8), ACSII 7-bit o japonés (ISO-2022-JP)). El resultado es que "á" se cambiará por "a" y un símbolo desconocido, por "?".

**Usar codificación Quoted-printable**: el origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo pude transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (áéíóú).

- **%TimeStamp%**: Fecha y hora del suceso.
- **%Scanner%**: Módulo correspondiente.
- **%ComputerName%**: Nombre del ordenador en el que se produjo la alerta.
- **%ProgramName%**: Programa que generó la alerta.
- **%InfectedObject%**: Nombre del archivo, mensaje u otro elemento infectado.
- **%VirusName%**: Identificación de la infección.
- **%Action%**: Acción adoptada respecto a la amenaza.
- **%ErrorDescription%**: Descripción de un suceso que no está relacionado con un virus.

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se utilizan en los mensajes de alerta de amenaza y **%ErrorDescription%**, en los mensajes de sucesos.

# Microsoft Windows® update

La función de actualización de Windows es un componente importante a la hora de proteger a los usuarios de software malicioso. Por eso es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Small Business Security le informa sobre las actualizaciones que le faltan, según el nivel que haya especificado en Configuración avanzada > **Herramientas**. Están disponibles los siguientes niveles:

- **Sin actualizaciones**: no se ofrecerá ninguna actualización del sistema para la descarga.
- **Actualizaciones opcionales**: se ofrecerán para la descarga las actualizaciones marcadas como de baja prioridad y de niveles superiores.
- **Actualizaciones recomendadas**: se ofrecerán para la descarga las actualizaciones marcadas como habituales y de niveles superiores.
- **Actualizaciones importantes**: se ofrecerán para la descarga las actualizaciones marcadas como importantes y de niveles superiores.

- **Actualizaciones críticas**: solo se ofrecerá la descarga de actualizaciones críticas.

# Cuadro de diálogo: Actualizaciones del sistema

Si hay actualizaciones para su sistema operativo, ESET Small Business Security muestra una notificación en la ventana principal del programa > **Información general**. Haga clic en **Más información** para abrir la ventana de actualizaciones del sistema.

En la ventana de actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para su descarga e instalación. El tipo de actualización se muestra junto a su nombre.

Haga doble clic en la fila de una de las actualizaciones para que se muestre la ventana Información de actualización con información adicional.

Haga clic en **Ejecutar actualización del sistema** para descargar e instalar todas las actualizaciones del sistema operativo incluidas en la lista.

# Información de actualización

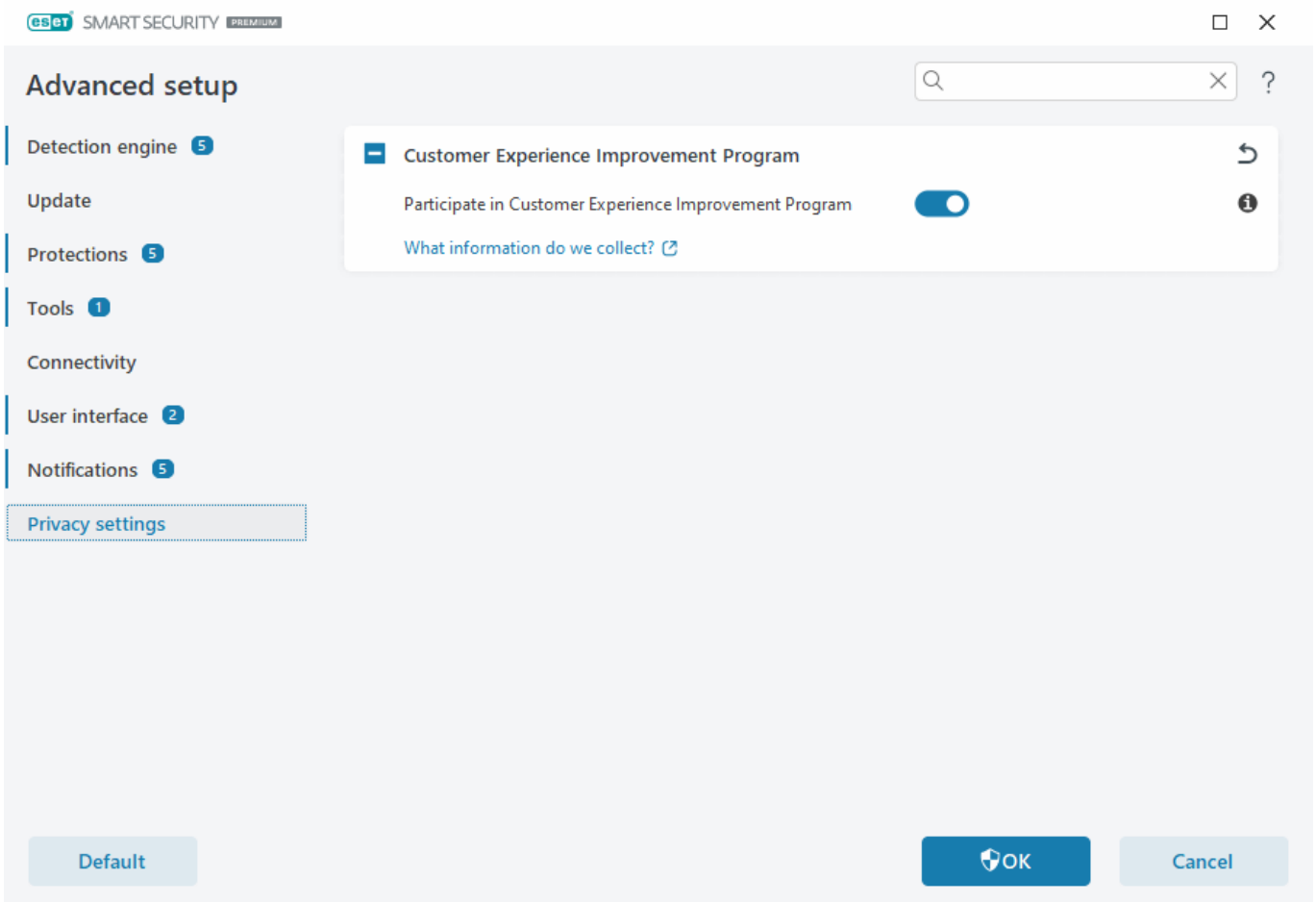
En la ventana de actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para su descarga e instalación. El nivel de prioridad de la actualización se muestra junto a su nombre.

Haga clic en **Ejecutar actualización del sistema** para iniciar la descarga e instalar las actualizaciones del sistema operativo.

Haga clic con el botón derecho del ratón en cualquier fila de actualización y, a continuación, haga clic en **Mostrar información** para abrir una ventana nueva con información adicional.

# Ajustes de privacidad

Abra Configuración avanzada > **Configuración de privacidad**.




## Programa de mejora de la experiencia de los clientes

Active el interruptor situado junto a **Participar en el Programa de mejora de la experiencia del cliente** para unirse a dicho programa. Al unirse, proporciona a ESET información anónima sobre el uso de productos de ESET. Los datos recopilados nos ayudarán a mejorar su experiencia y no se compartirán con terceros. ¿Qué información recopilamos?

# Recuperar configuración predeterminada

Haga clic en **Predeterminado** en Configuración avanzada para restablecer todos los ajustes del programa para todos los módulos. Esto restablecerá los ajustes al estado que habrían tenido tras una nueva instalación.

Consulte también Importar y exportar configuración.

# Restaurar todas las opciones de esta sección

Haga clic en la flecha curva  para restaurar los ajustes predeterminados definidos por ESET de todas las opciones de esta sección.

Tenga en cuenta que, al hacer clic en **Restaurar predeterminados**, se perderán todos los cambios realizados.

**Restaurar el contenido de las tablas**: si está activada, se perderán las reglas, tareas o perfiles que se hayan añadido de forma manual o automática.

Consulte también Importar y exportar configuración.

# Error al guardar la configuración

Este mensaje de error indica que la configuración no se guardó correctamente debido a un error.

Esto suele significar que el usuario que intentó modificar los parámetros del programa:

- no tiene suficientes derechos de acceso o no tiene los privilegios necesarios en el sistema operativo para modificar archivos de configuración y el registro del sistema.
  > Para realizar las modificaciones deseadas, el administrador del sistema debe iniciar sesión.

- ha activado recientemente Modo de aprendizaje en HIPS o Cortafuegos e intentado realizar cambios en Configuración avanzada.
  > Para guardar la configuración y evitar el conflicto de configuración, cierre Configuración avanzada sin guardar e intente realizar los cambios deseados de nuevo.

La segunda causa más común es que el programa ya no funcione correctamente, que esté dañado y, por lo tanto, se deba volver a instalar.

# Análisis de línea de comandos

El módulo antivirus de ESET Small Business Security se puede iniciar manualmente a través de la línea de comandos, con el comando "ecls" o con un archivo por lotes ("bat").

Uso del análisis de línea de comandos de ESET:

```
ecls [OPTIONS..] FILES..
```

Los siguientes parámetros y modificadores se pueden utilizar al ejecutar el análisis a petición desde la línea de comandos:

## Opciones

| | |
|---|---|
| /base-dir=CARPETA | cargar módulos desde una CARPETA |
| /quar-dir=CARPETA | CARPETA de cuarentena |
| /exclude=MÁSCARA | excluir del análisis los archivos que cumplan MÁSCARA |
| /subdir | analizar subcarpetas (predeterminado) |
| /no-subdir | no analizar subcarpetas |
| /max-subdir-level=NIVEL | máximo nivel de anidamiento para subcarpetas a analizar |
| /symlink | seguir enlaces simbólicos (predeterminado) |
| /no-symlink | omitir enlaces simbólicos |
| /ads | analizar ADS (predeterminado) |
| /no-ads | no analizar ADS |
| /log-file=ARCHIVO | registrar salida en ARCHIVO |
| /log-rewrite | sobrescribir el archivo de salida (predeterminado – agregar) |

| | |
|---|---|
| /log-console | enviar registro a la consola (predeterminado) |
| /no-log-console | no enviar registro a la consola |
| /log-all | registrar también los archivos sin infectar |
| /no-log-all | no registrar archivos sin infectar (predeterminado) |
| /aind | mostrar indicador de actividad |
| /auto | analizar y desinfectar automáticamente todos los discos locales |

## Opciones de análisis

| | |
|---|---|
| /files | analizar archivos (predeterminado) |
| /no-files | no analizar archivos |
| /memory | analizar memoria |
| /boots | analizar sectores de inicio |
| /no-boots | no analizar sectores de inicio (predeterminado) |
| /arch | analizar archivos comprimidos (predeterminado) |
| /no-arch | no analizar archivos |
| /max-obj-size=TAMAÑO | analizar solo archivos menores de TAMAÑO megabytes (predeterminado 0 = ilimitado) |
| /max-arch-level=NIVEL | máxima profundidad de anidamiento para archivos comprimidos (archivos anidados) a analizar |
| /scan-timeout=LÍMITE | analizar archivos comprimidos durante LÍMITE segundos como máximo |
| /max-arch-size=TAMAÑO | analizar los archivos dentro de un archivo comprimido solo si su tamaño es inferior a TAMAÑO (predeterminado 0 = ilimitado) |
| /max-sfx-size=TAMAÑO | analizar solo los archivos en un archivo comprimido de autoextracción si su tamaño es inferior a TAMAÑO megabytes (predeterminado 0 = ilimitado) |
| /mail | analizar archivos de correo (predeterminado) |
| /no-mail | no analizar archivos de correo |
| /mailbox | analizar buzones de correo (predeterminado) |
| /no-mailbox | no analizar buzones de correo |
| /sfx | analizar archivos comprimidos de autoextracción (predeterminado) |
| /no-sfx | no analizar archivos comprimidos de autoextracción |
| /rtp | analizar empaquetadores en tiempo real (predeterminado) |
| /no-rtp | no analizar empaquetadores en tiempo real |
| /unsafe | analizar en busca de aplicaciones potencialmente peligrosas |
| /no-unsafe | no analizar en busca de aplicaciones potencialmente peligrosas |
| /unwanted | analizar en busca de aplicaciones potencialmente indeseables |
| /no-unwanted | no analizar en busca de aplicaciones potencialmente indeseables (predeterminado) |
| /suspicious | analizar en busca de aplicaciones sospechosas (predeterminado) |
| /no-suspicious | no analizar en busca de aplicaciones sospechosas |
| /pattern | usar firmas (predeterminado) |
| /no-pattern | no usar firmas |
| /heur | activar heurística (predeterminado) |

| | |
|---|---|
| /no-heur | desactivar heurística |
| /adv-heur | activar heurística avanzada (predeterminado) |
| /no-adv-heur | desactivar heurística avanzada |
| /ext-exclude=EXTENSIONES | excluir EXTENSIONES de archivo del análisis, separándolas por el signo ":" (dos puntos) |
| /clean-mode=MODO | utilizar el MODO desinfección para objetos infectados<br><br>Están disponibles las opciones siguientes:<br>• `none` (predeterminado): no se realiza la desinfección automática.<br>• `standard`: ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados.<br>• `strict` (estricto): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados sin la intervención del usuario (no verá una notificación antes de que se eliminen los archivos).<br>• `rigorous` (riguroso): ecls.exe elimina los archivos sin intentar desinfectarlos, sea cual sea el archivo.<br>• `delete` (eliminar): ecls.exe elimina los archivos sin intentar desinfectarlos, pero no elimina archivos delicados como los archivos del sistema de Windows. |
| /quarantine | copiar archivos infectados (si se han desinfectado) a la carpeta Cuarentena (complementa la acción realizada durante la desinfección) |
| /no-quarantine | no copiar archivos infectados a cuarentena |

## Opciones generales

| | |
|---|---|
| /help | mostrar ayuda y salir |
| /version | mostrar información sobre la versión y salir |
| /preserve-time | conservar hora del último acceso |

## Códigos de salida

| | |
|---|---|
| 0 | no se ha detectado ninguna amenaza |
| 1 | amenaza detectada y eliminada |
| 10 | no se han podido analizar todos los archivos (podrían ser amenazas) |
| 50 | amenaza detectada |
| 100 | error |

Los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por lo tanto, puede estar infectado.

# Preguntas frecuentes

A continuación puede encontrar algunas de las preguntas y los problemas encontrados más frecuentes. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

- Cómo actualizar ESET Small Business Security
- ESET Small Business Security ha detectado una amenaza

- Cómo eliminar malware de mi PC
- Cómo permitir la comunicación para una aplicación determinada
- Cómo crear una tarea nueva en Tareas programadas
- Cómo programar una tarea de análisis (semanal)
- Cómo desbloquear la Configuración avanzada
- Cómo resolver la desactivación del producto desde ESET HOME

Si su problema no aparece en la lista anterior, pruebe a buscar en la Ayuda en línea de ESET Small Business Security.

Si no encuentra la solución a su problema o consulta en la Ayuda en línea de ESET Small Business Security, puede visitar la base de conocimiento en línea de ESET, que se actualiza periódicamente. A continuación se incluyen vínculos a los artículos más populares de la base de conocimiento:

- ¿Cómo renuevo mi suscripción?
- He recibido un error de activación al instalar mi producto ESET. ¿Qué significa?
- Activar mi producto para oficina pequeña de ESET para Windows con la clave de activación
- Desinstalar o reinstalar mi producto doméstico ESET
- He recibido el mensaje de que mi instalación de ESET ha finalizado prematuramente
- ¿Qué debo hacer después de renovar mi suscripción? (usuarios domésticos)
- ¿Qué sucede si cambio mi dirección de correo electrónico?
- Transferir mi producto ESET a un nuevo ordenador o dispositivo
- Cómo iniciar Windows en Modo seguro o en Modo seguro con funciones de red
- Evitar el bloqueo de un sitio web seguro
- Permitir el acceso de software de lectores de pantalla a la GUI de ESET

Si lo necesita, puede ponerse en contacto con el servicio de soporte técnico para hacerle llegar sus preguntas o sus problemas.

# Cómo actualizar ESET Small Business Security

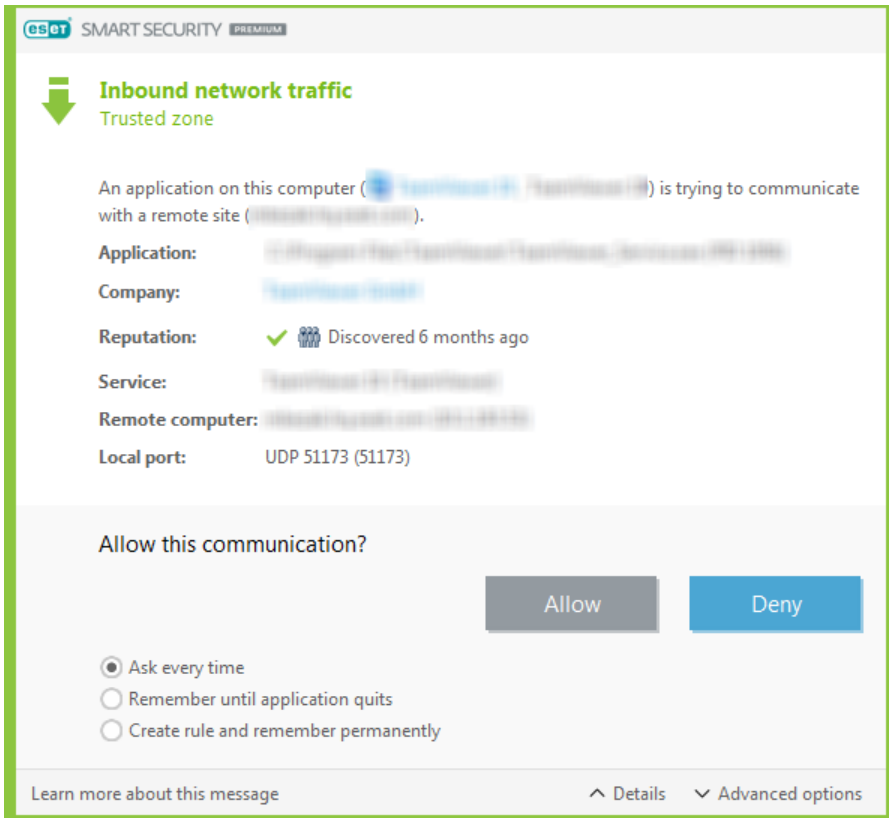
ESET Small Business Security Se puede actualizar de forma manual o automática. Para activar la actualización, haga clic en **Actualización** en la ventana principal del programa y, a continuación, haga clic en **Buscar actualizaciones**.

La configuración de instalación predeterminada crea una tarea de actualización automática que se lleva a cabo cada hora. Si es necesario cambiar el intervalo, vaya a **Herramientas** > Planificador de tareas.

0

# Cómo permitir la comunicación para una aplicación determinada

Si se detecta una nueva conexión en el modo interactivo y no hay ninguna regla que coincida, se le solicitará que **confirme** o **rechace** la conexión. Si desea que ESET Small Business Security lleve a cabo la misma acción cada vez que la aplicación intente establecer una conexión, active la casilla de verificación **Crear regla y recordar permanentemen**.




En la configuración del cortafuegos puede crear reglas del cortafuegos para aplicaciones antes de que ESET Small Business Security las detecte. Abra la ventana principal del programa > **Configuración** > **Protección de la red** > haga clic en junto a **Cortafuegos** > **Configurar** > **Avanzado** > **Reglas** > **Editar**.

Haga clic en el botón **Agregar** y, en la pestaña **General**, escriba el nombre, la dirección y el protocolo de comunicación de la regla. Esta ventana le permite definir la acción que se debe realizar cuando se aplica la regla.

Inserte la ruta al archivo ejecutable de la aplicación y al puerto de comunicación local en la pestaña **Local**. Haga clic en la pestaña **Remoto** para introducir la dirección y el puerto remotos (si corresponde). La regla que se acaba de crear se aplicará en cuanto la aplicación intente comunicarse de nuevo.

# Cómo crear una tarea nueva en el Planificador de

# tareas

Para crear una tarea nueva en **Herramientas** > **Planificador de tareas**, haga clic en **Agregar tarea** o haga clic con el botón derecho y seleccione **Agregar** en el menú contextual. Están disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

La **actualización** es una de las tareas programadas más frecuentes, por lo que a continuación explicaremos cómo se agrega una nueva tarea de actualización:

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Introduzca el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Están disponibles las opciones siguientes: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**.

Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las opciones siguientes:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución (horas)**)

En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. Aquí puede definir los perfiles principal y alternativo. El perfil alternativo se utiliza cuando la tarea no se puede completar con el perfil principal. Haga clic en **Finalizar** para confirmar la operación; la nueva tarea se agregará a la lista de tareas programadas actualmente.

# Cómo programar un análisis del ordenador semanal

Para programar una tarea periódica, abra la ventana principal del programa y haga clic en **Herramientas** > **Tareas programadas**. A continuación, se proporcionan las instrucciones básicas para programar una tarea que analice las unidades locales cada semana. Consulte el artículo de nuestra Base de conocimiento para ver instrucciones más detalladas.

Para programar una tarea:

1. Haga clic en **Agregar** en la pantalla principal del Planificador de tareas.

2. Escriba un nombre para la tarea y seleccione **Análisis del ordenador a petición** en el menú desplegable **Tipo de tarea**.

3. Seleccione **Semanalmente** como frecuencia de la tarea.

4. Establezca el día y la hora de ejecución de la tarea.

5. Seleccione **Ejecutar la tarea lo antes posible** para realizar la tarea más tarde si no se ejecuta a la hora programada por cualquier motivo (por ejemplo, si el ordenador estaba apagado).

6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.

7. En el menú desplegable **Objetos**, seleccione **Discos locales**.

8. Haga clic en **Finalizar** para aplicar la tarea.

# Cómo desbloquear la Configuración avanzada protegida por contraseña

Cuando desee acceder a la Configuración avanzada protegida, se mostrará la ventana de introducción de contraseña. Si olvida o pierde la contraseña, haga clic en **Restaurar contraseña** y escriba la dirección de correo electrónico que usó para registrar la suscripción. ESET le enviará un correo electrónico con el código de verificación. Escriba el código de verificación y, a continuación, escriba y confirme la nueva contraseña. El código de verificación tiene una validez de siete días.

**Restaurar la contraseña a través de su cuenta deESET HOME**: utilice esta opción si la suscripción utilizada para la activación está asociada a su cuenta de ESET HOME. Escriba la dirección de correo electrónico que utilice para iniciar sesión en su cuenta de ESET HOME.

Si no recuerda su dirección de correo electrónico o tiene problemas para restaurar la contraseña, haga clic en **Contactar con el soporte técnico**. Se le redirigirá al sitio web de ESET para que pueda ponerse en contacto con el departamento de soporte técnico.

**Generar código para soporte técnico**: esta opción genera un código para el soporte técnico. Copie el código proporcionado por el soporte técnico y haga clic en **Tengo un código de verificación**. Escriba el código de verificación y, a continuación, escriba y confirme la nueva contraseña. El código de verificación tiene una validez de siete días.

Para obtener más información, consulte Desbloquear su contraseña de configuración en productos para oficina pequeña de ESET para Windows.

# Cómo resolver la desactivación del producto desde ESET HOME

## El producto no está activado

Este mensaje de error aparece cuando el propietario de la suscripción desactiva su ESET Small Business Security desde el portal ESET HOME o la suscripción compartida con su cuenta de ESET HOME ya no está compartida. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Small Business Security.
- Póngase en contacto con el propietario de la suscripción para informarle de que su ESET Small Business Security ha sido desactivado por el propietario de la suscripción o que la suscripción ya no está compartida con usted. El propietario puede resolver el problema en ESET HOME.

## Producto desactivado, dispositivo desconectado

Este mensaje de error aparece después de quitar un dispositivo de la cuenta de ESET HOME. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Small Business Security.
- Póngase en contacto con el propietario de la suscripción si tiene información de que se ha desactivado ESET Small Business Security y de que el dispositivo se ha desconectado de ESET HOME.
- Si es el propietario de la suscripción y no tiene conocimiento de estos cambios, consulte la fuente de actividad de la cuenta de ESET HOME. Si encuentra alguna actividad sospechosa, cambie la contraseña de su cuenta de ESET HOME y póngase en contacto con el servicio de soporte técnico de ESET.

# Producto desactivado, dispositivo desconectado

Este mensaje de error aparece después de quitar un dispositivo de la cuenta de ESET HOME. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Small Business Security.
- Póngase en contacto con el propietario de la suscripción si tiene información de que se ha desactivado ESET Small Business Security y de que el dispositivo se ha desconectado de ESET HOME.
- Si es el propietario de la suscripción y no tiene conocimiento de estos cambios, consulte la fuente de actividad de la cuenta de ESET HOME. Si encuentra alguna actividad sospechosa, cambie la contraseña de su cuenta de ESET HOME y póngase en contacto con el servicio de soporte técnico de ESET.

# El producto no está activado

Este mensaje de error aparece cuando el propietario de la suscripción desactiva su ESET Small Business Security desde el portal ESET HOME o la suscripción compartida con su cuenta de ESET HOME ya no está compartida. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Small Business Security.
- Póngase en contacto con el propietario de la suscripción para informarle de que su ESET Small Business Security ha sido desactivado por el propietario de la suscripción o que la suscripción ya no está compartida con usted. El propietario puede resolver el problema en ESET HOME.

# Desinstalación

Para desinstalar ESET Small Business Security, siga estos pasos:

Windows 10

1. En el menú Inicio, haga clic en **Configuración** > **Aplicaciones** > **Aplicaciones y características**.
2. Busque **ESET** en la lista que se muestra, o escríbalo en el campo de búsqueda y haga clic en **Modificar**.
3. Si desea desinstalar el producto, haga clic en **Desinstalar**.

Windows 11

1. En el menú Inicio, haga clic en **Todas las aplicaciones**.
2. Busque **ESET** en la lista que se muestra, o escríbalo en el campo de búsqueda y haga clic en **Modificar**.
3. Mantenga pulsado ESET Security (o haga clic con el botón derecho) y seleccione **Desinstalar** o **Desinstalar/Cambiar**.

El Asistente de instalación le permite exportar la configuración del producto antes de quitar la instalación.

Para obtener más información sobre cómo desinstalar su producto ESET, consulte el artículo Desinstalar manualmente su producto ESET con la herramienta de desinstalación de ESET.

# Programa de mejora de la experiencia de los clientes

Al unirse al Programa de mejora de la experiencia del cliente, facilita a ESET información anónima relativa al uso de sus productos. Puede obtener más información sobre el tratamiento de datos en nuestra Política de privacidad.

## Su consentimiento

La participación en este programa es voluntaria y solo se realiza con su consentimiento. Tras unirse, la participación es pasiva, lo que significa que no tiene que hacer nada más. Puede modificar la configuración del producto en cualquier momento para revocar su consentimiento. Al hacerlo, nos impedirá continuar con el tratamiento de sus datos anónimos.

Puede modificar la configuración del producto en cualquier momento para revocar su consentimiento.

- Cambio de la configuración del Programa de mejora de la experiencia del cliente en productos domésticos

para Windows de ESET

## ¿Qué tipos de información recopilamos?

### Datos sobre interacciones con el producto

Esta información nos da más datos sobre cómo se utilizan nuestros productos. Gracias a ella podemos saber, por ejemplo, qué funcionalidades se usan con frecuencia, qué ajustes modifican los usuarios o cuánto tiempo pasan utilizando el producto.

### Datos sobre dispositivos

Recopilamos esta información para comprender dónde y en qué dispositivos se usan nuestros productos. Ejemplos típicos son el modelo de dispositivo, el país, la versión y el nombre del sistema operativo.

### Datos de diagnósticos de error

También se recopila información sobre errores y bloqueos, como, por ejemplo, qué error se ha producido y qué acciones lo han provocado.

## ¿Por qué recopilamos esta información?

Esta información anónima nos permite mejorar nuestros productos para usuarios como usted. Nos ayuda a conseguir que sean lo más pertinentes, sencillos de usar y perfectos posible.

## ¿Quién controla esta información?

ESET, spol. s r.o. es el único responsable del tratamiento de los datos recopilados en el marco del programa. Esta información no se comparte con terceros.

# Acuerdo de licencia para el usuario final

Fecha de entrada en vigor: 19 de octubre de 2021.

**IMPORTANTE:** Lea los términos y condiciones de la aplicación del producto que se detallan a continuación antes de descargarlo, instalarlo, copiarlo o utilizarlo. **LA DESCARGA, LA INSTALACIÓN, LA COPIA O LA UTILIZACIÓN DEL SOFTWARE IMPLICAN SU ACEPTACIÓN DE ESTOS TÉRMINOS Y CONDICIONES Y DE LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El

proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto…" durante la instalación, la descarga, la copia o la utilización del Software, expresa su aceptación de los términos y condiciones de este Acuerdo y acepta la Política de Privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de Privacidad, haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE SU UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE ACEPTA SU SUJECIÓN A LOS TÉRMINOS Y CONDICIONES.

1. **Software**. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo ("Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. **Instalación, Ordenador y una Clave de licencia**. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (“un AUC”) cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por

ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíqueselo inmediatamente al Proveedor.

c) **Home Edition o Business Edition.** La versión Home Edition del Software se utilizará exclusivamente en entornos privados o no comerciales para uso doméstico y familiar. Debe obtener una versión Business Edition del Software para poder utilizarlo en entornos comerciales y en servidores de correo, relays de correo, puertas de enlace de correo o puertas de enlace a Internet.

d) **Vigencia de la licencia.** Tiene derecho a utilizar el Software durante un período de tiempo limitado.

e) **Software OEM.** El Software clasificado como "OEM" solo se puede utilizar en el equipo con el que lo haya obtenido. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR.** El Software cuya venta esté prohibida o de prueba no se puede pagar, y únicamente se debe utilizar para demostraciones o para probar las características del Software.

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la Licencia, Usted debe eliminar, destruir o devolver (a sus expensas) el Software y todas las copias de seguridad del mismo a ESET o a la tienda donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El Proveedor podrá publicar actualizaciones del Software ("Actualizaciones") cuando lo estime oportuno, aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para proporcionar Actualizaciones, es necesario verificar la autenticidad de la licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La Política de final de la vida útil ("Política de final de la vida útil"), disponible en https://go.eset.com/eol_home, puede regir la forma de proporcionar las Actualizaciones. No se proporcionarán Actualizaciones después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil.

b) **Envío de amenazas e información al proveedor**. El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet ("amenazas") y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el Ordenador o la plataforma en la que el Software está instalado e información sobre las operaciones y las funciones del Software ("Información"). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario

final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las Amenazas junto con los metadatos asociados.

La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La función del sistema de reputación LiveGrid incluye la recopilación y el envío al proveedor de algoritmos hash unidireccionales relacionados con las amenazas. Esta función se activa en la sección de configuración estándar del software.

ii. La función del Sistema de Respuesta LiveGrid incluye la recopilación y el envío al Proveedor de las Amenazas con los metadatos y la Información asociados. Esta función la puede activar el Usuario final durante el proceso de instalación del Software.

El Proveedor solo podrá utilizar la Información y las Amenazas recibidas con fines de análisis e investigación de las Amenazas y mejora de la verificación de la autenticidad del Software y de la Licencia, y deberá tomar las medidas pertinentes para garantizar la seguridad de las Amenazas y la Información recibidas. Si se activa esta función del Software, el Proveedor podrá recopilar y procesar las Amenazas y la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. Estas funciones se pueden desactivar en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

Tras la terminación de este Acuerdo, el Proveedor y sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, estarán autorizados a transferir, procesar y almacenar sus datos identificativos fundamentales para fines relacionados con la facturación, la ejecución del Acuerdo y la transmisión de notificaciones en su Ordenador.

**En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos como persona interesada. También puede visitarla desde la sección de ayuda del Software.**

5. **Ejercicio de los derechos de usuario final**. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los Ordenadores o los sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes ni crear versiones derivadas del software. El uso del software está sujeto a las siguientes restricciones:

a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.

c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.

d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.

e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.

f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.

g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. **Copyright**. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

8. **Reserva de derechos**. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. **Versiones en varios idiomas, software en soporte dual, varias copias**. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. **Comienzo y rescisión del Acuerdo.** Este acuerdo es efectivo a partir de la fecha en que acepte sus términos. Puede terminar este acuerdo en cualquier momento mediante la desinstalación, destrucción o devolución (a sus expensas) del software, todas las copias de seguridad y todo el material relacionado que le hayan suministrado el proveedor o sus socios comerciales. Su derecho a usar el Software y sus funciones puede estar sujeto a la Política de final de la vida útil. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil, dejará de tener derecho a utilizar el Software. Independientemente del modo de terminación de este acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán en vigor de forma ilimitada.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE

SUMINISTRA "TAL CUAL", SIN GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y DENTRO DEL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, SUS PROVEEDORES DE LICENCIAS O SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, EXPRESA O IMPLÍCITA; EN PARTICULAR, NINGUNA GARANTÍA DE VENTAS O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJA UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE SATISFAGAN SUS REQUISITOS O QUE EL SOFTWARE FUNCIONE SIN INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN DEL SOFTWARE PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LA INSTALACIÓN, EL USO Y LOS RESULTADOS OBTENIDOS.

12. **Ninguna obligación adicional**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS, CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Ninguna de las disposiciones de este acuerdo se establece en perjuicio de los derechos estatutarios de una parte que actúe como consumidor en contra de lo aquí dispuesto.

15. **Soporte técnico**. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin ningún tipo de garantía o declaración. No se proporcionará soporte técnico después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil. El usuario final debe realizar una copia de seguridad de todos los datos, aplicaciones de software y programas almacenados en el ordenador antes de recibir soporte técnico. ESET y/o los terceros contratados por ESET no se hacen responsables de los daños, las pérdidas de datos, elementos en propiedad, software o hardware ni las pérdidas de ingresos a causa de la prestación del servicio de soporte técnico. ESET y/o los terceros contratados por ESET se reservan el derecho de determinar que la solución de un problema no entra dentro del ámbito de soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

16. **Transferencia de la licencia**. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal

como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a utilizar el Software de las siguientes maneras: (i) mediante un certificado de licencia emitido por el Proveedor o un tercero designado por el Proveedor; (ii) mediante un acuerdo de licencia por escrito, si se ha celebrado dicho acuerdo; (iii) mediante el envío de un mensaje de correo electrónico enviado por el Proveedor con la información de la licencia (nombre de usuario y contraseña). Pueden ser necesarios los datos de Licencia y de identificación del Usuario final de acuerdo con la Política de Privacidad para verificar la autenticidad del Software.

18. **Licencia para organismos públicos y gubernamentales de EE.UU.**. El software se proporcionará a los organismos públicos, incluido el gobierno de Estados Unidos, con los derechos y las restricciones de licencia descritos en este acuerdo.

19. **Cumplimiento de las normas de control comercial**.

a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo ("Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen.

(los actos jurídicos a los que se hace referencia en los puntos i e ii. anteriores se denominan, conjuntamente, "Leyes de control comercial").

b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es probable que incumpla lo dispuesto en el Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud del Acuerdo podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

c) Ninguna disposición del Acuerdo tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe interpretarse en ese sentido.

20. **Avisos**. Los avisos y las devoluciones del Software y la Documentación deben enviarse a ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle los cambios que se produzcan en este Acuerdo, en las Políticas de privacidad, en la Política de final de la vida útil y en la Documentación de conformidad con el art. 22 del Acuerdo. ESET puede enviarle correos electrónicos y notificaciones en la aplicación a través del Software o publicar la comunicación en su sitio web. Acepta recibir comunicaciones legales de ESET en formato electrónico, lo que incluye cualquier comunicación sobre cambios en los Términos, los Términos especiales o las Políticas de privacidad, cualquier propuesta o aceptación de contrato o invitación para negociar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. **Legislación aplicable**. Este acuerdo se regirá e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. **Disposiciones generales**. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

ESET se reserva el derecho a realizar cambios en el Software y a modificar los términos de este Acuerdo, sus Anexos, la Política de Privacidad, la Política de final de la vida útil y la Documentación, o de cualquier parte de lo anterior, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar los cambios del Software o en la forma en la que ESET desarrolla su actividad, (ii) por motivos legales, de legislación o de seguridad, o (iii) para evitar un uso inadecuado o perjuicios. Se le notificará cualquier modificación del Acuerdo por correo electrónico, mediante una notificación en la aplicación o a través de otros medios electrónicos. Si no está de acuerdo con los cambios propuestos para el Acuerdo, puede rescindirlo de acuerdo con el art. 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios propuestos se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

**ANEXO AL ACUERDO**

**Evaluación de seguridad de los dispositivos conectados a la red.** A la evaluación de seguridad de los dispositivos conectados a la red se le aplican las siguientes disposiciones adicionales:

El Software incluye una función destinada a comprobar la seguridad de la red local del Usuario final y la seguridad de los dispositivos de la red local. Esta función necesita el nombre de la red local e información sobre los dispositivos de la red local, como presencia, tipo, nombre, dirección IP y dirección MAC del dispositivo en la red local en conexión con la información de la licencia. La información también incluye el tipo de seguridad inalámbrica y el tipo de cifrado inalámbrico de los routers. Esta función también puede proporcionar información sobre la disponibilidad de una solución de software de seguridad destinada a proteger los dispositivos de la red local.

**Protección contra el mal uso de los datos.** A la protección contra el mal uso de los datos se le aplican las siguientes disposiciones adicionales:

El Software incluye una función que impide la pérdida o el uso indebido de datos esenciales en conexión directa con el robo de un Ordenador. Esta función está desactivada en la configuración predeterminada del Software. Se debe crear la Cuenta de ESET HOME para poder activarla; la función activa la recopilación de datos a través de esa cuenta en caso de producirse un robo del ordenador. Si activa esta función del Software, se recopilarán datos sobre el Ordenador robado y se enviarán al Proveedor; podrán incluirse datos sobre la ubicación de red del Ordenador, datos sobre el contenido mostrado en la pantalla del Ordenador, datos sobre la configuración del Ordenador o datos grabados por una cámara conectada al Ordenador (en adelante denominados "Datos"). El Usuario final solo tendrá derecho a utilizar los Datos obtenidos por esta función y facilitados a través de la Cuenta de ESET HOME para rectificar una situación adversa causada por el robo de un Ordenador. Únicamente a los efectos de esta función, el Proveedor procesa los Datos como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. El Proveedor permitirá al Usuario final acceder a los Datos durante el periodo necesario para alcanzar el fin con el que se obtuvieron los datos, que no debe superar el periodo de retención especificado en la Política de Privacidad. La protección contra el uso indebido de datos solo se utilizará con Ordenadores y cuentas a los que el Usuario final tenga acceso legítimo. Cualquier uso ilegal se denunciará ante la autoridad competente. El Proveedor cumplirá las leyes pertinentes y colaborará con las autoridades encargadas del cumplimiento de las leyes en caso de uso indebido. Reconoce y acepta que es responsable de salvaguardar la contraseña para acceder a la Cuenta de ESET HOME y que no debe revelar su contraseña a terceros. El Usuario final es responsable de cualquier actividad que se realice utilizando la función de protección contra el uso indebido de datos y la Cuenta de ESET HOME, esté autorizada o no dicha actividad. Si su Cuenta de ESET HOME se ve expuesta, notifíqueselo inmediatamente al Proveedor. Las disposiciones adicionales sobre la protección contra el uso indebido de datos solo serán aplicables a usuarios finales de ESET Internet Security y ESET Smart Security Premium.

**ESET Secure Data.** A ESET Secure Data se le aplican las siguientes disposiciones adicionales:

1. Definiciones. En estas disposiciones adicionales a ESET Secure Data, las siguientes palabras tienen los significados correspondientes:

a) "Información" información o datos cifrados o descifrados utilizando el software;

b) "Productos"ESET Secure Datael software y la documentación;

c) "ESET Secure Data" el software que se utiliza para el cifrado y descifrado de datos electrónicos;

Todas las referencias en plural incluirán el singular y todas las referencias al género masculino incluirán los géneros femenino y neutro, y viceversa. Las palabras sin definición específica se utilizarán de acuerdo con las definiciones estipuladas por el Acuerdo.

2. Declaración adicional del Usuario final. Acuerda y acepta que:

a) usted asume la responsabilidad de proteger, mantener y realizar copias de seguridad de la información;

b) debe realizar una copia de seguridad completa de toda la información y datos (incluidos, sin limitación, cualquier información y datos críticos) presentes en su equipo antes de la instalación del ESET Secure Data;

c) Debe mantener un registro seguro de las contraseñas o demás información utilizada para configurar y utilizar ESET Secure Data; también debe hacer copias de seguridad de todas las claves de cifrado, códigos de licencias, archivos de claves y demás datos generados para separar los soportes de almacenamiento;

d) Es responsable del uso de los Productos. El Proveedor no será responsable de pérdidas, reclamaciones o daños que se deriven de cualquier cifrado o descifrado no autorizados o incorrectos de Información u otros datos, independientemente del lugar y medio de almacenamiento de esa Información o esos otros datos;

e) Aunque el Proveedor ha adoptado todas las medidas razonables para garantizar la integridad y seguridad de ESET Secure Data, los Productos (o cualquiera de ellos) no se deben emplear en ninguna zona que dependa de un nivel de seguridad a prueba de fallos o que presente riesgos o peligros potenciales, incluidas, entre otras, instalaciones nucleares, navegación aérea, sistemas de control o comunicación, sistemas de armamento y defensa y sistemas de soporte vital o de monitorización de signos vitales;

f) Es responsabilidad del Usuario final asegurar que el nivel de seguridad y cifrado que los productos proporcionan sea adecuado para sus requisitos;

g) Usted asume la responsabilidad de Su uso de los Productos o cualquiera de ellos, lo que incluye, entre otras responsabilidades, garantizar que dicho uso cumpla todas las leyes y normativas aplicables en Eslovaquia o en los países, las regiones o los estados en los que se utilicen los Productos. Debe asegurarse de que, antes de realizar cualquier uso de los Productos, no se contravenga ningún embargo gubernamental (en Eslovaquia o en otro lugar);

h) ESET Secure Data puede ponerse en contacto con los servidores del Proveedor periódicamente en busca de datos de licencia, parches, paquetes de servicio y otras actualizaciones que puedan mejorar, mantener, modificar o mejorar el funcionamiento de ESET Secure Data y puede enviar información general sobre el sistema relativa a su funcionamiento de acuerdo con la Política de Privacidad.

i) El Proveedor no será responsable frente a pérdidas, daños, gastos o reclamaciones que se deriven de pérdida, robo, mal uso, corrupción, daño o destrucción de contraseñas, información de configuración, claves de cifrado, códigos de activación de licencia y otros datos generados o almacenados durante el uso del software.

Las disposiciones adicionales a ESET Secure Data solo serán aplicables a los usuarios finales de ESET Smart Security Premium.

**Password Manager Software.** Al software Password Manager se le aplican las siguientes disposiciones adicionales:

1. Declaración adicional del Usuario final. Reconoce y acepta que no podrá:

a) utilizar el software Password Manager para operar con aplicaciones importantes que puedan entrañar riesgos para la vida humana o la propiedad. Es consciente de que el objetivo del software Password Manager no es ser utilizado para esos fines, y de que un fallo en estos casos podría causar la muerte, lesiones personales o graves daños a la propiedad o ambientales, de los que el Proveedor no será responsable.

EL SOFTWARE PASSWORD MANAGER NO ESTÁ DISEÑADO, PREVISTO NI LICENCIADO PARA SER UTILIZADO EN ENTORNOS PELIGROSOS EN LOS QUE SEAN NECESARIOS CONTROLES A PRUEBA DE FALLOS, ENTRE LOS QUE SE INCLUYEN, SIN LIMITACIÓN, EL DISEÑO, CONSTRUCCIÓN, MANTENIMIENTO O FUNCIONAMIENTO DE INSTALACIONES NUCLEARES, SISTEMAS DE NAVEGACIÓN AÉREA O COMUNICACIÓN, CONTROL DEL TRÁFICO AÉREO Y SISTEMAS DE SOPORTE VITAL O ARMAMENTO. EL PROVEEDOR NIEGA ESPECÍFICAMENTE CUALQUIER TIPO DE GARANTÍA EXPLÍCITA O IMPLÍCITA DE IDONEIDAD PARA DICHAS FINALIDADES.

b) utilizar el Software Password Manager de forma que incumpla este acuerdo o las leyes de Eslovaquia o su jurisdicción. En concreto, no podrá utilizar el software Password Manager para realizar o promover actividades ilegales, entre las que se incluye cargar datos de contenido dañino o contenido que pueda ser utilizado para actividades ilegales o que, de algún modo, infrinja la ley o conculque los derechos de un tercero (incluidos los derechos de propiedad intelectual), lo que incluye, entre otras actividades, intentar acceder a cuentas de Almacenamiento (a efectos de estos términos adicionales al software Password Manager, "Almacenamiento" hace referencia al espacio de almacenamiento de datos administrado por el Proveedor o por un tercero que no sea ni el Proveedor ni el usuario para permitir la sincronización y la copia de seguridad de los datos del usuario) o a cuentas y datos de otros usuarios del software Password Manager o del Almacenamiento. Si infringe cualquiera

de estas disposiciones, el Proveedor tendrá derecho a rescindir inmediatamente este acuerdo y repercutirle el coste de las soluciones necesarias, así como a dar los pasos oportunos para impedirle continuar utilizando el Software Password Manager, sin posibilidad de reembolso.

2. LIMITACIÓN DE RESPONSABILIDAD. EL SOFTWARE PASSWORD MANAGER SE PROPORCIONA “TAL CUAL”. NO SE OFRECE NINGUNA GARANTÍA EXPLÍCITA O IMPLÍCITA. USTED ASUME TODOS LOS RIESGOS DERIVADOS DE UTILIZAR EL SOFTWARE. EL PRODUCTOR NO ES RESPONSABLE DE PÉRDIDAS DE DATOS, DAÑOS NI LIMITACIÓN DE LA DISPONIBILIDAD DEL SERVICIO, LO QUE INCLUYE LOS DATOS ENVIADOS POR EL SOFTWARE PASSWORD MANAGER A UN ALMACENAMIENTO EXTERNO A LOS EFECTOS DE SINCRONIZACIÓN Y COPIA DE SEGURIDAD DE DICHOS DATOS. QUE USTED CIFRE LOS DATOS UTILIZANDO EL SOFTWARE PASSWORD MANAGER NO IMPLICA RESPONSABILIDAD ALGUNA DEL PROVEEDOR SOBRE LA SEGURIDAD DE DICHOS DATOS. USTED ACEPTA EXPRESAMENTE QUE LOS DATOS ADQUIRIDOS, UTILIZADOS, CIFRADOS, ALMACENADOS, SINCRONIZADOS O ENVIADOS A TRAVÉS DEL SOFTWARE PASSWORD MANAGER TAMBIÉN PUEDEN ALMACENARSE EN SERVIDORES DE TERCEROS (SE APLICA ÚNICAMENTE CUANDO SE UTILICE EL SOFTWARE PASSWORD MANAGER CON LOS SERVICIOS DE SINCRONIZACIÓN Y COPIA DE SEGURIDAD ACTIVADOS). SI EL PROVEEDOR, SEGÚN SU PROPIO CRITERIO, DECIDE UTILIZAR ALMACENAMIENTO, SITIOS WEB, PORTALES WEB, SERVIDORES O SERVICIOS DE TERCEROS, EL PROVEEDOR NO SERÁ RESPONSABLE DE LA CALIDAD, SEGURIDAD O DISPONIBILIDAD DE DICHOS SERVICIOS DE TERCEROS, Y EN NINGÚN CASO SERÁ EL PROVEEDOR RESPONSABLE ANTE USTED POR INCUMPLIMIENTOS DE OBLIGACIONES CONTRACTUALES O LEGALES DE DICHOS TERCEROS NI POR DAÑOS, LUCRO CESANTE, DAÑOS FINANCIEROS O NO FINANCIEROS O CUALQUIER OTRO TIPO DE PÉRDIDA QUE SE PRODUZCAN DURANTE EL USO DE ESTE SOFTWARE. EL PROVEEDOR NO SERÁ RESPONSABLE DEL CONTENIDO DE LOS DATOS ADQUIRIDOS, UTILIZADOS, CIFRADOS, ALMACENADOS, SINCRONIZADOS O ENVIADOS A TRAVÉS DEL SOFTWARE PASSWORD MANAGER O QUE SE ENCUENTREN EN EL ALMACENAMIENTO. USTED RECONOCE QUE EL PROVEEDOR NI TIENE ACCESO AL CONTENIDO DE LOS DATOS ALMACENADOS NI PUEDE CONTROLARLO NI RETIRAR CONTENIDO LEGALMENTE DAÑINO.

El Proveedor es el propietario de todos los derechos sobre mejoras, actualizaciones y revisiones relacionadas con el software Password MANAGER (“Mejoras”), aun en el caso de que dichas mejoras se hubieran creado a partir de datos, ideas o sugerencias enviados por usted de alguna forma. No tendrá derecho a compensación alguna en relación con dichas mejoras, lo que incluye los derechos de autor.

NI LAS ENTIDADES NI LOS PROVEEDORES DE LICENCIAS DEL PROVEEDOR SERÁN RESPONSABLES ANTE USTED POR NINGÚN TIPO DE DEMANDAS Y RESPONSABILIDADES DERIVADAS (O RELACIONADAS DE CUALQUIER FORMA CON ELLO) DEL USO DEL SOFTWARE PASSWORD MANAGER REALIZADO POR USTED O POR TERCEROS, DEL USO O NO USO DE AGENCIAS DE CORREDORES O CORREDORES DE VALORES O DE LA VENTA O COMPRA DE VALORES, INDEPENDIENTEMENTE DE LA TEORÍA LEGAL O DE EQUIDAD EN LA QUE SE BASEN DICHAS DEMANDAS Y RESPONSABILIDADES.

NI LAS ENTIDADES NI LOS PROVEEDORES DE LICENCIAS DEL PROVEEDOR SERÁN RESPONSABLES ANTE USTED POR NINGÚN TIPO DE DAÑOS DIRECTOS, ACCIDENTALES, ESPECIALES, INDIRECTOS O SUCESIVOS DERIVADOS (O RELACIONADOS CON ELLO) DE SOFTWARE DE TERCEROS, DE DATOS A LOS QUE SE HAYA ACCEDIDO A TRAVÉS DEL SOFTWARE PASSWORD MANAGER, DE SU USO DEL SOFTWARE PASSWORD MANAGER O SU INCAPACIDAD DE USARLO O ACCEDER AL MISMO O DE DATOS FACILITADOS A TRAVÉS DEL SOFTWARE PASSWORD MANAGER, INDEPENDIENTEMENTE DE LA TEORÍA LEGAL O DE EQUIDAD EN LA QUE SE BASEN LAS DEMANDAS POR DICHOS DAÑOS. ENTRE LOS DAÑOS EXCLUIDOS POR ESTA CLÁUSULA SE INCLUYEN, SIN LIMITACIÓN, LOS RELATIVOS A PÉRDIDA DE BENEFICIOS EMPRESARIALES, DAÑOS PERSONALES O MATERIALES, INTERRUPCIÓN DEL NEGOCIO O PÉRDIDA DE INFORMACIÓN COMERCIAL O PERSONAL. ALGUNAS JURISDICCIONES NO PERMITEN LIMITAR LOS DAÑOS ACCIDENTALES O SUCESIVOS, DE MODO QUE ES POSIBLE QUE NO SE LE APLIQUE ESTA RESTRICCIÓN. EN ESE CASO, LA RESPONSABILIDAD DEL PROVEEDOR SERÁ LA MÍNIMA QUE PERMITA LA LEGISLACIÓN APLICABLE.

LA INFORMACIÓN FACILITADA A TRAVÉS DEL SOFTWARE PASSWORD MANAGER, LO QUE INCLUYE COTIZACIONES DE BOLSA, ANÁLISIS, INFORMACIÓN SOBRE EL MERCADO, NOTICIAS Y DATOS FINANCIEROS, PUEDE ESTAR

RETRASADA, SER IMPRECISA O CONTENER ERRORES U OMISIONES, Y NI LAS ENTIDADES NI LOS PROVEEDORES DE LICENCIAS DEL PROVEEDOR TENDRÁN RESPONSABILIDAD ALGUNA AL RESPECTO. EL PROVEEDOR PUEDE CAMBIAR O CANCELAR CUALQUIER ASPECTO O CARACTERÍSTICA DEL SOFTWARE PASSWORD MANAGER O EL USO DE TODAS LAS CARACTERÍSTICAS O TECNOLOGÍAS DEL SOFTWARE PASSWORD MANAGER (O DE ALGUNA DE ELLAS) EN CUALQUIER MOMENTO SIN NOTIFICÁRSELO PREVIAMENTE.

SI LAS DISPOSICIONES DE ESTE ARTÍCULO FUESEN NULAS POR CUALQUIER MOTIVO O EL PROVEEDOR SE CONSIDERASE RESPONSABLE DE PÉRDIDAS, DAÑOS, ETC. EN VIRTUD DE LA LEGISLACIÓN APLICABLE, LAS PARTES ACUERDAN QUE LA RESPONSABILIDAD DEL PROVEEDOR ANTE USTED SE LIMITARÁ A LA CANTIDAD TOTAL DE LAS TASAS DE LICENCIA PAGADAS POR USTED.

USTED SE COMPROMETE A INDEMNIZAR, DEFENDER Y EXIMIR DE TODA RESPONSABILIDAD AL PROVEEDOR Y A SUS EMPLEADOS, SUBSIDIARIAS, AFILIADOS, SOCIOS DE REPOSICIONAMIENTO DE MARCA Y DEMÁS SOCIOS ANTE TODO TIPO DE DEMANDAS, RESPONSABILIDADES, DAÑOS, PÉRDIDAS, COSTES, GASTOS Y TASAS DE TERCEROS (INCLUIDOS PROPIETARIOS DE DISPOSITIVOS O PARTES CUYOS DERECHOS SE HAYAN VISTO AFECTADOS POR LOS DATOS UTILIZADOS EN EL SOFTWARE PASSWORD MANAGER O EN EL ALMACENAMIENTO), EN LOS QUE DICHOS TERCEROS HAYAN INCURRIDO A CONSECUENCIA DEL USO REALIZADO POR USTED DEL SOFTWARE PASSWORD MANAGER.

3. Datos del software Password Manager. A menos que usted seleccione explícitamente lo contrario, todos los datos que introduzca y se guarden en una base de datos del software Password Manager se almacenarán en formato cifrado en su ordenador o en el dispositivo de almacenamiento que usted indique. Es consciente de que, en caso de que se eliminen o dañen cualquier base de datos del software Password Manager u otros archivos, todos los datos contenidos en los mismos se perderán de forma irreversible, y comprende y acepta el riesgo de dicha pérdida. El hecho de que sus datos personales se almacenen en formato cifrado en el ordenador no significa que una persona que obtenga la contraseña maestra o acceda al dispositivo de activación definido por el cliente para abrir la base de datos no pueda robar o utilizar mal la información. Usted es responsable de mantener la seguridad de todos los métodos de acceso.

4. Transmisión de datos personales al Proveedor o al Almacenamiento. Si selecciona esta opción, y exclusivamente para garantizar la exactitud de la sincronización y la copia de seguridad de los datos, el software Password Manager transmite o envía datos personales desde la base de datos del software Password Manager (sobre todo contraseñas, información de inicio de sesión, cuentas e identidades) al Almacenamiento a través de Internet. Los datos solo se transmiten de forma cifrada. El uso del software Password Manager para rellenar formularios en línea con contraseñas, datos de inicio de sesión u otros datos puede requerir que la información se envíe a través de Internet al sitio web identificado por usted. Esta transmisión de datos no la inicia el software Password Manager y, por ello, el Proveedor no puede considerarse responsable de la seguridad de dichas interacciones con sitios web de distintos proveedores. Usted asume todos los riesgos derivados de las transacciones que decida realizar en Internet, junto con el software Password Manager o no, y será el único responsable de las pérdidas de datos o los daños que puedan producir en su sistema informático la descarga o el uso de esos materiales o servicios. Para minimizar el riesgo de perder datos valiosos, el Proveedor recomienda que los clientes realicen copias de seguridad periódicas de la base de datos y de otros archivos importantes en unidades externas. El Proveedor no podrá ayudarle a recuperar los datos perdidos o dañados. Si el Proveedor ofrece servicios de copia de seguridad de los archivos de base de datos del usuario en caso de daño o eliminación de los archivos del PC del usuario, dichos servicios de copia de seguridad no suponen garantía alguna, ni implican responsabilidad alguna del Proveedor ante usted.

Mediante el uso del Software Password Manager, acepta que el software puede ponerse en contacto con los servidores del Proveedor periódicamente en busca de datos de licencia, parches, paquetes de servicio y otras actualizaciones que puedan mejorar, mantener o modificar el funcionamiento del Software Password Manager. El software puede enviar información general sobre el sistema relativa al funcionamiento del Software Password Manager de acuerdo con la Política de Privacidad.

5. Instrucciones e información de desinstalación. La información de la base de datos que desee conservar debe exportarse antes de desinstalar el software Password Manager.

Las disposiciones adicionales al software Password Manager solo serán aplicables a los usuarios finales de ESET Smart Security Premium.

**ESET LiveGuard**. A ESET LiveGuard se le aplican las siguientes disposiciones adicionales:

El Software incluye una función de análisis adicional de los archivos enviados por el Usuario final. El Proveedor solo puede usar los archivos enviados por el Usuario final y los resultados del análisis de acuerdo con la Política de Privacidad y de acuerdo con las normativas aplicables.

Las disposiciones adicionales a ESET LiveGuard solo serán aplicables a los usuarios finales de ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

# Política de privacidad

La protección de los datos personales es muy importante para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, n.º de registro de la empresa: 31333532 como Responsable del tratamiento ("ESET"). Cumplimos con el requisito de transparencia que se estipula en el Reglamento general de protección de datos de la UE ("RGPD"). Para lograr este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes ("Usuario final" o "Usted") sobre los siguientes temas de protección de datos personales:

- Fundamento jurídico del tratamiento de datos personales
- Intercambio y confidencialidad de datos
- Seguridad de datos
- Sus derechos como interesado
- Tratamiento de sus datos personales
- Información de contacto.

## Fundamento jurídico del tratamiento de datos personales

Solo hay varias disposiciones jurídicas para el tratamiento de datos que usamos de acuerdo con el marco jurídico aplicable a la protección de los datos personales. El tratamiento de los datos personales en ESET es necesario para la ejecución del Acuerdo de licencia para el usuario final ("EULA") con el Usuario final (artículo 6 1] b] del RGPD), que se aplica a la prestación de servicios o productos de ESET a menos que se indique explícitamente lo contrario, por ejemplo:

- El fundamento jurídico de interés legítimo (artículo 6 1] b] del RGPD), que nos permite tratar los datos sobre el uso que los clientes hacen de nuestros Servicios y su satisfacción para ofrecer a los usuarios los mejores niveles de protección, asistencia y experiencia que sea posible. Incluso el marketing es reconocido por la legislación aplicable como un interés legítimo, por lo que nos basamos en ese concepto para las comunicaciones de marketing con nuestros clientes.

- El consentimiento (artículo 6 1] b] del RGPD), que podemos solicitarle en situaciones concretas en las que consideramos que este fundamento jurídico es el más adecuado o si la ley lo requiere.

- El cumplimiento de una obligación legal (artículo 6 1] b] del RGPD), por ejemplo, estipulando los requisitos de comunicación electrónica o retención de facturas o documentos de facturación.

## Intercambio y confidencialidad de datos

No compartimos sus datos con terceros. Sin embargo, ESET es una empresa que opera en todo el mundo a través de empresas o socios que forman parte de su red de ventas, servicio y asistencia. La información de licencias, facturación y asistencia técnica tratada por ESET puede transferirse entre filiales o socios para cumplir el EULA en aspectos como la prestación de servicios o la asistencia.

ESET prefiere procesar sus datos en la Unión Europea (UE). No obstante, en función de su ubicación (uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transferir sus datos a un país fuera de la UE. Por ejemplo, utilizamos servicios de terceros para prestar servicios de informática en la nube. En estos casos, seleccionamos cuidadosamente a los proveedores de servicios y ofrecemos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por lo general, aceptamos las cláusulas contractuales tipo de la UE con la normativa contractual aplicable si es necesario.

En algunos países de fuera de la UE, como el Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos comparable. Gracias al nivel de protección de datos, la transferencia de datos a estos países no requiere ninguna autorización o acuerdo especial.

## Seguridad de datos

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar la confidencialidad, la integridad, la disponibilidad y la resistencia de los sistemas y los servicios de procesamiento. En caso de filtración de datos que pongan en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora correspondiente y a los usuarios finales en calidad de interesados.

## Derechos del titular de los datos.

Los derechos de los usuarios finales son importantes para nosotros, sean de un país de la UE o de fuera de la UE. Por lo tanto, en ESET les garantizamos los derechos siguientes. Para ejercer los derechos de los interesados, puede ponerse en contacto con nosotros a través del formulario de asistencia o por correo electrónico en la dirección dpo@eset.sk. Le pediremos la información siguiente con fines de identificación: Nombre, dirección de correo electrónico y, si procede, clave de licencia o número de cliente y empresa. No nos envíe otros datos personales, como la fecha de nacimiento. Cabe destacar que trataremos sus datos personales con fines de identificación y procesamiento de solicitudes.

**Derecho a retirar el consentimiento.** El derecho a retirar el consentimiento solo se aplica si se tratan los datos con su consentimiento previo. Si nos da su consentimiento para tratar sus datos personales, podrá retirarlo en cualquier momento sin explicar los motivos. La retirada del consentimiento solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite.

**Derecho de objeción.** El derecho a oponerse al tratamiento se aplica si el tratamiento se basa en el interés legítimo de ESET o terceros. Si tratamos sus datos personales para proteger un interés legítimo, puede oponerse a dicho interés legítimo y al tratamiento de sus datos personales en cualquier momento. La oposición solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite. Si

tratamos sus datos personales con fines de marketing directo, no es necesario explicar los motivos por los que se opone. Esto también se aplica a la creación de perfiles, ya que está relacionada con el marketing directo. En el resto de casos, debe enviarnos las quejas que tenga en relación con el interés legítimo de ESET para tratar sus datos personales.

En algunos casos, a pesar de su consentimiento, podemos seguir tratando sus datos personales sobre la base de otro fundamento jurídico (como la ejecución de un contrato).

**Derecho de acceso.** Como interesado, puede solicitar información sobre los datos personales que ESET almacena en cualquier momento sin coste alguno.

**Derecho de rectificación.** Si tratamos datos personales incorrectos de manera involuntaria, puede pedir que se corrija esta información.

**Derecho a eliminar y restringir el tratamiento de datos personales.** Como interesado, puede solicitar la eliminación o restricción del tratamiento de sus datos personales. Por ejemplo, si tratamos datos personales con su consentimiento y lo retira sin otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. Sus datos personales también se eliminarán cuando dejen de ser necesarios para los fines indicados al finalizar el periodo de retención.

Si solo utilizamos sus datos personales con fines de marketing directo y revoca su consentimiento o se opone al interés legítimo de ESET, restringiremos el tratamiento una vez que incluyamos sus datos de contacto en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales se eliminarán.

Puede que estemos obligados a almacenar sus datos hasta que expiren las obligaciones de retención y los periodos emitidos por el organismo de legislación o las autoridades supervisoras. También pueden surgir periodos u obligaciones de retención porque la legislación eslovaca así lo exija. En ese caso, los datos correspondientes se eliminarán de forma rutinaria a partir de ese momento.

**Derecho a la portabilidad de datos.** Dado que es un interesado, le proporcionamos los datos personales que trata ESET en formato XLS.

**Derecho a presentar una queja.** Como interesado, puede presentar una reclamación ante una autoridad supervisora en cualquier momento. ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. La autoridad supervisora que gestiona cuestiones de datos es la Oficina de protección de datos personales de Eslovaquia, situada en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

## Tratamiento de sus datos personales

Los servicios de ESET que se hayan implementado en nuestros productos se prestan en virtud de las condiciones de EULA, pero algunos pueden requerir atención especial. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos distintos servicios descritos en el EULA y la documentación del documentación. Para que todo funcione, debemos recopilar la siguiente información:

**Datos de licencias y facturación.** ESET recopila y trata el nombre, la dirección de correo electrónico, la clave de licencia y, si procede, la dirección, la afiliación y los pagos de la empresa para facilitar la activación de la licencia, la entrega de la clave de licencia, los recordatorios de caducidad, las solicitudes de asistencia, la verificación de autenticidad de la licencia, la prestación de nuestros servicios y otras notificaciones (como mensajes de marketing) en virtud de la legislación aplicable o su consentimiento. Aunque ESET debe retener la información de facturación durante un periodo de 10 años, la información de la licencia se anonimizará en un plazo máximo de

12 meses una vez que la licencia caduque.

**Actualizaciones y otras estadísticas.** Los datos tratados abarcan información relativa al proceso de instalación y a su ordenador, incluidas la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos (como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto). Todo ello se trata en el marco de los servicios de actualización con fines de mantenimiento, seguridad y mejora de la infraestructura de backend.

Estos datos se retienen junto con la información de identificación necesaria para las licencias y la facturación, ya que no es necesario identificar al Usuario final. El periodo de retención asciende a cuatro años.

Sistema de Reputación **ESET LiveGrid®.** Trata algoritmos hash unidireccionales relativos a infiltraciones para ejecutar el Sistema de Reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones antimalware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube. Durante este proceso no se identifica al Usuario final.

Sistema de Respuesta **ESET LiveGrid®.** Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe

- Infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;

- Información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;

- Archivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

La información obtenida y tratada con el Sistema de Respuesta ESET LiveGrid® se debe utilizar sin identificar al Usuario final.

**Evaluación de seguridad de los dispositivos conectados a la red.** Para ofrecer la función de evaluación de seguridad tratamos el nombre de la red local y la información sobre los dispositivos de dicha red (como presencia, tipo, nombre, dirección IP y dirección MAC del dispositivo en la red local) en relación con la información de la licencia. La información también incluye el tipo de seguridad inalámbrica y el tipo de cifrado inalámbrico de los routers. La información de licencia que identifique al Usuario final se anonimizará en un plazo máximo de 12 meses una vez que la licencia caduque.

**Soporte técnico.** La información de contacto o licencia y los datos contenidos en sus solicitudes de asistencia pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Podemos pedirle que nos facilite otra información para facilitar el servicio de asistencia. Los datos tratados para ofrecer asistencia técnica se almacenan durante cuatro años.

**Protección contra el mal uso de los datos.** Si se crea la Cuenta de ESET HOME en https://home.eset.com y el

Usuario final activa la función en relación con el robo del ordenador, se recopilarán y tratarán la información de ubicación, las capturas de pantalla, los datos sobre la configuración del ordenador y las imágenes grabadas por la cámara del ordenador. Los datos recopilados se almacenan en nuestros servidores o en los servidores de nuestros proveedores de servicios durante un periodo de tres meses.

**Password Manager.** Si activa la función de Password Manager, los datos de inicio de sesión se almacenarán de forma cifrada en su ordenador o el dispositivo designado. Si activa el servicio de sincronización, los datos cifrados se almacenan en nuestros servidores o en los servidores de nuestros proveedores de servicios para garantizar dicho servicio. Ni ESET ni el proveedor de servicios tienen acceso a los datos cifrados. Solo usted tiene la clave para descifrar los datos. Los datos se eliminarán una vez que la función se desactive.

**ESET LiveGuard**. Si activa la función ESET LiveGuard, debe enviar muestras, por ejemplo, archivos predefinidos y seleccionados por el Usuario final. Las muestras que elija para el análisis remoto se cargarán en el servicio de ESET, y el resultado del análisis se enviará de nuevo a su ordenador. Las muestras sospechosas se tratarán según la información recopilada por el Sistema de Respuesta ESET LiveGrid®.

**Programa de mejora de la experiencia de los clientes.** Si opta por activar Programa de mejora de la experiencia de los clientes , se recopilará y utilizará la información de telemetría anónima relativa al uso de Nuestros productos sobre la base de Su consentimiento.

Si la persona que utiliza nuestros productos o servicios no es el Usuario final que ha adquirido el producto o servicio ni ejecutado el EULA con ESET (como un empleado o familiar del Usuario final o una persona autorizada por este para utilizar el producto o servicio en virtud del EULA, el tratamiento de los datos se llevará a cabo según el interés legítimo de ESET conforme al artículo 6 1) f) del RGPD. De este modo, la persona autorizada por el Usuario final podrá utilizar nuestros productos y servicios en virtud del EULA.

## Información de contacto

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk