ESET Security Ultimate

Guía para el usuario

Haga clic aquí para mostrar la versión de ayuda de este documento

Digital Security
Progress. Protected.

ESET Security Ultimate ha sido desarrollado por ESET, spol. s r.o.

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

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

REV. 12/04/2024

ESET Security Ultimate

ESET Security Ultimate representa un nuevo enfoque para la seguridad del equipo plenamente integrada. La versión más reciente del motor de exploración ESET LiveGrid®, en combinación con nuestros módulos personalizados de firewall y antispam, utilizan velocidad y precisión para mantener el equipo seguro. El resultado es un sistema inteligente constantemente en alerta frente a los ataques y el software malicioso que podrían amenazar su equipo.

ESET Security Ultimate es una completa solución de seguridad que combina la máxima protección con el mínimo impacto en el sistema. Nuestras tecnologías avanzadas usan la inteligencia artificial para prevenir infiltraciones de virus, spyware, troyanos, gusanos, adware, rootkits y otras amenazas sin entorpecer el rendimiento del sistema ni perturbar el equipo.

Características y beneficios

Interfaz del usuario rediseñada	La interfaz del usuario en esta versión se ha rediseñado y simplificado considerablemente con base en los resultados de las pruebas de usabilidad. Todas las etiquetas y notificaciones de la interfaz gráfica del usuario se han revisado cuidadosamente. Ahora, la interfaz es compatible con idiomas de derecha a izquierda, como hebreo y árabe. La ayuda en línea se encuentra integrada en ESET Security Ultimate y ofrece contenido de soporte actualizado en forma dinámica.
Modo oscuro	Una extensión que le ayuda a cambiar rápidamente la pantalla a un tema oscuro. Puede elegir su esquema de colores preferido en Elementos de la interfaz de usuario.
Antivirus y antispyware	Detecta en forma proactiva y desinfecta más cantidad de amenazas conocidas y desconocidas, tales como virus, gusanos, troyanos y rootkits. La Heurística avanzada identifica hasta al malware nunca antes visto. Lo protege de amenazas desconocidas, a las que neutraliza antes de que lleguen a causar daño. La protección de acceso a la web y la protección anti-phishing controlan la comunicación entre los navegadores y los servidores remotos (incluido SSL). La Protección del cliente de correo electrónico proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S).
Actualizaciones de rutina	La actualización frecuente del motor de detección (anteriormente conocido como “base de datos de firmas de virus”) y de los módulos de programa es el mejor método para asegurar el máximo nivel de seguridad en su equipo.
ESET LiveGrid® (Reputación basada en la nube)	Usted podrá verificar la reputación de los procesos en ejecución y de los archivos directamente desde ESET Security Ultimate.
Control de dispositivos	Explora automáticamente todas las unidades flash USB, las tarjetas de memoria, los CD y los DVD. Bloquea los medios extraíbles en función del tipo de medio, el fabricante, el tamaño y otros atributos.
Funcionalidad del HIPS	Puede personalizar el comportamiento del sistema a un nivel superior: especificar reglas para el registro del sistema, activar procesos y programas, y ajustar su posición de seguridad.
Modo de juego	Pospone todas las ventanas emergentes, actualizaciones y demás actividades que consumen recursos del sistema a fin de conservarlos para los juegos y otras actividades de pantalla completa.

Características en ESET Security Ultimate

Banca y navegación seguras	La Banca y navegación seguras provee un navegador seguro para utilizar al acceder a la banca en línea o puertas de enlace de pago en línea para asegurarse de que todas las transacciones en línea se realizan en un ambiente confiable y seguro.
Soporte para firmas de red	Las firmas de red permiten una identificación rápida y bloquea el tráfico malicioso de entrada y salida de dispositivos de usuarios como robots y paquete de exploits. Esta característica puede considerarse como una mejora a la Protección de botnet.
Firewall inteligente	Evita que los usuarios no autorizados accedan a su equipo y saquen provecho de sus datos personales.
Antispam del cliente de correo electrónico	El spam representa hasta 50% de todas las comunicaciones por correo electrónico. El antispam del cliente de correo electrónico protege contra este problema.
Anti-Theft	Anti-Theft amplía la seguridad de nivel de usuario ante el robo o pérdida de un equipo. Cuando instale ESET Security Ultimate y Anti-Theft, su dispositivo aparecerá en la interfaz web. La interfaz web le permite administrar la configuración de Anti-Theft y las características de Anti-Theft de su dispositivo.
Control parental	Protege a su familia del contenido Web potencialmente ofensivo mediante el bloqueo de varias categorías de sitios Web.
Password Manager	Password Manager protege y almacena sus contraseñas y datos personales.
Secure Data	Secure Data le permite cifrar datos en su equipo y unidades extraíbles para evitar el uso indebido de información privada y confidencial.
ESET LiveGuard	Detecta y detiene amenazas nunca vistas y procesa información para detectar futuras amenazas.
VPN	Mantenga sus datos seguros, evite el seguimiento no deseado y mejore su privacidad con la seguridad adicional de una dirección IP anónima.
ESET Identity Protection	Protege su información personal, crediticia y financiera. ESET Identity Protection detecta la venta ilegal de su información personal proporcionando un monitoreo continuo.

Una suscripción debe estar activa para que las características de ESET Security Ultimate estén operativas. Le recomendamos que renueve su suscripción varias semanas antes de que la suscripción para ESET Security Ultimate venza.

Novedades

Novedades de la versión 17.1 de ESET Security Ultimate

- Pequeñas mejoras en el Inspector de red
- Pequeñas mejoras en banca y navegación seguras
- ESET LiveGuard: el envío de los documentos ahora está habilitado de forma predeterminada
- Otras correcciones de errores menores y mejoras

Para deshabilitar **las notificaciones de novedades**:
1. Abra Configuración avanzada > **Notificaciones** > **Notificaciones en el escritorio**.
2. Haga clic en **Editar** junto a **Notificaciones de escritorio**.
3. Anule la selección de la casilla de verificación **Mostrar notificaciones de novedades** y haga clic en **Aceptar**.

Para obtener más información sobre las notificaciones, consulte la sección Notificaciones.

Para obtener una lista detallada de los cambios en ESET Security Ultimate, consulte ESET Security Ultimate registro de cambios.

¿Qué producto tengo?

ESET ofrece capas múltiples de seguridad con productos nuevos, desde una solución de antivirus rápida y potente hasta una solución de seguridad todo en un uno con mínimo impacto en el sistema:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

Para determinar qué producto 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).

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Motor de detección	✔	✔	✔	✔
Aprendizaje automático avanzado	✔	✔	✔	✔
Bloqueador de exploits	✔	✔	✔	✔
Protección contra ataque basado en script	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Protección del acceso a la Web	✔	✔	✔	✔
HIPS (incluida la Protección contra ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Inspector de red		✔	✔	✔
Protección de la cámara web		✔	✔	✔
Protección contra ataques de red		✔	✔	✔
Protección contra Botnet		✔	✔	✔
Banca y navegación seguras		✔	✔	✔
Seguridad y privacidad del navegador		✔	✔	✔
Control parental		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
VPN				✔
Identity Protection				✔

Es posible que algunos de los productos anteriores no estén disponibles en su idioma / región.

Requisitos del sistema

Su sistema debe reunir los siguientes requisitos de hardware y software para que ESET Security Ultimate funcione correctamente:

Procesadores compatibles

Intel o AMD procesador de 32 bits (x86) con conjunto de SSE2 o procesador de 64 bits (x64), 1 GHz o superior procesador basado en 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 lanzados después de julio de 2023. Más información.

Siempre intente mantener su sistema operativo actualizado.

Requisitos de características de ESET Security Ultimate

Consulte los requisitos del sistema para características específicas de ESET Security Ultimate en la tabla que aparece a continuación:

Característica	Requisitos
Intel® Threat Detection Technology	Consulte los procesadores compatibles.
Banca y navegación seguras	Consulte los navegadores web compatibles.
Fondo transparente	Versión para Windows 10 RS4 y posterior.
Limpiador especializado	Procesador que no está basado en ARM64.
Limpiador de sistema	Procesador que no está basado en ARM64.
Bloqueador de exploits	Procesador que no está basado en ARM64.
Inspección profunda del comportamiento	Procesador que no está basado en ARM64.

Otros

Se requiere conexión a Internet para que la activación y las actualizaciones de ESET Security Ultimate funcionen correctamente.

Si dos programas antivirus se ejecutan simultáneamente en un solo dispositivo, se producen conflictos inevitables entre los recursos del sistema, como la ralentización del sistema, la cual lo haría inoperable.

Versión obsoleta de Microsoft Windows

Problema

- Quiere instalar la versión más reciente de ESET Security Ultimate en un equipo con Windows 7, Windows 8 (8.1) o Windows Home Server 2011
- ESET Security Ultimate muestra un error de **Sistema operativo obsoleto** durante la instalación

Detalles

La versión más reciente de ESET Security Ultimate requiere sistemas operativos Windows 10 o Windows 11.

Solución

Están disponibles las soluciones siguientes:

Actualizar a Windows 10 o Windows 11

El proceso de actualización es relativamente fácil y, en muchos casos, puede hacerlo sin perder archivos. Antes de actualizar a Windows 10:

1. Copia de seguridad de datos importantes.
2. Lea las Preguntas frecuentes sobre la actualización a Windows 10 o las Preguntas frecuentes sobre la actualización a Windows 11 de Microsoft y actualice su sistema operativo Windows.

Instale la versión 16.0 de ESET Security Ultimate

Si no puede actualizar Windows, instale la versión 16.0 de ESET Security Ultimate. Para obtener más información, consulte la Ayuda en línea sobre la versión 16.0 de ESET Security Ultimate.

Prevención

Cuando trabaja con su equipo y, en particular, cuando navega por Internet, recuerde que ningún sistema antivirus del mundo puede eliminar completamente el riesgo de las infiltraciones y de los ataques remotos. Para ofrecer la máxima protección y conveniencia, es imprescindible utilizar su solución antivirus correctamente y atenerse a varias reglas útiles:

Actualizaciones habituales

De acuerdo con las estadísticas de ESET LiveGrid®, cada día se crean miles de infiltraciones nuevas y únicas para evadir las medidas de seguridad existentes y generar ganancias para sus creadores (a costa de otros usuarios). Los especialistas del laboratorio de investigación de ESET analizan dichas amenazas diariamente, y luego preparan y lanzan actualizaciones para mejorar en forma continua el nivel de protección de los usuarios. Para asegurar la máxima eficacia de estas actualizaciones, es importante configurarlas adecuadamente en el sistema. Para obtener más información sobre cómo configurar las actualizaciones, consulte el capítulo Configuración de la actualización.

Descargas de revisiones de seguridad

Los creadores de software malicioso suelen aprovechar diversas vulnerabilidades del sistema para incrementar la eficacia de la propagación de los códigos maliciosos. Por eso, las empresas de software controlan cuidadosamente la aparición de vulnerabilidades en sus aplicaciones y lanzan actualizaciones de seguridad que eliminan amenazas potenciales en forma habitual. Es importante descargar estas actualizaciones de seguridad apenas se emiten. Microsoft Windows y los navegadores Web como Internet Explorer son ejemplos de los programas que publican actualizaciones de seguridad de manera periódica.

Copia de seguridad de datos importantes

A los creadores de malware en general no les importan las necesidades de los usuarios, y la actividad de los programas maliciosos suele generar un funcionamiento totalmente defectuoso de un sistema operativo, así como la pérdida de datos importantes. Es imprescindible realizar copias de seguridad habituales de los datos importantes y confidenciales en una fuente externa, como un DVD o un disco externo. Este tipo de precauciones facilitan y aceleran la recuperación de datos en caso de una falla del sistema.

Exploración habitual del equipo en busca de virus

El módulo de protección del sistema de archivos en tiempo real maneja la detección de virus, gusanos, troyanos y rootkits más conocidos y desconocidos. Esto significa que, cada vez que accede a un archivo o lo abre, se lo explora para evitar actividades de malware. Se recomienda realizar una exploración completa del equipo al menos una vez por mes, ya que las firmas de malware varía y el motor de detección se actualiza todos los días.

Seguimiento de reglas de seguridad básicas

Esta es la regla más útil y más efectiva de todas: siempre hay que tener cuidado. Hoy en día, muchas infiltraciones requieren la interacción del usuario para ejecutarse y propagarse. Si el usuario es precavido al abrir nuevos archivos, ahorrará un tiempo y esfuerzo considerables, que de otra forma se emplearían en desinfectar las infiltraciones. Estas son algunas pautas útiles:

- No visitar sitios Web sospechosos con muchas ventanas emergentes y anuncios intermitentes.
- Tener cuidado al instalar programas gratuitos, paquetes de códecs, etc. Solamente usar programas seguros y visitar sitios Web de Internet seguros.
- Tener cuidado al abrir los archivos adjuntos de los correos electrónicos, en especial los mensajes de envío masivo y los mensajes de remitentes desconocidos.
- No usar una cuenta de administrador para trabajar diariamente en el equipo.

Páginas de ayuda

Bienvenido a la guía de usuario de ESET Security Ultimate. La información que se proporciona aquí sirve para presentar el producto y ayudarlo a hacer que su equipo sea más seguro.

Introducción

Antes de utilizar ESET Security Ultimate, puede leer información sobre diversos tipos de detecciones y ataques remotos que puede encontrarse al usar el equipo. También hemos recopilado una lista de nuevas características introducidas en ESET Security Ultimate.

Comience por instalar ESET Security Ultimate. Si ya tiene ESET Security Ultimate instalado, consulte Trabajar con ESET Security Ultimate.

Cómo usar las páginas de ayuda de ESET Security Ultimate

La ayuda en línea se divide en diversos capítulos y subcapítulos. Pulse **F1** en ESET Security Ultimate para ver información sobre la ventana abierta actualmente.

El programa le permite buscar en un tema de ayuda por palabra clave o buscar contenido una vez que introduce palabras o frases. La diferencia entre ambos métodos es que una palabra clave puede estar lógicamente relacionada con las páginas de ayuda que no contienen esa palabra clave específica en el texto. La búsqueda por palabras y frases buscará el contenido de todas las páginas y mostrará solo aquéllas que contengan la palabra o fase en el texto real.

A fin de garantizar la consistencia y ayudar a evitar la confusión, la terminología que se usa en esta guía se basa en la interfaz de usuario de ESET Security Ultimate. También usamos un conjunto uniforme de símbolos para resaltar temas de interés o de una importancia particular.

Una nota es una observación breve. Aunque puede omitirlas, las notas pueden proporcionar información valiosa, tales como características específicas o un enlace a un tema relacionado.

Es algo que requiere su atención y no recomendamos dejarlo de lado. Normalmente, ofrece información que no es vital, pero sí importante.

Esta información requiere precaución y atención adicional. Las advertencias se incluyen específicamente para evitar que cometa errores potencialmente perjudiciales. Lea y comprenda el texto, ya que hace referencia a una configuración del sistema muy delicada o a algún elemento que puede ser de riesgo.

Este es un ejemplo de uso o ejemplo práctico que apunta a ayudarlo a entender cómo puede utilizarse una cierta función o característica.

Convención	Significado
En negrita	Nombres de elementos de interfaces como cuadros y botones de opciones.
En cursiva	Marcadores de posición de la información que proporciona. Por ejemplo, nombre de archivo o ruta significa que escriba la ruta real o el nombre del archivo.
`Courier New`	Comandos o ejemplos de códigos.
Hipervínculo	Proporciona un acceso fácil y rápido a temas con referencias cruzadas o una ubicación web externa. Los hipervínculos están resaltados en azul y pueden estar subrayados.
%ProgramFiles%	Directorio del sistema Windows que almacena los programas instalados.

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

Instalación

Existe varios métodos para la instalación de ESET Security Ultimate en su equipo. Los métodos de instalación pueden variar dependiendo del país y los medios de distribución:

- Instalador Live: se ha descargado del sitio web o CD/DVD de ESET. El paquete de instalación es universal para todos los idiomas (elija el idioma correspondiente). El Instalador Live es un archivo pequeño; los archivos adicionales necesarios para la instalación de ESET Security Ultimate se descargan automáticamente.

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

Asegúrese de que no haya otros programas antivirus instalados en el equipo antes de instalar ESET Security Ultimate. Si hay dos o más soluciones antivirus instaladas en el mismo equipo, pueden entrar en conflicto. Es recomendable desinstalar cualquier otro programa antivirus que haya en el sistema. Consulte nuestro artículo de la base de conocimiento de ESET para obtener una lista de herramientas del desinstalador para el software antivirus común (disponible en inglés y otros idiomas más).

Instalador activo

Cuando haya descargado Live installer installation package, haga doble clic en el archivo de instalación y siga las instrucciones detalladas en la ventana 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 configuraciones protegidas con contraseña, escriba su contraseña. Puede configurar la contraseña de configuración en Configuración del acceso.

2. Seleccione su preferencia para las siguientes características, 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 continúe para activar todas las características:

- Sistema de comentarios de ESET LiveGrid®
- Aplicaciones potencialmente no deseadas
- Programa de mejora de la experiencia del cliente

Al hacer clic en **Continuar** o **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 su dispositivo a la cuenta 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 adelante.

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

5. El Asistente de instalación determina qué producto de ESET se instala según su suscripción. La versión con más funciones de seguridad siempre está preseleccionada. Haga clic en **Cambiar producto** si desea instalar una versión diferente del producto ESET. Haga clic en **Continuar** para iniciar el proceso de instalación. Podría demorar unos minutos.

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

6. Haga clic en **Finalizar** para salir de la instalación.

Solucionador de problemas de instalación.

Después de instalar y activar el producto, los módulos comienzan a descargarse. La protección está iniciándose y es posible que algunas funciones no sean completamente funcionales a menos que la descarga esté completa.

Instalación fuera de línea

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

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Descargar versión para 64 bits Descargar versión para 32 bits Descargar ARM	Descargar versión para 64 bits Descargar versión para 32 bits Descargar ARM	Descargar versión para 64 bits Descargar versión para 32 bits Descargar ARM	Descargar versión para 64 bits Descargar versión para 32 bits Descargar ARM

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

Una vez que haya iniciado el instalador sin conexión (.exe), el asistente de instalación lo guiará a través del 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 configuraciones protegidas con contraseña, escriba su contraseña. Puede configurar la contraseña de configuración en Configuración del acceso.

2. Seleccione su preferencia para las siguientes características, 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 continúe para activar todas las características:

- Sistema de comentarios de ESET LiveGrid®
- Aplicaciones potencialmente no deseadas
- Programa de mejora de la experiencia del cliente

Al hacer clic en **Continuar** o **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.** Cuando tenga conexión a Internet, puede conectar su dispositivo a su cuenta ESET HOME.

4. Haga clic en **Omitir activación**. Para que la instalación funcione en su totalidad, ESET Security Ultimate debe activarse después de la instalación. La activación del producto requiere una conexión activa a Internet.

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

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

6. Haga clic en **Finalizar** para salir de la instalación.

Solucionador de problemas de instalación.

Actualización de la suscripción

Esta ventana de notificación aparece cuando ha cambiado la suscripción usada para activar su producto ESET. Su suscripción modificada le permite activar un producto con más características de seguridad. Si no se realizó ningún cambio, ESET Security Ultimate le mostrará, una vez, una ventana de alerta llamada **Cambiar a un producto con más funciones**.

Sí (recomendado): instalará automáticamente el producto con más funciones de seguridad.

No, gracias: no se realizarán cambios y la notificación desaparecerá permanentemente.

Para cambiar el producto más tarde, consulte nuestro artículo de la base de conocimiento de ESET. Para obtener más información sobre la suscripción de ESET, consulte Preguntas frecuentes sobre suscripciones.

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Motor de detección	✔	✔	✔	✔
Aprendizaje automático avanzado	✔	✔	✔	✔
Bloqueador de exploits	✔	✔	✔	✔
Protección contra ataque basado en script	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Protección del acceso a la Web	✔	✔	✔	✔
HIPS (incluida la Protección contra ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Inspector de red		✔	✔	✔
Protección de la cámara web		✔	✔	✔
Protección contra ataques de red		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Protección contra Botnet		✔	✔	✔
Banca y navegación seguras		✔	✔	✔
Seguridad y privacidad del navegador		✔	✔	✔
Control parental		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Actualización del producto

Ha descargado un instalador predeterminado y decidió cambiar el producto que se activará o desea cambiar el producto instalado a uno con más funciones de seguridad.

Cambie el producto durante la instalación.

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Motor de detección	✔	✔	✔	✔
Aprendizaje automático avanzado	✔	✔	✔	✔
Bloqueador de exploits	✔	✔	✔	✔
Protección contra ataque basado en script	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Protección del acceso a la Web	✔	✔	✔	✔
HIPS (incluida la Protección contra ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Inspector de red		✔	✔	✔
Protección de la cámara web		✔	✔	✔
Protección contra ataques de red		✔	✔	✔
Protección contra Botnet		✔	✔	✔
Banca y navegación seguras		✔	✔	✔
Seguridad y privacidad del navegador		✔	✔	✔
Control parental		✔	✔	✔
Anti-Theft		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Restauración de la suscripción

Esta ventana de diálogo aparece cuando ha cambiado la suscripción usada para activar su producto ESET. Solo puede utilizarse su suscripción modificada con un producto ESET diferente con menos características de seguridad. El producto se ha modificado automáticamente para evitar la pérdida de protección.

Para obtener más información sobre la suscripción de ESET, consulte Preguntas frecuentes sobre suscripciones.

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Motor de detección	✔	✔	✔	✔
Aprendizaje automático avanzado	✔	✔	✔	✔
Bloqueador de exploits	✔	✔	✔	✔
Protección contra ataque basado en script	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Protección del acceso a la Web	✔	✔	✔	✔
HIPS (incluida la Protección contra ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Inspector de red		✔	✔	✔
Protección de la cámara web		✔	✔	✔
Protección contra ataques de red		✔	✔	✔
Protección contra Botnet		✔	✔	✔
Banca y navegación seguras		✔	✔	✔
Seguridad y privacidad del navegador		✔	✔	✔
Control parental		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Identity Protection				✔

Cambio del producto a una categoría inferior

El producto que tiene instalado actualmente tiene más funciones de seguridad que el que está a punto de activar. VPN, Protección de identidad, Secure Data y Password Manager no son parte de este producto. No podrá crear archivos cifrados.

La tabla a continuación detalla las funciones disponibles para cada producto específico.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Motor de detección	✔	✔	✔	✔
Aprendizaje automático avanzado	✔	✔	✔	✔
Bloqueador de exploits	✔	✔	✔	✔
Protección contra ataque basado en script	✔	✔	✔	✔
Anti-Phishing	✔	✔	✔	✔
Protección del acceso a la Web	✔	✔	✔	✔
HIPS (incluida la Protección contra ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Firewall		✔	✔	✔
Inspector de red		✔	✔	✔
Protección de la cámara web		✔	✔	✔
Protección contra ataques de red		✔	✔	✔
Protección contra Botnet		✔	✔	✔
Banca y navegación seguras		✔	✔	✔
Seguridad y privacidad del navegador		✔	✔	✔
Control parental		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Solucionador de problemas de instalación

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

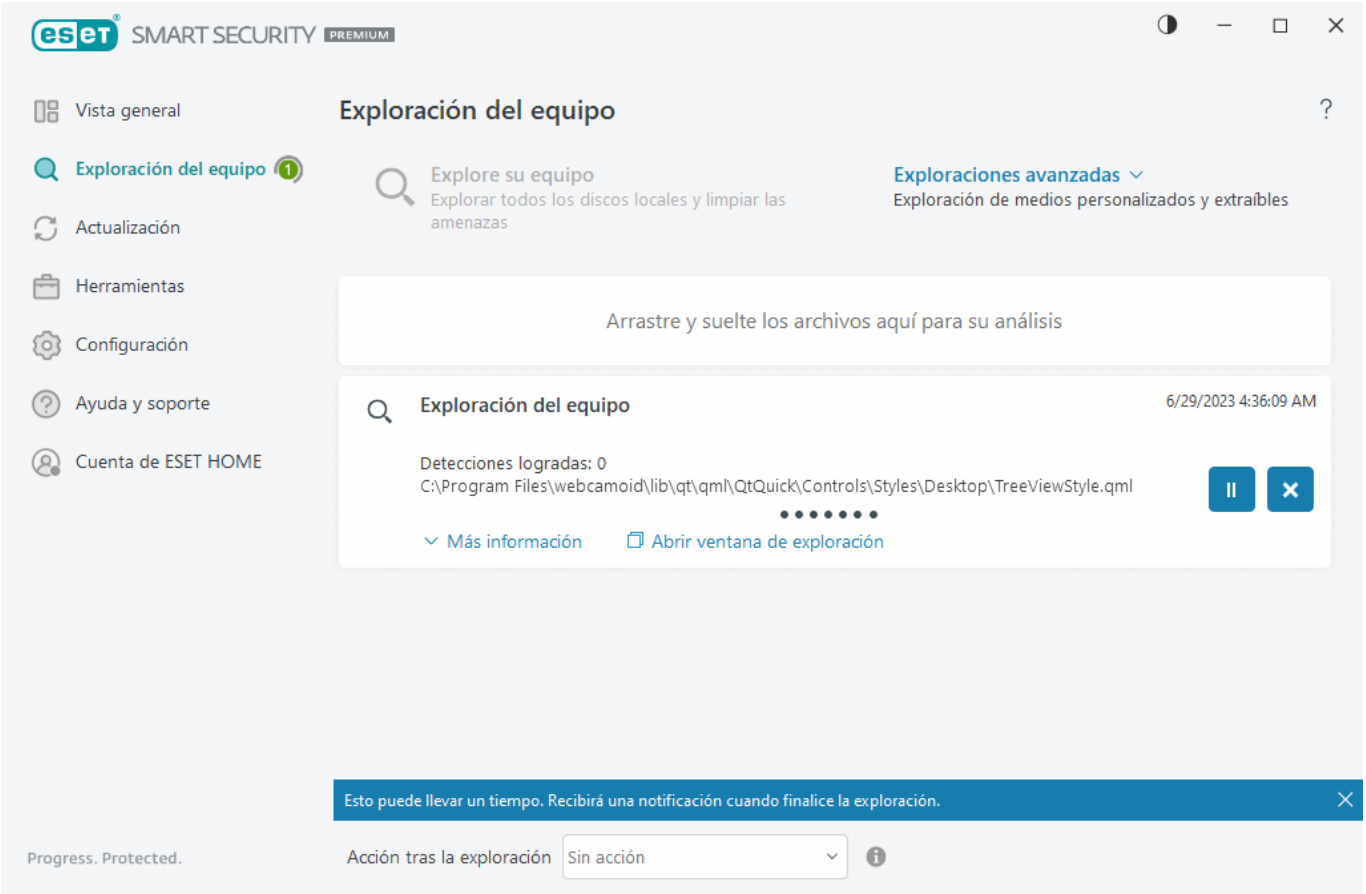
Haga clic en **Ejecutar solucionador de problemas** para iniciar el solucionador. Cuando termine, siga la solución recomendada.

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

Primera exploración después de la instalación

Luego de instalar ESET Security Ultimate, se iniciará una exploración del equipo automáticamente luego de la primera actualización exitosa para verificar códigos malintencionados.

También puede iniciar una exploración del equipo manualmente desde la ventana principal del programa > **Exploración del equipo** > **Explore el equipo**. Para obtener más información sobre las exploraciones del equipo, consulte la sección Exploración del equipo.



Reemplazo a una versión más reciente

Las versiones nuevas de ESET Security Ultimate se emiten para implementar mejoras o resolver problemas que no se pueden solucionar mediante la actualización automática de los módulos del programa. Actualizar a una versión más reciente se puede realizar de varias maneras:

1. Reemplazar automáticamente mediante una actualización del programa.
Como el reemplazo de componentes del programa por una versión posterior se distribuye a todos los usuarios y puede afectar ciertas configuraciones del sistema, se emite luego de un largo período de prueba para asegurar la funcionalidad en todas las configuraciones posibles de sistema. Si necesita actualizar el programa por una versión posterior inmediatamente después de su lanzamiento, use uno de los siguientes métodos. Asegúrese de tener habilitada la opción **Actualizaciones de características de la aplicación** en Configuración

avanzada > **Actualización** > **Perfiles** > **Actualizaciones**.

2. Manualmente, en la ventana principal del programa al hacer clic en **Buscar actualizaciones** en la sección **Actualizar**.

3. En forma manual, mediante la descarga e instalación de la versión más reciente sobre la instalación previa.

Para obtener información adicional e instrucciones ilustradas, consulte:

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

Actualización automática de versión antigua del producto

Su versión del producto ESET ya no es compatible y se ha actualizado hacia la más reciente.

Problemas comunes de instalación

> Cada nueva versión de los productos ESET presenta una gran cantidad de reparación de errores y mejoras. Los clientes existentes con una suscripción válida de un producto ESET pueden actualizar a la versión más reciente del mismo producto gratis.

Para completar la instalación:

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

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

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

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

Se instalará ESET Security Ultimate

Este cuadro de diálogo puede mostrarse:

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

La opción **Cambiar producto** le permite cambiar entre los productos hogareños de ESET Windows según su

suscripción de ESET. Consulte ¿Qué producto tengo? para obtener más información.

Cambiar a una línea diferente de productos

Según su suscripción de ESET, puede cambiar entre varios productos hogareños de ESET Windows. Consulte ¿Qué producto tengo? para obtener más información.

Registro

Registre su suscripción al completar los campos que se incluyen en el formulario de registro y haga clic en **Activar**. Los campos marcados como requeridos son obligatorios. Esta información solo se usará en cuestiones relacionadas con su suscripción de ESET.

Progreso de la activación

Espere unos segundos hasta que finalice el proceso de activación (el tiempo necesario puede variar en función de la velocidad de su conexión a Internet o su equipo).

La activación se completó correctamente.

Se completó el proceso de activación. Siga el asistente de instalación para finalizar la configuración de ESET Security Ultimate.

En unos segundos, se iniciará una actualización del módulo. Las actualizaciones periódicas de ESET Security Ultimate se iniciarán inmediatamente.

La exploración inicial comenzará automáticamente en el plazo de 20 minutos después de la actualización del módulo.

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

Guía para principiantes

Esta sección ofrece una visión general introductoria sobre ESET Security Ultimate y su configuración básica.

Ícono de la bandeja del sistema

Algunas de las opciones de configuración y funciones más importantes están disponibles al hacer clic derecho en el ícono de la bandeja del sistema .

Detener la protección: muestra el cuadro de diálogo de confirmación que deshabilita el Motor de detección, que protege ante ataques maliciosos al sistema mediante el control de los archivos, y las comunicaciones por medio de Internet y correo electrónico. En el menú desplegable **Intervalo de tiempo** puede especificar durante cuánto tiempo se deshabilitará la protección.

Pausar firewall (permitir todo tráfico) – cambia el firewall a un estado inactivo. Consulte Red para obtener más información.

Bloquear todo el tráfico de red – bloquea todo el tráfico de red. Para volver a habilitarlo, haga clic en **Detener el bloqueo de todo el tráfico de red**.

Configuración avanzada – abre la Configuración avanzada de ESET Security Ultimate. 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 sobre los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las detecciones.

Abrir ESET Security Ultimate – abre la ventanaprincipal del programa ESET Security Ultimate

Restablecer disposición de la ventana: restablece la ventana de ESET Security Ultimate a su tamaño y posición predeterminados en la pantalla.

Modo de color—abre la configuración de la interfaz de usuario, donde puede cambiar el color de la GUI.

Buscar actualizaciones – inicia un módulo o una actualización del producto para garantizar su protección. ESET Security Ultimate busca actualizaciones automáticamente varias veces al día.

Acerca de – proporciona información del sistema, detalles sobre la versión instalada de ESET Security Ultimate, los módulo del programa instalados e información sobre el sistema operativo y los recursos del sistema.

Accesos directos del teclado

Para mejorar la navegación en ESET Security Ultimate, puede utilizar los siguientes accesos directos del teclado:

Accesos directos desde teclado	Acción
F1	abre las páginas de ayuda
F5	abre la configuración avanzada
Flecha arriba/flecha abajo	navegación en elementos del menú desplegable
TAB	mover al siguiente elemento de la interfaz gráfica de usuario de una ventana
Shift+TAB	mover al elemento de la interfaz gráfica de usuario anterior en una ventana
ESC	cierra la ventana de diálogo activa
Ctrl+U	Muestra información sobre la suscripción de ESET (detalles para Soporte técnico)

Accesos directos desde teclado	Acción
Ctrl+R	restablece la ventana del producto a su tamaño y posición predeterminados en la pantalla
ALT + Flecha izquierda	volver
ALT + Flecha derecha	avanzar
ALT+Home	ir al inicio

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

Perfiles

El administrador de perfiles se usa en dos partes de ESET Security Ultimate – en la sección **Exploración bajo demanda** y en **Actualización**.

Exploración del equipo

Hay cuatro perfiles de exploración predefinidos en ESET Security Ultimate:

- **Análisis inteligente** – Es el perfil de exploración avanzada predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se encontraron limpios en una exploración anterior y que no se han modificado desde esa exploración. Esto permite tener tiempos de exploración más bajos con un impacto mínimo en la seguridad del sistema.

- **Exploración del menú contextual** – Puede iniciar la exploración del menú contextual de cualquier archivo desde el menú contextual. El perfil de exploración del menú contextual le permite definir una configuración de exploración que se utilizará cuando se ejecuta la exploración de esta manera.

- **Exploración exhaustiva** – El perfil de exploración exhaustiva no utiliza la optimización inteligente de forma predeterminada, por lo que no se excluye ningún archivo de la exploración mediante este perfil.

- **Exploración del equipo** – Es el perfil predeterminado utilizado en la exploración estándar del equipo.

Es posible guardar los parámetros preferidos de exploración para usarlos en el futuro. Se recomienda crear un perfil distinto (con varios objetos para explorar, métodos de exploración y otros parámetros) para cada exploración utilizada regularmente.

Para crear un nuevo perfil, abra Configuración avanzada > **Motor de detección** > **Exploración de malware** > **Exploración a demanda** > **Lista de perfiles** > **Editar**. La ventana **Administrador de perfiles** incluye el menú desplegable **Perfil seleccionado** que enumera los perfiles de exploración existentes así como la opción de crear uno nuevo. Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte ThreatSense, donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

> Suponga que desea crear su propio perfil de exploración y la configuración de **Explore su equipo** es parcialmente adecuada, pero no desea explorar empaquetadores en tiempo real o aplicaciones potencialmente no seguras y, además, quiere aplicar una **Reparar siempre la detección**. Ingrese el nombre de su nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione su nuevo perfil desde el menú desplegable **Perfil seleccionado** y ajuste los parámetros restantes para cumplir con sus requisitos, y haga clic en **Aceptar** para guardar su nuevo perfil.

Actualización

El editor de perfiles en la configuración de la actualización permite crear nuevos perfiles de actualización. Cree y use sus propios perfiles personalizados (distintos al perfil predeterminado: **Mi perfil**) únicamente si su equipo se conecta a los servidores de actualización de varias formas.

Un ejemplo es un equipo portátil que normalmente se conecta a un servidor local (mirror) desde la red local, pero que descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (durante un viaje de negocios) puede usar dos perfiles: el primero para conectarse al servidor local; el otro para conectarse a los servidores de ESET. Una vez configurados estos perfiles, navegue a **Herramientas** > **Tareas programadas** y edite los parámetros de las tareas de actualización. Designe un perfil como principal y el otro como secundario.

Actualizar perfil – El perfil de actualización utilizado actualmente. Para cambiarlo, elija un perfil del menú desplegable.

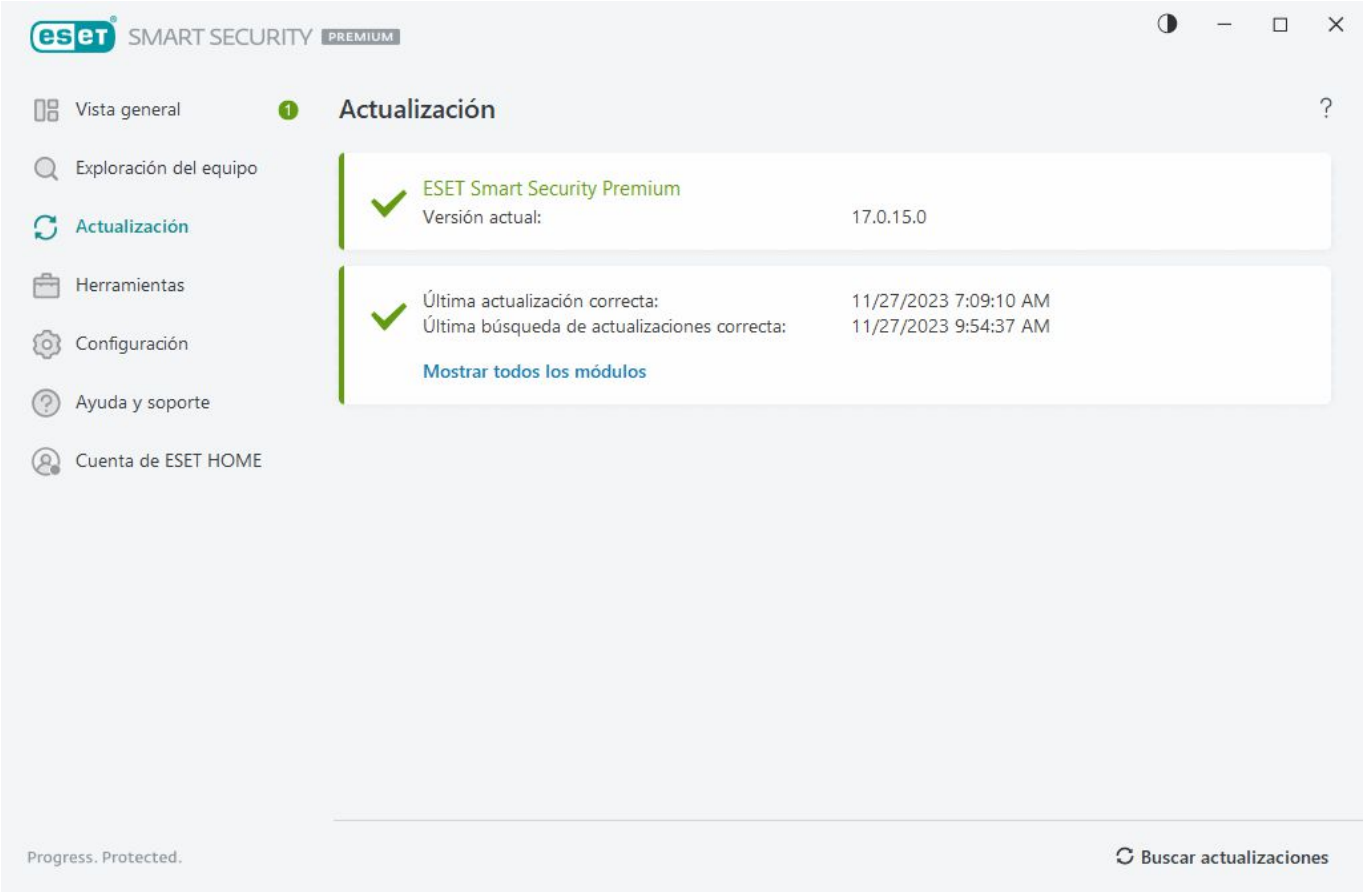
Lista de perfiles – cree perfiles nuevos o elimine perfiles de actualización existentes.

Actualizaciones

La actualización habitual de ESET Security Ultimate es la mejor forma de asegurar el máximo nivel de seguridad en el equipo. El módulo de actualización se asegura de que los módulos del programa y los componentes del sistema estén siempre actualizados.

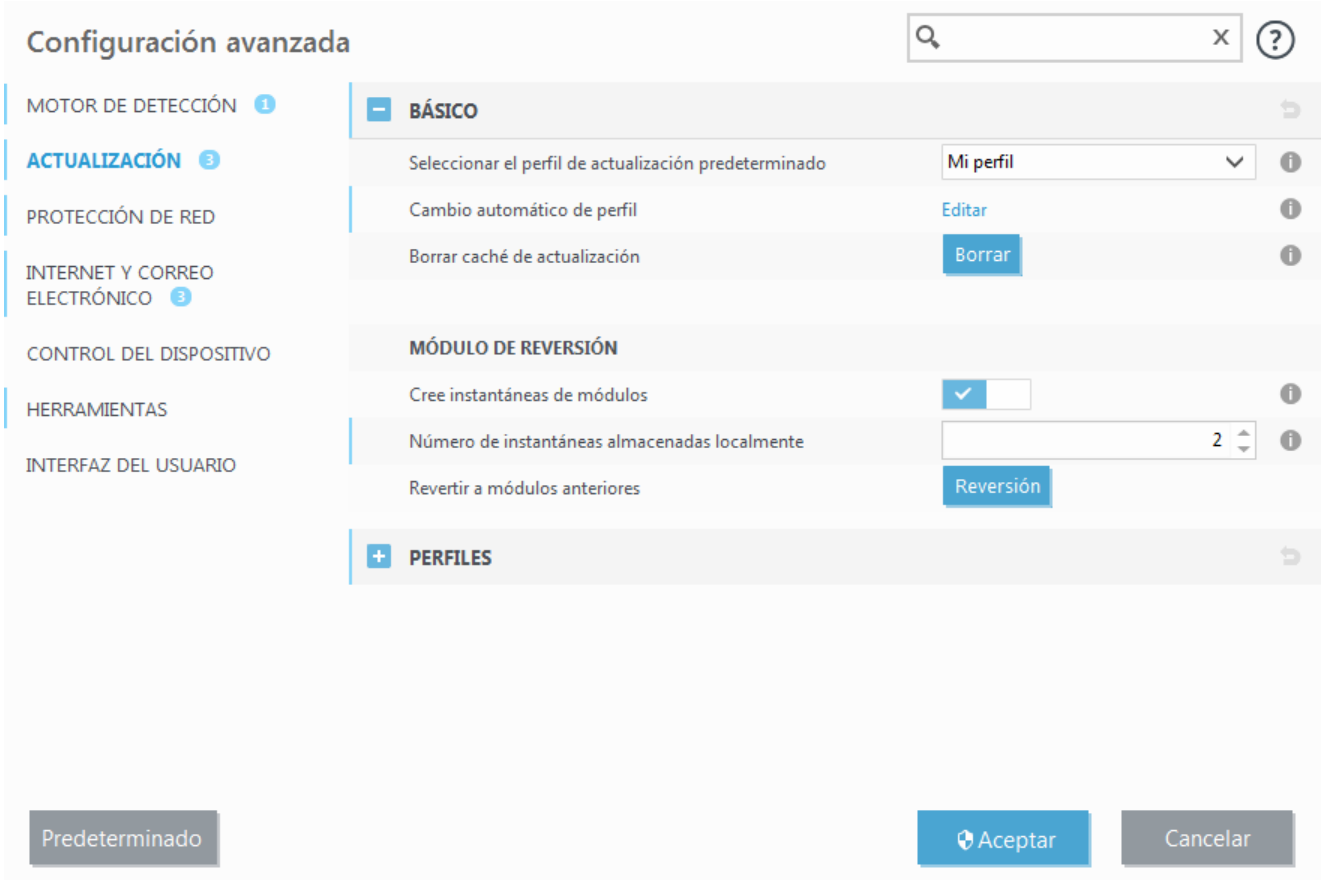
Al hacer clic en **Actualización** en la ventana principal del programa, verá el estado actual de la actualización, incluyendo la fecha y la hora de la última actualización correcta y si es necesario actualizar.

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 tiene 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 Resolución de problemas para el mensaje "Error de actualización de módulos".



Configurar la protección de red

De manera predeterminada, ESET Security Ultimate 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 red a **Preguntar**. La configuración de la protección de red se mostrará cada vez que el equipo se conecte a una nueva red.

Puede elegir entre los siguientes perfiles de conexión de red:

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

Privado: para redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de 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.

Público: para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a 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 suponer un riesgo para la seguridad de su equipo.

Habilitar Anti-Theft

Los dispositivos personales corren constantemente el riesgo de perderse o ser robados en nuestros desplazamientos diarios del hogar al trabajo o a otros lugares públicos. Anti-Theft es una característica que amplía la seguridad en el nivel de usuario en caso de pérdida o robo del dispositivo. Anti-Theft le permite supervisar el uso del dispositivo y rastrear el dispositivo perdido mediante la localización por dirección IP en ESET HOME, lo cual lo ayuda a recuperar el dispositivo y a proteger sus datos personales.

En el uso de las tecnologías modernas, como la búsqueda de dirección IP geográfica, la captura de imágenes con la cámara Web, la protección de la cuenta del usuario y la supervisión del dispositivo, Anti-Theft puede ayudar a usted y a una organización encargada del cumplimiento de la ley a ubicar su equipo o dispositivo si lo perdió o se lo robaron. En ESET HOME, puede ver la actividad que tiene lugar en el equipo o el dispositivo.

Para obtener más información sobre Anti-Theft en ESET HOME, consulte la Ayuda en línea de ESET HOME.

Es posible que Anti-Theft no funcione correctamente en los equipos de los dominios debido a restricciones en la administración de cuentas de usuario.

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

- En la ventana principal del programa > **Vista general**, haga clic en **CONFIGURAR** junto a **Anti-Theft**.
- Si aparece el mensaje "Anti-Theft está disponible" en la pantalla de **Vista general** de la ventana principal del programa, haga clic en **Activar Anti-Theft**.
- En la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad**. Habilite el interruptor **Anti-Theft** y siga las instrucciones en pantalla.

Si su dispositivo no está conectado a ESET HOME, debe hacer lo siguiente:
1. Iniciar sesión en su cuenta de ESET HOME al activar Anti-Theft.
2. Configure un nombre del dispositivo.

Anti-Theft no admite Microsoft Windows Home Server.

Tras activar Anti-Theft, puede optimizar la seguridad del dispositivo desde la ventana principal del programa en > **Configuración** > **Herramientas de seguridad** > **Anti-Theft**.

Control parental

Si ya activó el Control parental en ESET Security Ultimate, también debe configurar el Control parental para todas las cuentas de usuario relacionadas.

Cuando el control parental está activo y las cuentas de usuario no están configuradas, ESET Security Ultimate muestra la notificación "El control parental no está configurado" en la pantalla **Descripción general**. Haga clic en **Configurar reglas** y consulte la sección Control parental para obtener más información.

Activación del producto

Hay varios métodos disponibles para activar su producto. La disponibilidad de un escenario de activación particular en la ventana de activación puede variar dependiendo del país y los medios de distribución (CD/DVD, página Web de ESET, etc.):

- Si compró una versión comercial del producto en caja o recibió un mensaje de correo electrónico con detalles de la suscripción, active el producto haciendo clic en **Usar una clave de activación comprada**. Para que la activación se realice correctamente, deberá ingresar la clave de activación tal como fue suministrada. Clave de activación: una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX que se utiliza para la identificación del propietario de la suscripción y para la activación de la suscripción. Por lo general, la clave de activación aparece en el interior o al dorso del paquete del producto.

- Tras seleccionar Usar cuenta ESET HOME, se le pedirá que inicie sesión en su cuenta ESET HOME.

- Si no tiene una suscripción y desea comprar una, haga clic en **Adquirir suscripción**. Será redirigido al sitio Web de su distribuidor local de ESET. Las suscripciones a productos hogareños de ESET Windows no son gratuitas.

Podrá cambiar la suscripción de su producto en cualquier momento. Para realizar esto, haga clic en **Ayuda y soporte** > **Cambiar suscripción** en la ventana principal del programa. Verá la identificación pública que se usa para identificar su suscripción con el soporte de ESET.

¿Error en la activación del producto?

Introducción de la clave de activación durante la activación

Las actualizaciones automáticas son importantes para su seguridad. ESET Security Ultimate solo recibirá actualizaciones después de activarlas.

Al ingresar su **clave de activación**, es importante que la ingrese tal como está escrita. Su clave de activación una cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX que se usa para identificar al propietario de la suscripción y para activarla.

Le recomendamos copiar y pegar su clave de activación desde el correo electrónico de registro para asegurarse de no equivocarse.

Si no ingresó suclave de activación luego de la instalación, el producto no se activará. Puede activar ESET Security Ultimate en la ventana principal del programa > **Ayuda y soporte** > **Activar suscripción**.

Las suscripciones a productos hogareños de ESET Windows no son gratuitas.

Usar ESET HOME cuenta

Conecte su dispositivo a ESET HOME para ver y administrar todas las suscripciones y los dispositivos de ESET activados. Puede renovar, actualizar o ampliar la suscripción y ver detalles importantes de ella. En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar diferentes suscripciones, descargar productos en sus dispositivos, comprobar el estado de seguridad del producto o compartir suscripciones por correo electrónico. Para obtener más información, visite ayuda en línea de ESET HOME.

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

1. Ingrese a su cuenta ESET HOME.

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

2. Configure un **Nombre del dispositivo** para su 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 Security Ultimate.

Clave de activación gratuita de ESET

La suscripción para ESET Security Ultimate no es gratuita.

La clave de activación de ESET es una secuencia única de letras y números separados por guion que proporciona ESET para permitir el uso legal de ESET Security Ultimate de conformidad con el Acuerdo de licencia de usuario final. Todos los Usuarios finales tienen derecho a usar la clave de activación solo en la medida en que tengan derecho a usar ESET Security Ultimate según la cantidad de licencias otorgadas por ESET. La clave de activación se considera confidencial y no se puede compartir; Sin embargo, puede compartir una suscripción mediante ESET HOME.

Existen fuentes en Internet que pueden proporcionar una clave de activación de ESET "gratuita", pero recuerde:

- Hacer clic en un anuncio de "Suscripción de ESET gratuita" puede comprometer su equipo o dispositivo e infectarlo con malware. El malware puede ocultarse en contenido web no oficial (p. ej., videos), sitios web que muestran anuncios para ganar dinero en base a sus visitas, etc. En general, estos son una trampa.
- ESET puede deshabilitar y deshabilita las suscripciones pirateadas.
- Tener una clave de activación pirateada no cumple con el Acuerdo de licencia de usuario final que debe aceptar para instalar ESET Security Ultimate.
- Compre suscripciones de ESET solo a través de canales oficiales como www.eset.com, distribuidores o revendedores de ESET (no compre suscripciones en sitios web de terceros no oficiales como eBay ni suscripciones compartidas de terceros).
- La descarga de un producto ESET Security Ultimate es gratuita, pero la activación durante la instalación requiere una clave de activación de ESET válida (puede descargarlo e instalarlo, pero sin activación, no funcionará).
- No comparta su suscripción en Internet ni en las redes sociales (puede hacerse popular).

Para identificar e informar una suscripción de ESET pirata, visite nuestro artículo de la base de conocimiento para obtener instrucciones.

Si no está seguro acerca de comprar un producto de seguridad de ESET, puede usar una versión de prueba mientras lo decide:

1. Activar ESET Security Ultimate con una de prueba gratuita
2. Participar en el Programa ESET Beta
3. Instalar ESET Mobile Security si está usado un dispositivo móvil Android, es freemium.

Para obtener un descuento/extender su licencia, Renueve ESET.

Falló la activación - situaciones comunes

Si la activación de ESET Security Ultimate no se realiza correctamente, las situaciones más habituales son:

- La clave de activación ya está en uso.
- Ha introducido una clave de activación no válida.
- Falta información en el formulario de activación o no es válida.
- Error al comunicarse con el servidor de activación.
- Sin conexión con los servidores de activación de ESET o con conexión deshabilitada.

Compruebe que ha introducido la clave de activación correcta y que su conexión a Internet está activa. Intente activar ESET Security Ultimate de nuevo. Si usa una cuenta de ESET HOME para la activación, consulte Suscripción

y administración de suscripciones de ESET HOME: ayuda en línea.

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

Si sigue sin poder activarlo ESET Security Ultimate, el Solucionador de problemas de activación de ESET lo guía por las 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 su suscripción a su cuenta ESET HOME, consulte Agregar una suscripción.

> Si no tiene la cuenta ESET HOME, puede crear una nueva cuenta 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 de estado de la suscripción, abra la Configuración avanzada > **Notificaciones** > **Estados de la aplicación**. Haga clic en **Editar** junto a **Estados de la aplicación**, expanda **Licencias** y anule la selección de la casilla de verificación situada junto a la notificación que desee deshabilitar. Deshabilitar la notificación no soluciona el problema.

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

Estado de suscripción	Descripción	Solución
Activo	La suscripción es válida y no es necesario que intervenga. ESET Security Ultimate puede activarse y puede encontrar los detalles de la suscripción en la ventana principal del programa > **Ayuda y soporte**.	
Sobreusada	Más dispositivos de los permitidos están usando esta suscripción. Recibirá un error de activación.	Consulte Error de activación debido a una suscripción sobreusada para obtener más información.
Suspendida	Su suscripción se suspendió 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 la cuenta ESET HOME, en la notificación que se muestra en la ventana principal del programa, haga clic en **Administrar su suscripción en ESET HOME** y revise sus datos de pago. De lo contrario, póngase en contacto con el distribuidor de la suscripción. Error de activación—si tiene la cuenta ESET HOME, en la ventana de 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.

Estado de suscripción	Descripción	Solución
Expiró	Su suscripción venció y no puede usarla para activar ESET Security Ultimate. Puede recibir este error durante la activación o en la ventana principal del programa. Si ya tiene instalado ESET Security Ultimate, el equipo no está protegido ni actualizada.	Producto instalado—en la notificación que se muestra en la ventana principal del programa, haga clic en **Renovar suscripción** y siga las instrucciones de ¿Cómo renuevo mi suscripción?, o haga clic en **Activar producto** y elija su método de activación. Error de activación: en la ventana de error de activación, haga clic en **Renovar su suscripción** y siga las instrucciones de ¿Cómo renuevo mi suscripción?, o escriba una clave de activación nueva o renovada y haga clic en **Renovar suscripción**.
Cancelada	ESET o su distribuidor de suscripciones cancelaron su suscripción.	Si recibe un error: Canceló la suscripción en la ventana principal del programa o durante la activación y su suscripción debería funcionar correctamente, póngase en contacto con el distribuidor de la suscripción.

Error de activación debido a una suscripción sobreusada

Problema

- Es posible que su suscripción esté sobreusada o abusada
- Error de activación debido a una suscripción sobreusada

Solución

Hay más dispositivos de los permitidos por esta suscripción. Puede ser víctima de una falsificación o piratería de software. No se puede utilizar la suscripción para activar otros productos de ESET. Puede resolver este problema directamente si puede administrar la suscripción de su cuenta de ESET HOME o si compró una suscripción de una fuente legítima. Si aún no tiene una cuenta, cree una.

Si es el dueño de una suscripción y no se le pidió que ingrese 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 sobreusada.

2. Para identificar e informar una suscripción de ESET pirateada, visite nuestro artículo Identificar e informar suscripciones de ESET pirateadas a fin de obtener instrucciones.

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

Si no es propietario de una suscripción, comuníquese con el propietario para informarle que no puede activar el

producto ESET debido a que la suscripción está sobreusada. El propietario puede resolver el problema en el portal ESET HOME.

Si se le pide que confirme su dirección de correo electrónico (solo en los casos graves), ingrese la dirección de correo electrónico que originalmente usó para comprar o activar su ESET Security Ultimate.

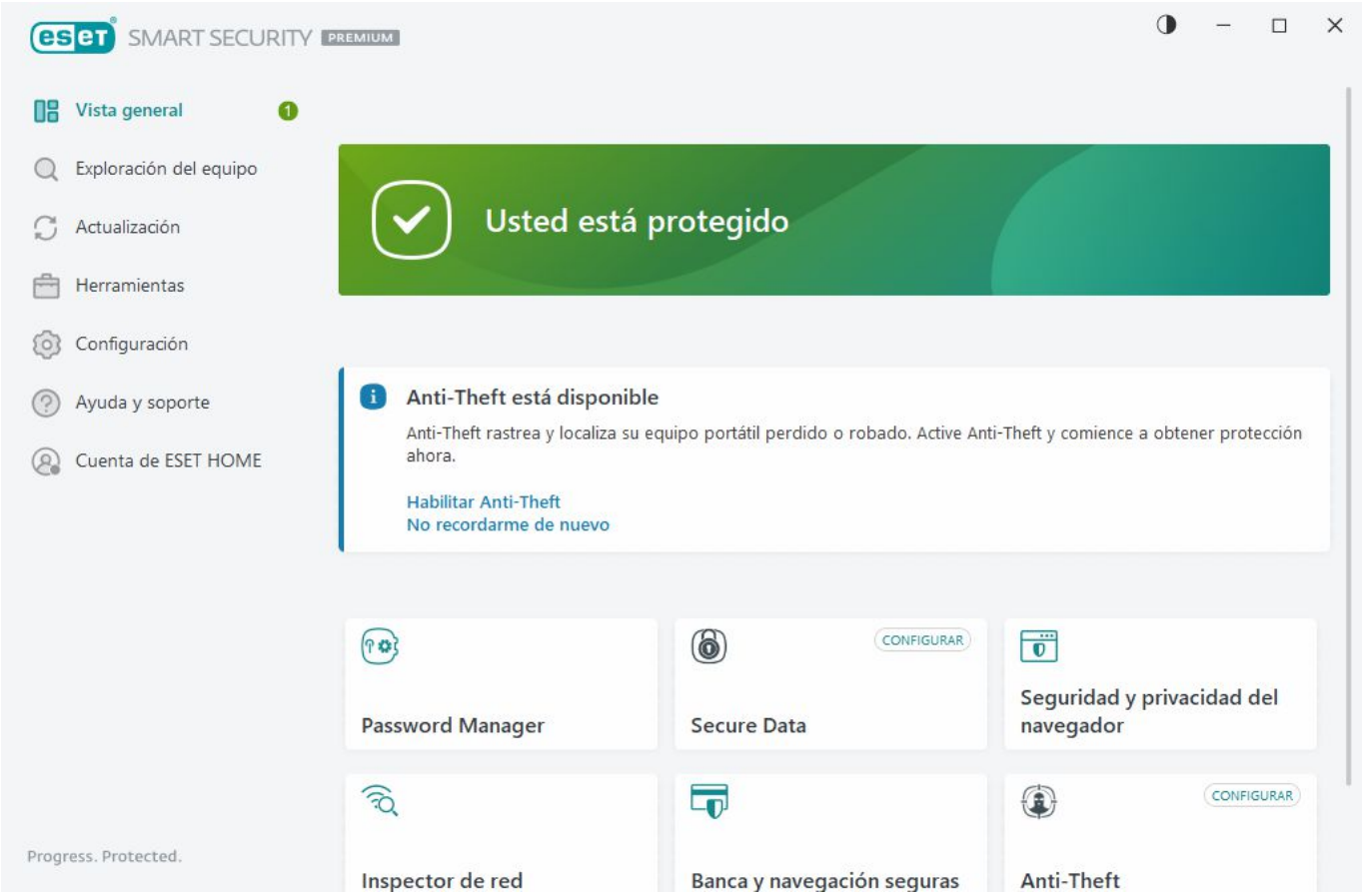
Trabajar con ESET Security Ultimate

La ventana principal del programa de ESET Security Ultimate se divide en dos secciones. La ventana primaria que está a la derecha muestra información correspondiente a la opción seleccionada en el menú principal de la izquierda.

> **Instrucciones ilustradas**
> Consulte Abrir la ventana principal del programa de los productos de ESET para Windows para obtener instrucciones ilustradas disponibles en inglés y en otros idiomas.

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

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



Opciones del menú principal:

Vista general: proporciona información sobre el estado de protección de ESET Security Ultimate.

Exploración del equipo: configura y ejecuta una exploración de tu ordenador o crea una exploración personalizada.

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

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

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

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

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

Visión general

En la ventana **Vista general** se muestra información sobre la protección actual del equipo junto con vínculos rápidos a las características de seguridad de ESET Security Ultimate.

En la ventana **Vista general** se muestran notificaciones con información detallada y soluciones recomendadas para mejorar la seguridad de ESET Security Ultimate, activar funciones adicionales o garantizar la máxima protección. Si hay más notificaciones, haga clic en **X más notificaciones** para ampliar todas.

Password Manager — Abre las instrucciones sobre cómo configurar Password Manager.

Inspector de red – Verifique la seguridad de su red.

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

Banca y navegación seguras: abre el navegador establecido como predeterminado en Windows en un modo seguro.

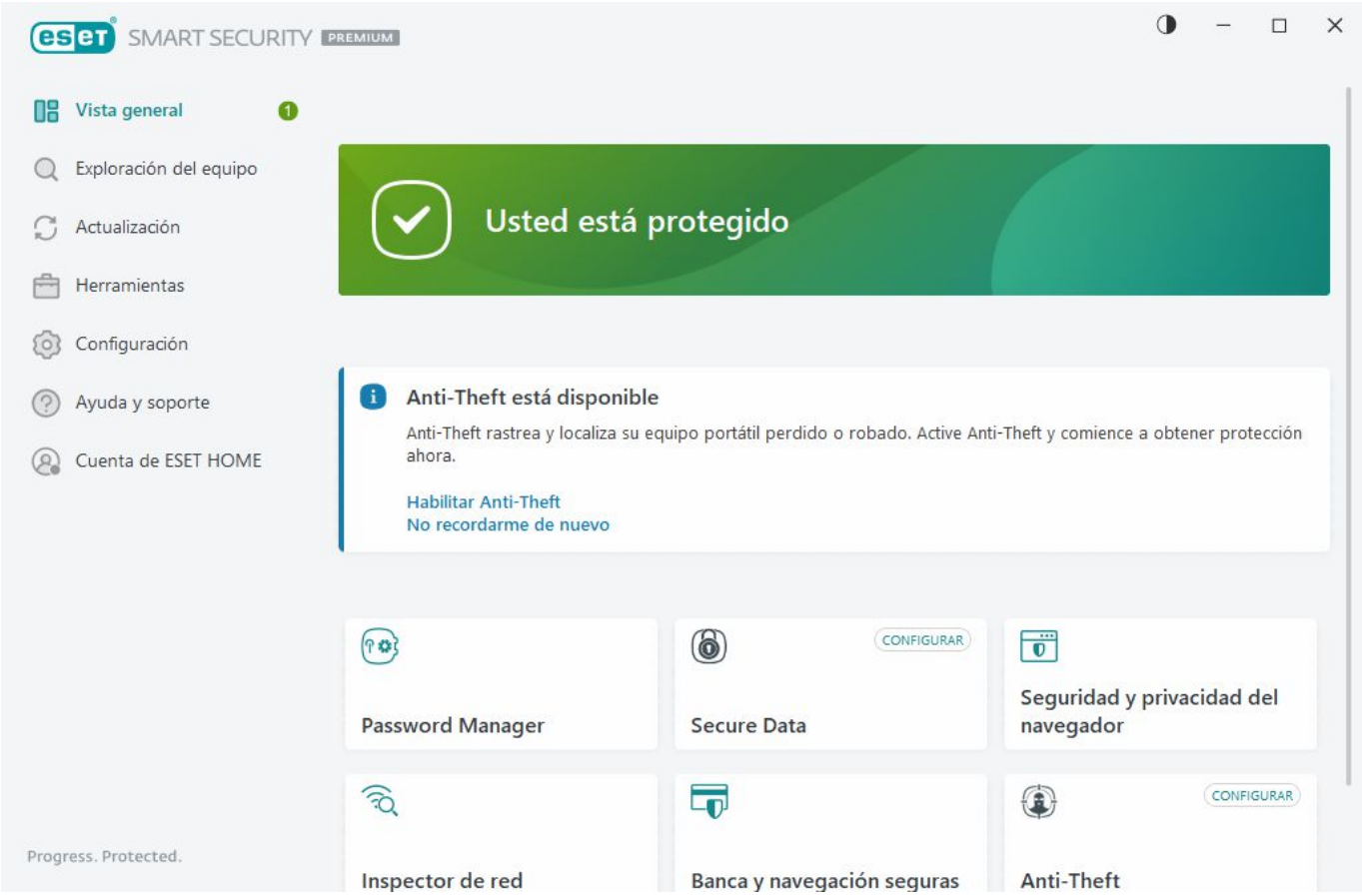
Seguridad y privacidad del navegador: puede seleccionar la instalación de qué extensiones se permitirá en un navegador protegido por ESET.

Anti-Theft — Inicia la configuración de Anti-Theft. Si ya configuró Anti-Theft, el enlace rápido abre la página de Anti-Theft.

VPN – Mantenga sus datos seguros, evite el seguimiento no deseado y mejore su privacidad con la seguridad adicional de una dirección IP anónima.

Identity Protection: Protege su información personal, crediticia y financiera. Identity Protection detecta la venta

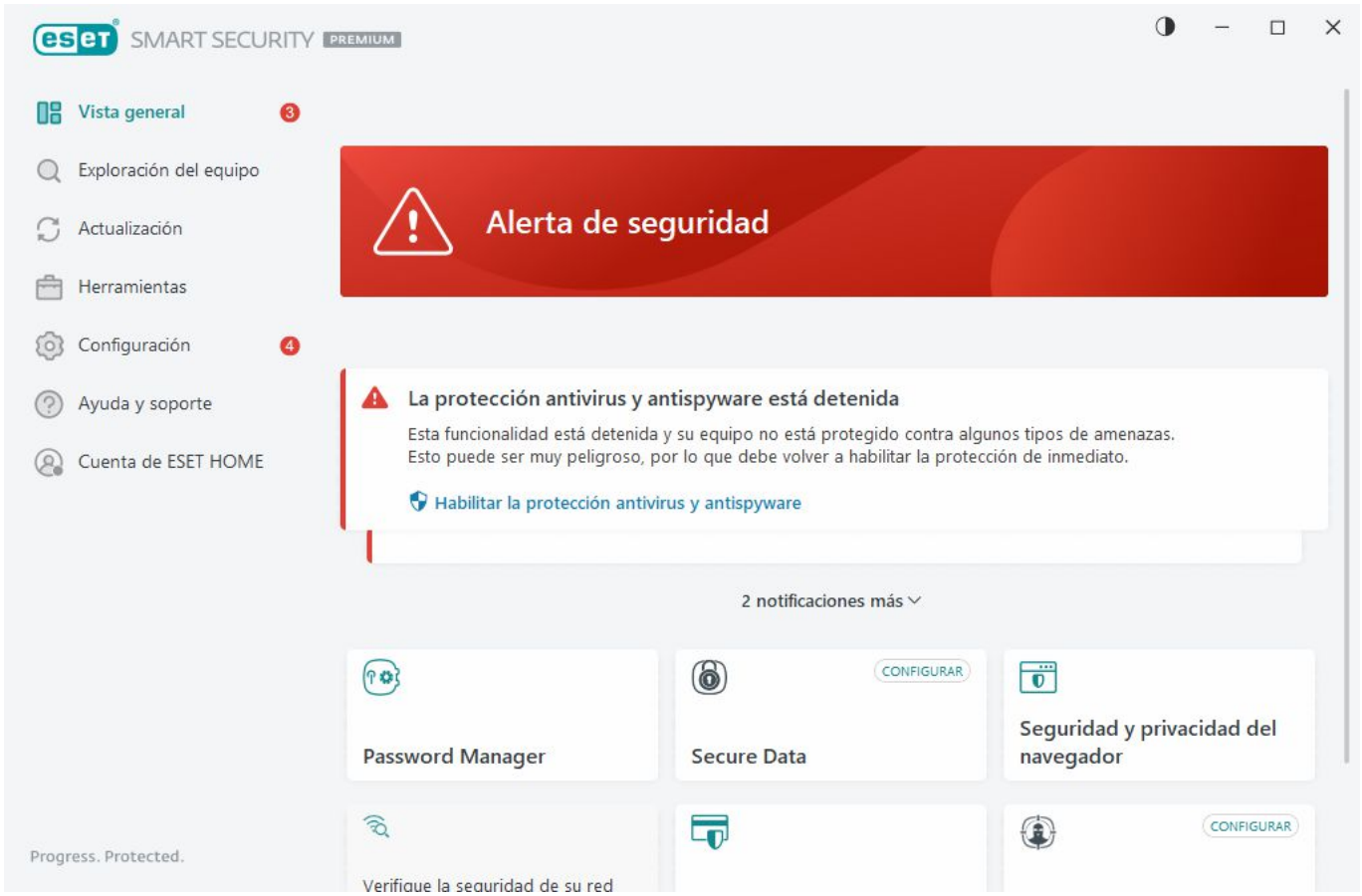
ilegal de su información personal proporcionando un monitoreo continuo.



El ícono verde y el estado verde **Está protegido** indican que la máxima protección está asegurada.

Qué hacer si el programa no funciona correctamente

Si un módulo de protección activo trabaja correctamente, el icono de estado de protección se volverá verde. Un signo de exclamación rojo o un icono de notificación naranja indican que no se asegura el máximo nivel de protección. Se muestra información adicional sobre el estado de protección de cada módulo y las soluciones sugeridas para restaurar la protección total como una notificación en la ventana **Descripción general**. Para cambiar el estado de un módulo individual, haga clic en **Configuración** y seleccione el módulo deseado.



El ícono rojo y el estado rojo **Alerta de seguridad** indican que existen problemas críticos. Existen varios motivos por los cuales se puede mostrar este estado, por ejemplo:

- **El producto no está activado** o **La suscripción está vencida** – Se indica mediante un icono rojo de estado de protección. Una vez que se vence la suscripción, el programa no se podrá actualizar. Siga las instrucciones en la ventana de alerta para renovar la suscripción.
- **El motor de detección está desactualizado** – este error aparecerá luego de varios intentos insatisfactorios de actualizar el motor de detección. Es recomendable verificar la configuración de la actualización. El motivo más común de este error es el ingreso incorrecto de los datos de autenticación o la configuración incorrecta de las opciones de conexión.
- **Se deshabilitó la protección del sistema de archivos en tiempo real**: el usuario deshabilitó la protección en tiempo real. Su computadora no está protegida contra amenazas. Haga clic en **Habilitar protección del sistema de archivos en tiempo real** para volver a habilitar esta funcionalidad.
- **Protección antivirus y antispyware deshabilitada**: puede volver a activar la protección antivirus y antispyware con un clic en **Habilitar todos los módulos de protección antivirus y antispyware**.
- **El firewall de ESET está deshabilitado**: este problema también se indica mediante una notificación de seguridad ubicada junto al elemento **Red** de su escritorio. Para volver a habilitar la protección de red, haga clic en **Habilitar el firewall**.

El icono naranja indica una protección limitada. Por ejemplo, puede haber un problema con la actualización del programa o en poco tiempo se cumpliría la fecha de vencimiento de la suscripción. Existen varios motivos por los cuales se puede mostrar este estado, por ejemplo:

- **Advertencia de optimización de Anti-Theft**: este dispositivo no se encuentra optimizado para Anti-Theft. Por ejemplo, es posible que la cuenta fantasma (una característica de seguridad que se activa

automáticamente cuando usted marca un dispositivo como perdido) no se haya creado en su equipo. Puede crearla con la característica Optimización en la interfaz web de Anti-Theft.

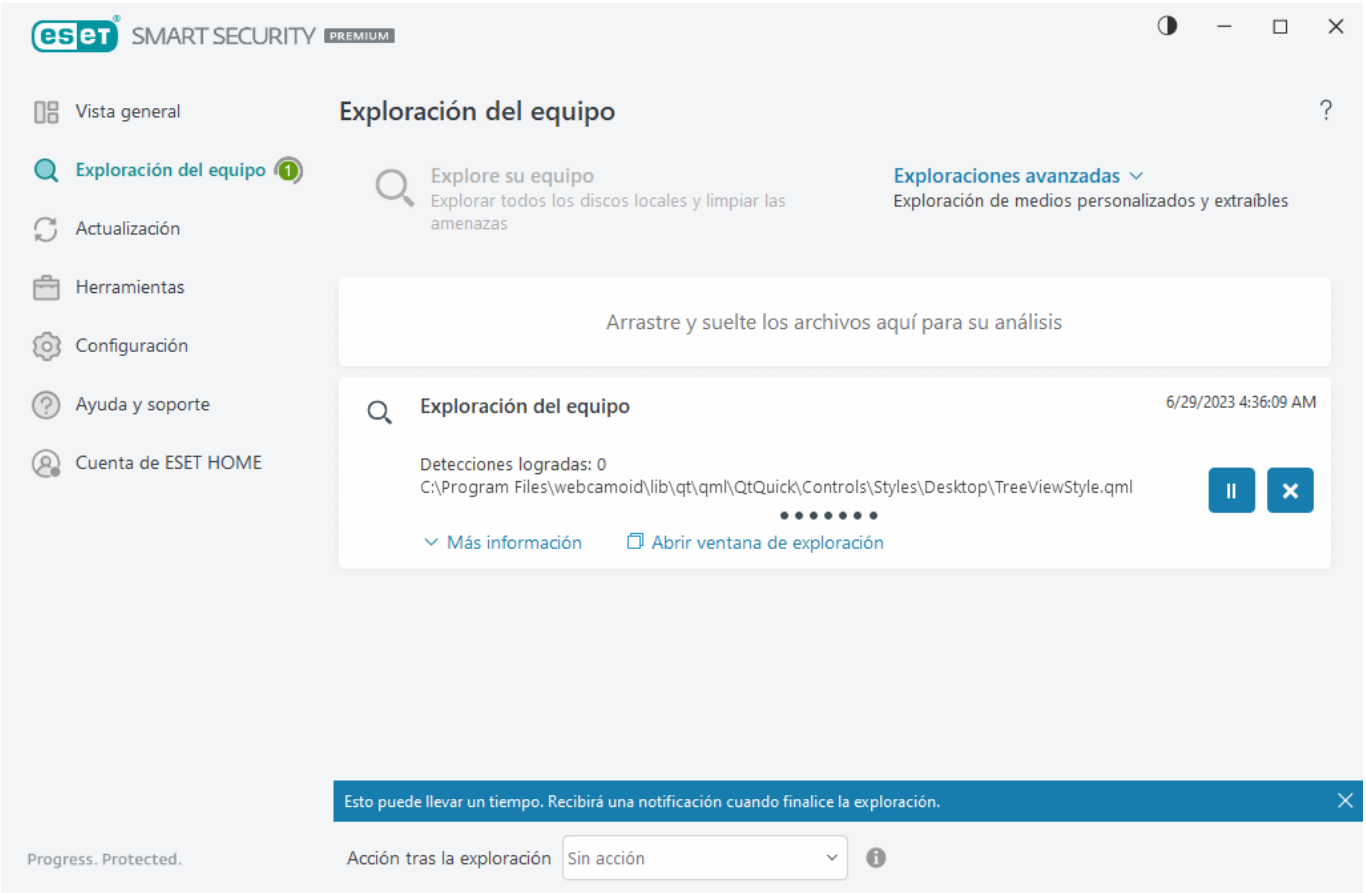
- **Modo de juego activo**: habilitar el Modo de juego es un riesgo potencial de la seguridad. Si se activa esta característica, se desactivan todas las ventanas de alerta y notificaciones, y se detienen las tareas programadas.

- **La suscripción se vencerá pronto/Su suscripción vence hoy**: se indica mediante un ícono de estado de protección y un signo de exclamación junto al reloj del sistema. Una vez que se vence la suscripción, el programa no podrá actualizarse y el ícono de estado de protección se pondrá rojo.

Si no puede solucionar el problema mediante las sugerencias, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o buscar en la base de conocimiento de ESET. Si aún necesita asistencia, puede enviar una petición de soporte. El Soporte técnico de ESET responderá rápidamente a sus preguntas y lo ayudará a encontrar una resolución.

Exploración del equipo

El módulo de exploración bajo demanda es una parte importante de la solución antivirus. Se usa para realizar la exploración de los archivos y las carpetas del equipo. Desde el punto de vista de la seguridad, es esencial que las exploraciones del equipo se ejecuten en forma habitual como parte de las medidas de seguridad de rutina, no solo cuando existen sospechas de una infección. Es recomendable realizar habitualmente exploraciones profundas del sistema para detectar los virus que la Protección del sistema de archivos en tiempo real no capturó cuando se guardaron en el disco. Esta situación puede ocurrir si la protección del sistema de archivos en tiempo real no estaba habilitada en el momento, si el motor de detección es obsoleto o si el archivo no se detecta como un virus cuando se guarda en el disco.



Se encuentran disponibles dos tipos de **Exploración del equipo**. **Explorar el equipo** explora de manera rápida el sistema sin especificar parámetros de exploración. **La exploración personalizada** (en Exploración avanzada) le permite seleccionar perfiles de exploración predefinidos diseñados para ciertas ubicaciones de destino y elegir objetos de exploración específicos.

Para obtener más información sobre el proceso de la exploración, consulte Progreso de la exploración.

> De forma predeterminada, ESET Security Ultimate intentar limpiar o quitar de forma automática las detecciones encontradas durante la exploración del equipo. En algunos casos, si no se puede realizar ninguna acción, recibe una alerta interactiva y debe seleccionar una acción de limpieza (por ejemplo, quitar o ignorar). Para cambiar el nivel de limpieza y para obtener información más detallada, consulte Limpieza. Para revisar exploraciones anteriores, consulte Archivos de registro.

Explore su equipo

Explore el equipo le permite iniciar rápidamente una exploración del equipo y desinfectar los archivos infectados sin necesidad de la intervención del usuario. La ventaja de la **Explore el equipo** es su facilidad de uso y que no requiere una configuración detallada de la exploración. Esta exploración verifica todos los archivos de las unidades locales y limpia o elimina en forma automática las infiltraciones detectadas. El nivel de desinfección está establecido automáticamente en el valor predeterminado. Para obtener información más detallada sobre los tipos de desinfección, consulte Desinfección.

También puede utilizar la función **Arrastrar y soltar para explorar** un archivo o una carpeta manualmente haciendo clic en el archivo o la carpeta, moviendo el puntero del mouse hacia el área marcada al mismo tiempo que mantiene el botón pulsado, y luego lo suelta. Después de eso, la aplicación se mueve al primer plano.

Las siguientes opciones de exploración están disponibles en **Exploraciones avanzadas**:

Exploración personalizada

La **Exploración personalizada** permite especificar parámetros de exploración, como los objetos o métodos. La ventaja de la **Exploración personalizada** consiste en que puede configurar los parámetros detalladamente. Es posible guardar las configuraciones en perfiles de exploración definidos por el usuario, lo que resulta útil si la exploración se efectúa reiteradamente con los mismos parámetros.

Exploración de medios extraíbles

Es similar a **Explore el equipo**: inicia rápidamente una exploración de los medios extraíbles (por ej., CD/DVD/USB) que estén conectados al equipo en ese momento. Puede ser útil cuando conecta al equipo una unidad flash USB y desea explorar sus contenidos en busca de malware y otras amenazas potenciales.

Este tipo de exploración también puede iniciarse al hacer clic en **Exploración personalizada**, luego seleccionar **Medios extraíbles** del menú desplegable de **Objetos para explorar** y, por último, hacer clic en **Explorar**.

Repetir la última exploración

Le permite lanzar rápidamente la exploración realizada anteriormente, con los mismos ajustes.

El menú desplegable **Acción después de la exploración** permite establecer una acción que se realice automáticamente tras finalizar una exploración:

- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.
- **Apagar** – el equipo se apaga después de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo se reinicia solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Reiniciar** – cierra todos los programas abiertos, y reinicia el equipo luego de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo fuerza el reinicio solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.
- **Suspender**– guarda su sesión y pone el equipo en un estado de energía baja para que pueda volver a trabajar rápidamente.
- **Hibernar**– toma todo lo que se está ejecutando en la memoria RAM y lo envía a un archivo especial de su disco duro. Su equipo se apaga, pero reanudará su estado anterior la próxima vez que lo inicie.

> Las acciones **Suspender** o **Hibernar** están disponibles en función de la configuración de Activar o Hibernar del sistema operativo o de las capacidades de su equipo/computadora portátil. Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad cuando el equipo funciona con la alimentación de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

La acción seleccionada comenzará tras la finalización de las exploraciones en ejecución. Cuando seleccione **Apagar** o **Reiniciar**, aparecerá un cuadro de diálogo de confirmación con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

> Se recomienda ejecutar una exploración del equipo al menos una vez al mes. La exploración se puede configurar como una tarea programada en **Herramientas** > **Tareas programadas**. ¿Cómo programo una exploración semanal del equipo?

Iniciador de la exploración personalizada

Puede usar la exploración personalizada para explorar la memoria operativa, la red o las partes específicas de un disco, en lugar del disco completo. Para hacerlo, haga clic en **Exploraciones avanzadas** > **Exploración personalizada** y seleccione los objetivos específicos de la estructura de la carpeta (árbol).

En el menú desplegable **Perfil**, puede elegir un perfil que podrá usar al explorar objetos específicos. El perfil predeterminado es **Análisis inteligente**. Hay otros tres perfiles de exploración predefinidos denominados **Exploración exhaustiva**, **Exploración del menú contextual** y **Exploración del equipo**. Estos perfiles de exploración usan diferentes parámetros deThreatSense. Las opciones disponibles se describen en Configuración avanzada > **Motor de detección** > **Exploraciones de malware** > **Exploración bajo demanda** > ThreatSense.

La estructura de la carpeta (árbol) también contiene objetos específicos para explorar.

- **Memoria operativa** – explora todos los procesos y datos que la memoria operativa utiliza actualmente.

• **Sectores de inicio/UEFI** – explora los sectores de inicio y UEFI para detectar la presencia de virus. Lea más sobre el análisis UEFI en el glosario.

• **Base de datos WMI**: explora la base de datos Windows Management Instrumentation (WMI) en su totalidad, todos los espacios de nombre, las instancias y propiedades. Busca referencias para archivos infectados o malware insertados como datos.

• **Registro del sistema**: explora el registro del sistema en su totalidad, como claves y subclaves. Busca referencias para archivos infectados o malware insertados como datos. Al desinfectar las detecciones, la referencia permanece en el registro para garantizar que no se pierdan datos importantes.

Para ir rápidamente a un objeto de exploración (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 la exploración, marque la casilla de verificación en la estructura de árbol.

> **Cómo programar una exploración semanal del equipo**
> Para programar una tarea regular, consulte Cómo programar una exploración semanal del equipo.

Puede configurar los parámetros de limpieza para la exploración en Configuración avanzada > **Motor de detección** > **Exploración de malware** > **Exploración a demanda** > **ThreatSense** > **Desinfección**. Para ejecutar una exploración sin acciones de limpieza, haga clic en **Configuración avanzada** y seleccione **Explorar sin limpieza**. El historial de la exploración se guarda en el registro de la exploración.

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

Haga clic en **Explorar** para ejecutar la exploración con los parámetros personalizados establecidos.

Explorar como administrador permite ejecutar la exploración desde una cuenta de administrador. Use en esta opción si el usuario actual no tiene los privilegios necesarios para acceder a los archivos que desea explorar. Este botón no está disponible si el usuario actual no puede realizar operaciones UAC como administrador.

Para ver el registro de exploración del equipo cuando finaliza una exploración, haga clic en Mostrar registro.

Progreso de la exploración

La ventana de progreso de la exploración muestra el estado actual de la exploración junto con información sobre la cantidad detectada de archivos con códigos maliciosos.

Es común que algunos archivos, como los archivos protegidos por contraseña o los que usa el sistema de manera exclusiva (habitualmente, archivos *pagefile.sys* y ciertos archivos de registro), no se puedan explorar. Puede encontrar más detalles en nuestro artículo de la base de conocimiento.

Cómo programar una exploración semanal del equipo

Para programar una tarea regular, consulte Cómo programar una exploración semanal del equipo.

Progreso de la exploración: la barra de progreso muestra el estado de la exploración en ejecución.

Destino – el nombre del objeto actualmente explorado y su ubicación.

Detecciones logradas: muestra la cantidad total de archivos explorados, de amenazas encontradas y de amenazas eliminadas durante una exploración.

Haga clic en Más información para mostrar la siguiente información:

- **Usuario**: nombre de la cuenta de usuario que inició la exploración.
- **Objetos explorados**: cantidad de objetos ya explorados.
- **Duración**: tiempo transcurrido.

Icono de pausa: pausa una exploración.

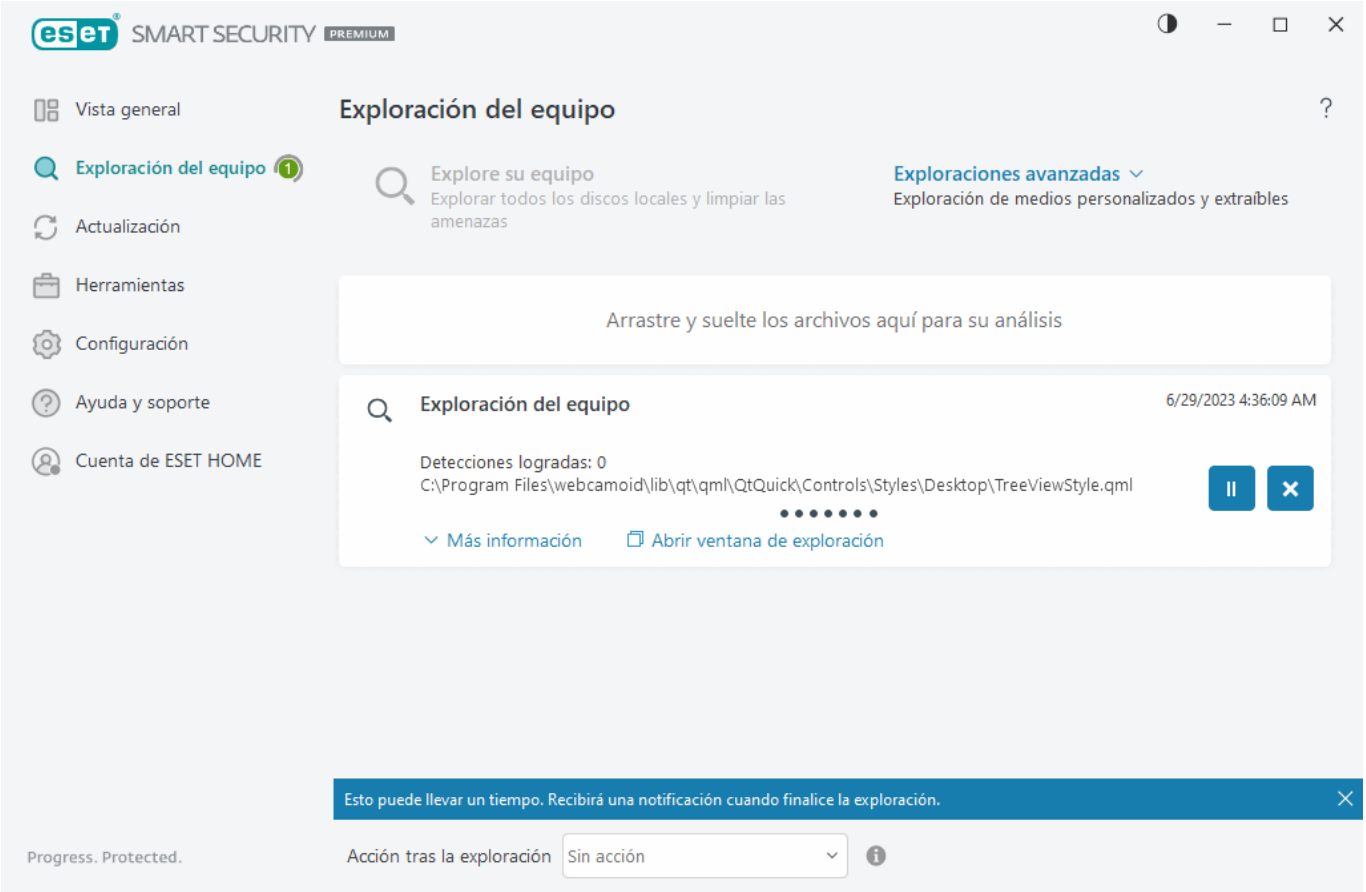
Reanudar: esta opción se muestra cuando el progreso de la exploración está en pausa. Haga clic en el icono para continuar explorando.

Icono de detención: finaliza la exploración.

Haga clic en la **ventana Abrir exploración** para abrir el registro de escaneo del equipo con más detalles sobre la exploración.

Desplazarse por el registro de exploración – si la opción está habilitada, el registro de exploración se desplazará hacia abajo automáticamente a medida que las nuevas entradas se van agregando para que sean visibles las más recientes.

Haga clic en la lupa o flecha para mostrar los detalles sobre la exploración actualmente en ejecución. Si desea ejecutar otra exploración en paralelo, haga clic en **Explorar el equipo** o **Exploraciones avanzadas** > **Exploración personalizada**.



El menú desplegable **Acción después de la exploración** permite establecer una acción que se realice automáticamente tras finalizar una exploración:

- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.
- **Apagar** – el equipo se apaga después de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo se reinicia solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Reiniciar** – cierra todos los programas abiertos, y reinicia el equipo luego de la finalización de la exploración.
- **Reiniciar si es necesario**: el equipo fuerza el reinicio solo si es necesario para completar la limpieza de las amenazas detectadas.
- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.
- **Suspender**– guarda su sesión y pone el equipo en un estado de energía baja para que pueda volver a trabajar rápidamente.
- **Hibernar**– toma todo lo que se está ejecutando en la memoria RAM y lo envía a un archivo especial de su disco duro. Su equipo se apaga, pero reanudará su estado anterior la próxima vez que lo inicie.

Las acciones **Suspender** o **Hibernar** están disponibles en función de la configuración de Activar o Hibernar del sistema operativo o de las capacidades de su equipo/computadora portátil. Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad cuando el equipo funciona con la alimentación de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

La acción seleccionada comenzará tras la finalización de las exploraciones en ejecución. Cuando seleccione **Apagar** o **Reiniciar**, aparecerá un cuadro de diálogo de confirmación con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

Registro de la exploración del equipo

Puede ver información detallada relacionada con una exploración específica en Archivos de registro. El registro la exploración contiene la siguiente información:

- Versión del motor de detección:
- Fecha y hora de inicio
- Lista de discos, carpetas y archivos explorados
- Nombre de la exploración programada (solo exploración programada)
- Usuario que inició la exploración.
- Estado de la exploración
- Cantidad de objetos explorados
- Cantidad de detecciones encontradas
- Hora de finalización
- Tiempo total de exploración

Se omite el nuevo inicio de una tarea de exploración programada del equipo si se sigue ejecutando la misma tarea programada que se ejecutó anteriormente. La tarea de exploración programada omitida creará un registro de exploración del equipo con 0 objetos analizados y el estado **No se inició la exploración porque la exploración anterior todavía estaba en ejecución**.

Para buscar registros de exploración anteriores, en la ventana principal del programa, seleccione **Herramientas** > **Archivos de registro**. En el menú desplegable, seleccione **Exploración del equipo** y haga doble clic en el registro deseado.

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

Haga clic en el ícono del interruptor **Filtrado** para abrir la ventana Filtrado de registros para reducir la búsqueda según criterios personalizados. Para ver el menú contextual, haga clic derecho en una entrada de registro específica:

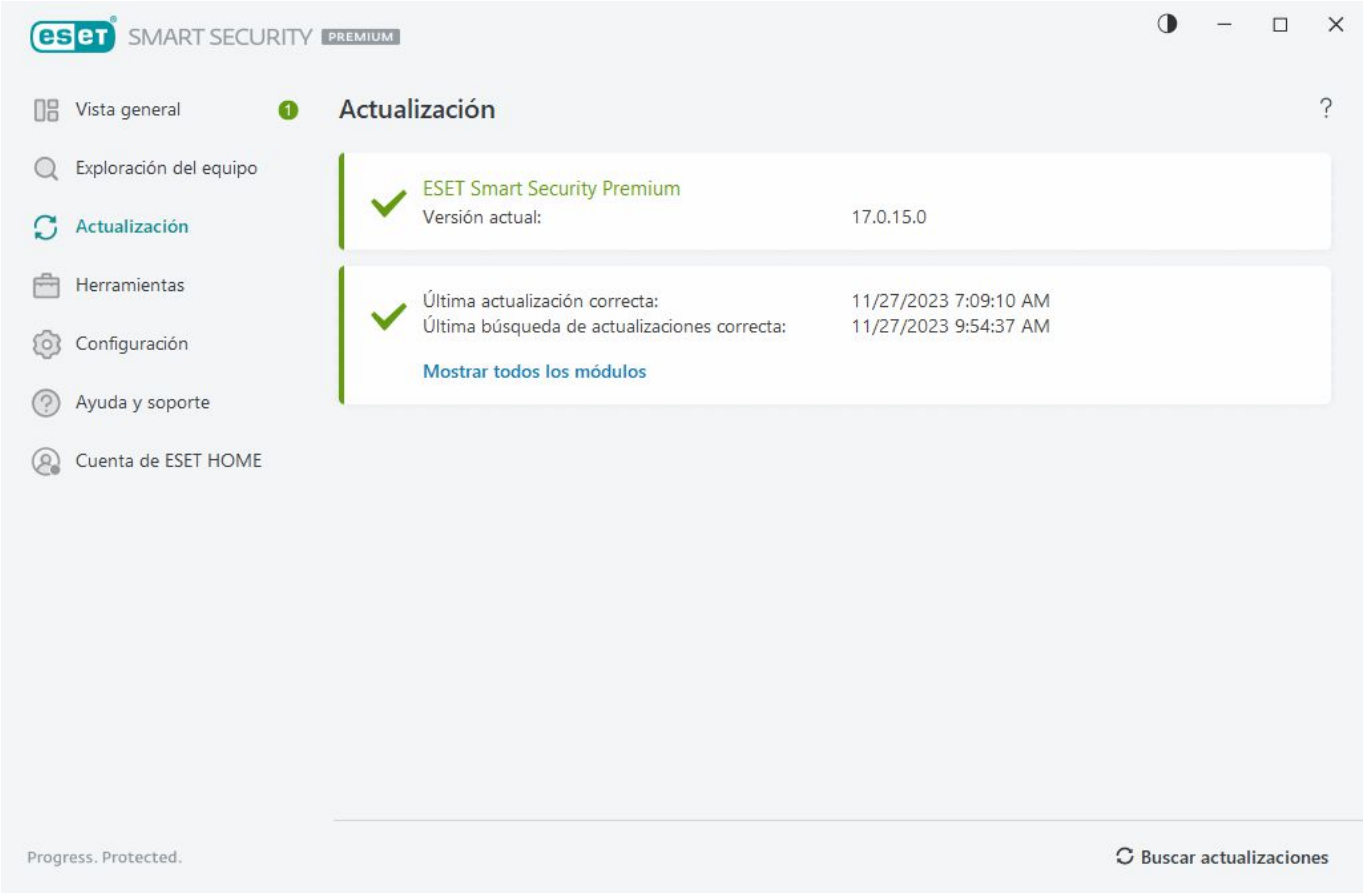
Acción	Uso
Filtrar los mismos registros	Activa el filtrado de registros. El registro solo mostrará los registros del mismo tipo que el seleccionado.
Filtrar	Esta opción abre la ventana de filtrado de registros y le permite definir los criterios de entradas de registro específicas. Acceso directo: `Ctrl+Shift+F`
Deshabilitar el filtro	Activa la configuración del filtro. Si activa el filtro por primera vez, debe definir la configuración y se abrirá la ventana de filtrado de registros.
Deshabilitar el filtro	Desactiva el filtro (es lo mismo que hacer clic en el botón 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 del portapapeles en un archivo XML.
Exportar todo	Esta opción exporta todos los registros de la ventana en 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 actualización habitual de ESET Security Ultimate es la mejor forma de asegurar el máximo nivel de seguridad en el equipo. El módulo de actualización se asegura de que los módulos del programa y los componentes del sistema estén siempre actualizados.

Al hacer clic en **Actualización** en la ventana principal del programa, verá el estado actual de la actualización, incluyendo la fecha y la hora de la última actualización correcta y si es necesario actualizar.

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual. La actualización frecuente de los módulos y componentes del programa es un aspecto importante para mantener una protección completa contra los códigos maliciosos. Preste atención a su configuración y funcionamiento. Debe activar su producto mediante su clave de activación para recibir las actualizaciones. Si no lo hizo durante la instalación, puede activar ESET Security Ultimate para acceder a los servidores de actualización de ESET. ESET le provee su clave de activación por correo electrónico después de la compra de ESET Security Ultimate.



Versión actual: muestra el número de la versión actual instalada.

Última actualización exitosa: muestra la fecha de la última actualización exitosa. Si no visualiza una fecha reciente, es posible que los módulos de producto no estén actualizados.

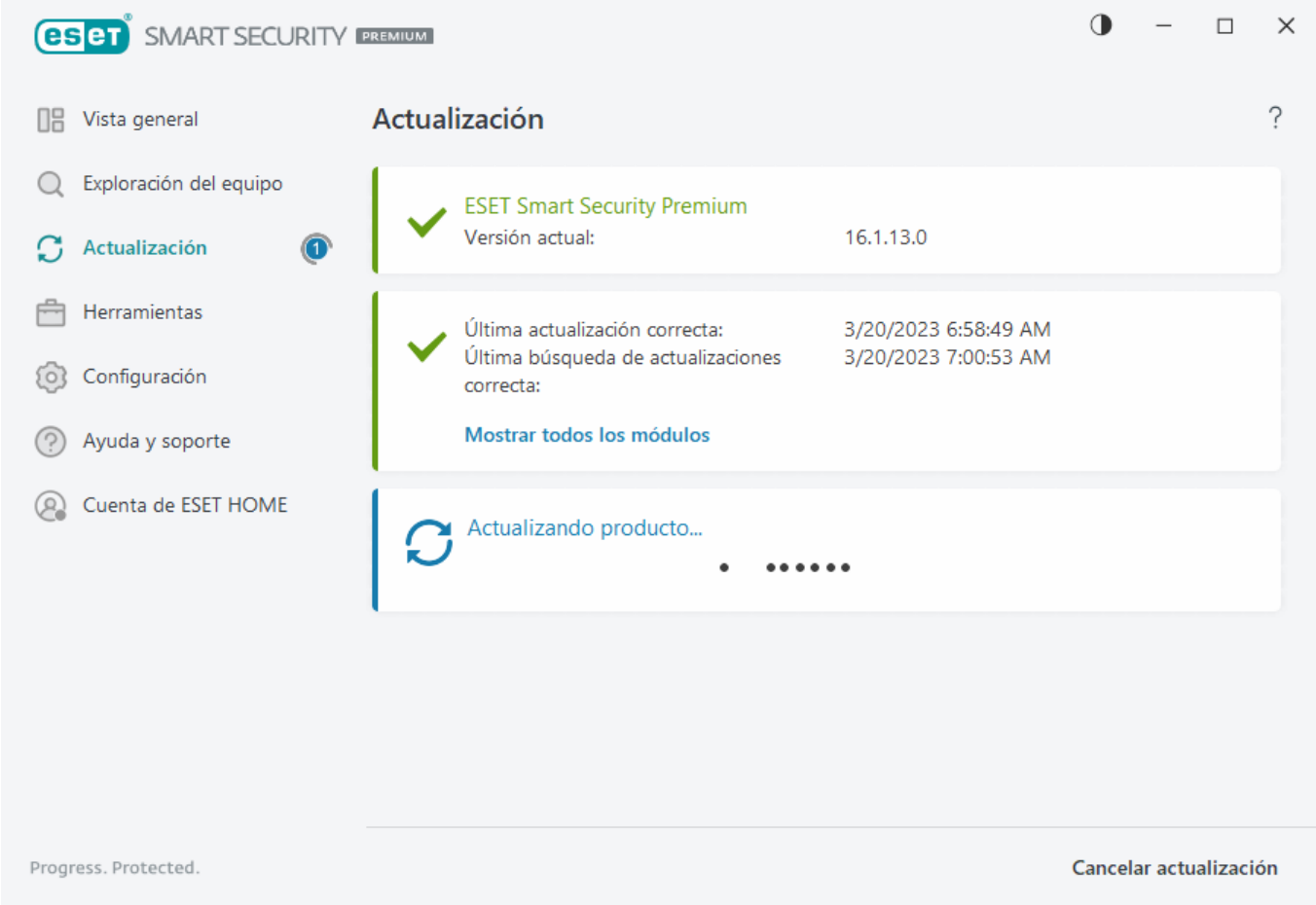
Último verificación exitosa de actualizaciones: muestra la fecha de la última verificación exitosa de actualizaciones.

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

Haga clic en **Verificar actualizaciones** para verificar la versión disponible de ESET Security Ultimate más reciente.

Proceso de actualización

Luego de hacer clic en **Buscar actualizaciones**, comienza el proceso de descarga. Se mostrará una barra de progreso de la descarga y el tiempo restante para su finalización. Para interrumpir la actualización, haga clic en **Cancelar actualización**.



En circunstancias normales, puede ver la marca de verificación verde en la ventana **Actualización** que indica que el programa está actualizado. Si este no es el caso, el programa está desactualizado y más vulnerable a una infección. Actualice los módulos lo antes posible.

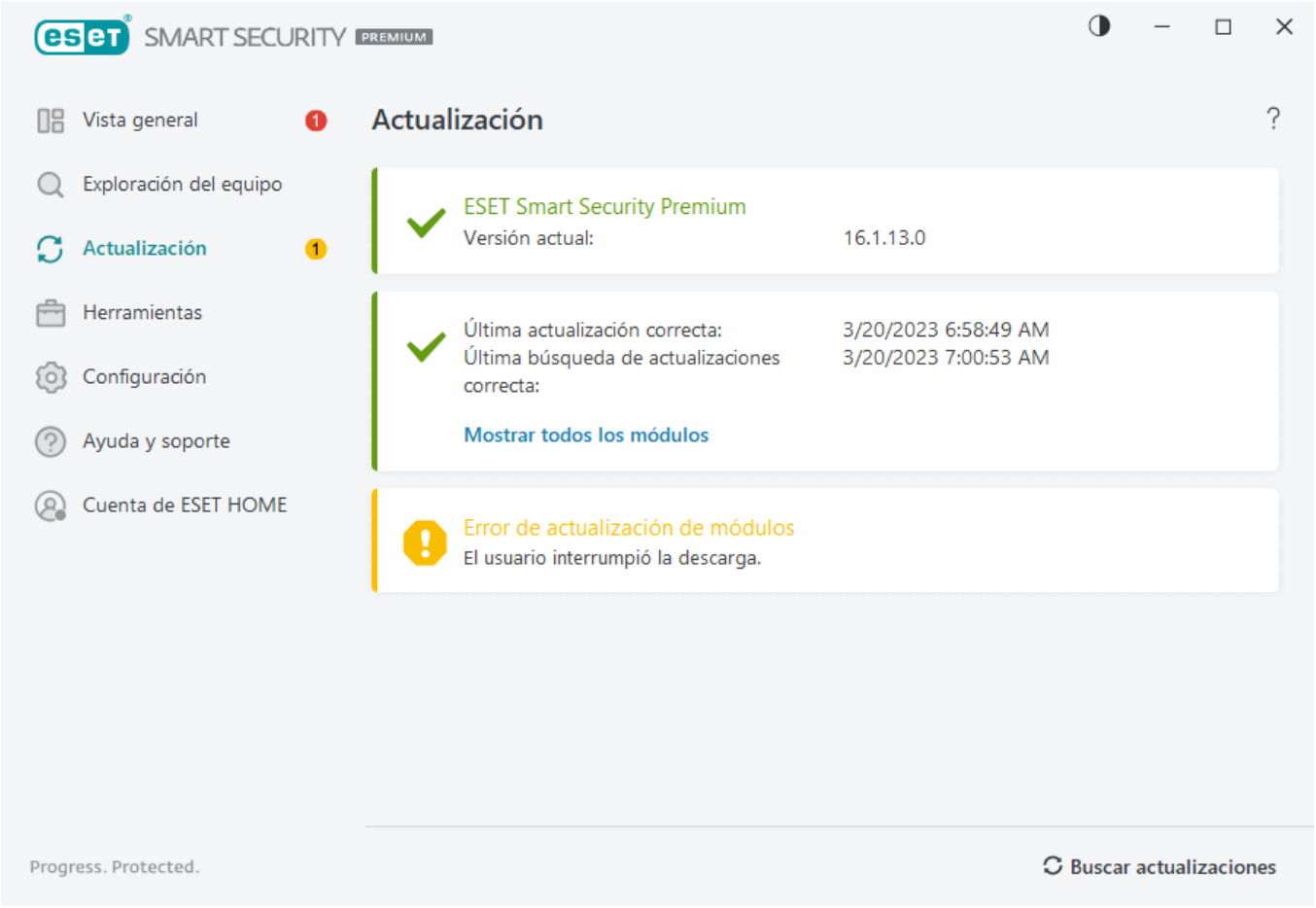
Última actualización exitosa

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

1. **Suscripción no válida**: la suscripción que se usó para la activación no es válida o está vencida. En la ventana principal del programa, haga clic en **Ayuda y soporte** > **Cambiar suscripción** y active su producto.

2. **Se produjo un error al descargar los archivos de actualización**: una causa posible de este error es la configuración de la conexión a Internet incorrecta. Es recomendable verificar su conectividad a Internet (para ello, abra cualquier sitio Web en su navegador Web). Si el sitio Web no se abre, es probable que la conexión a

Internet no esté establecida o que haya problemas de conectividad en el equipo. Consulte el problema con su proveedor de servicios de Internet (ISP) si su conexión está inactiva.



Debe reiniciar su equipo después de una actualización exitosa de ESET Security Ultimate a una versión de producto más reciente para asegurarse de que todos los módulos del programa se actualizaron correctamente. No es necesario que reinicie su computadora luego de las actualizaciones regulares de los módulos.

Para obtener más información, visite este artículo sobre el mensaje «Falló la actualización de los módulos» de la sección de resolución de problemas.

Cuadro de diálogo: es necesario reiniciar

Después de actualizar ESET Security Ultimate con una nueva versión, es necesario reiniciar el equipo. Las versiones nuevas de ESET Security Ultimate se emiten para implementar mejoras o corregir problemas que las actualizaciones automáticas de los módulos del programa no pueden resolver.

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

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

Cómo crear tareas de actualización

Las actualizaciones pueden accionarse manualmente con un clic en **Buscar actualizaciones** en la ventana primaria que se muestra al hacer clic en **Actualizar** en el menú principal.

Las actualizaciones también pueden ejecutarse como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Tareas programadas**. Las siguientes tareas de actualización se encuentran activas en forma predeterminada en ESET Security Ultimate:

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

Cada tarea de actualización puede modificarse acorde a sus necesidades. Además de las tareas de actualización predeterminadas, puede crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más detalles sobre la creación y la configuración de tareas de actualización, consulte la sección Tareas programadas.

Herramientas

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

 Archivos de registro

 Procesos en ejecución (si ESET LiveGrid® se encuentra habilitado en ESET Security Ultimate)

 Informe de seguridad

 Conexiones de red (si el Firewall se encuentra habilitado en ESET Security Ultimate)

 ESET SysInspector

 Tareas programadas

 Limpiador de sistema

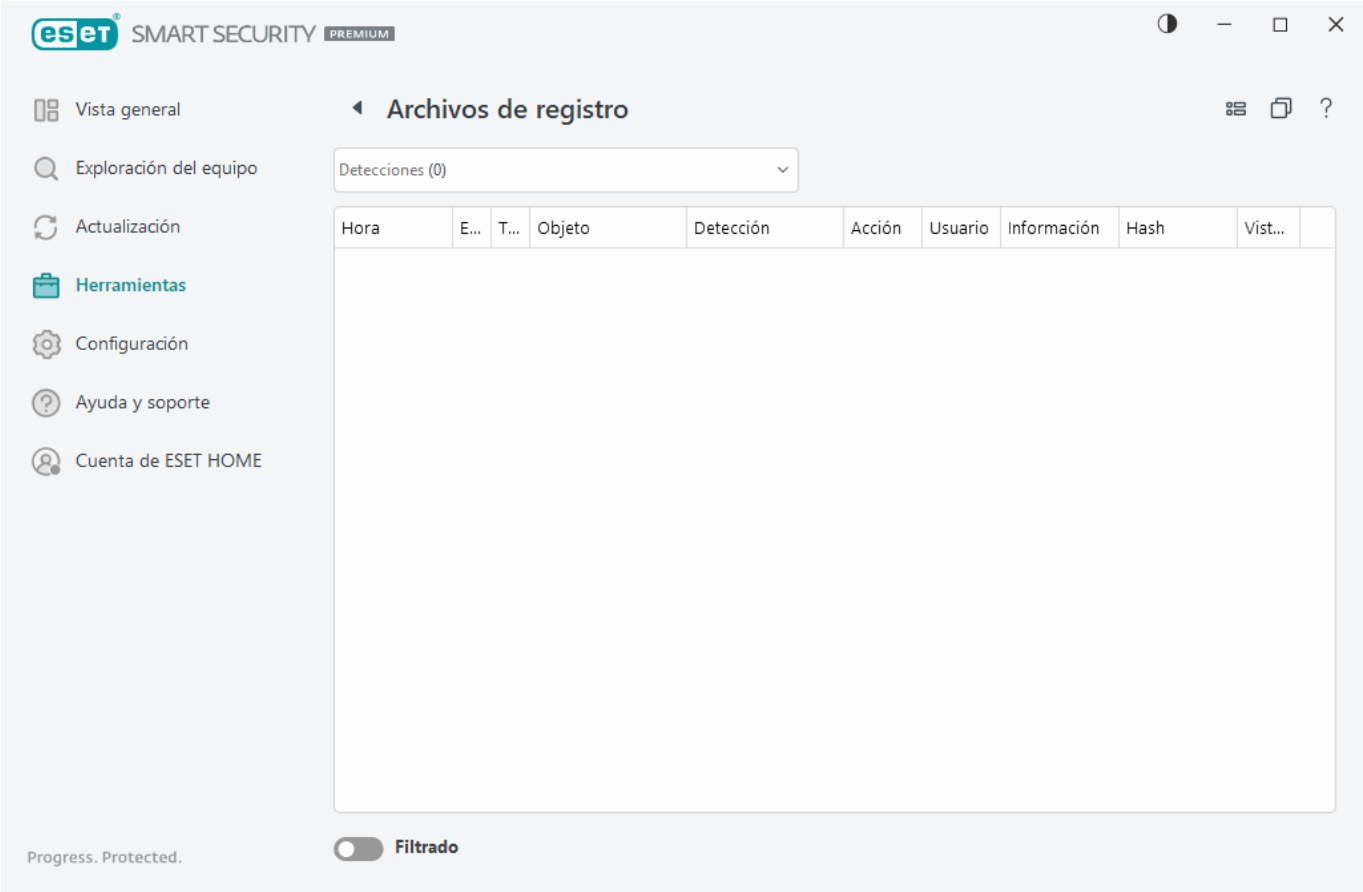
 Inspector de red

 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 sobre los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las amenazas detectadas. La emisión de registros es un componente esencial para el análisis del sistema, la detección de amenazas y la solución de problemas. La emisión de registros se mantiene activa en segundo plano sin necesidad de la interacción del usuario. La información se registra de acuerdo con el nivel de detalle actualmente configurado. Se pueden ver los mensajes de texto y los registros directamente desde el entorno de ESET Security Ultimate, donde además se pueden archivar registros.



Para acceder a los archivos de registro, diríjase a la ventana principal del programa y haga clic en **Herramientas** > **Archivos de registro**. Seleccione el tipo de registro deseado del menú desplegable Registro.

- **Amenazas detectadas**: el registro de amenazas ofrece información detallada sobre las infiltraciones y amenazas detectadas por ESET Security Ultimate. La información de registro incluye la hora de la detección, el tipo de exploración, el tipo de objeto, el nombre de la detección, la acción realizada y el nombre del usuario registrado cuando se detectó la infiltración, el hash y la primera ocurrencia. Las infiltraciones no limpiadas se marcan siempre con texto rojo sobre un fondo rojo claro. Mientras que las infiltraciones limpiadas se marcan con texto amarillo sobre un fondo blanco. Las aplicaciones no deseadas o potencialmente inseguras no limpiadas se marcan con texto amarillo sobre fondo blanco.

- **Sucesos** – todas las acciones importantes que ESET Security Ultimate lleva a cabo se registran en el registro de sucesos. El registro de sucesos contiene información sobre los sucesos y errores que se produjeron en el programa. Se diseñó para que los administradores de sistemas y los usuarios puedan solucionar problemas. Con frecuencia, la información aquí incluida puede ayudarlo a encontrar una solución a un problema que ocurra en el programa.

- **Exploración del equipo**: en esta ventana, se muestran los resultados de todas las exploraciones anteriores. Cada línea corresponde a un único exploración del equipo. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración seleccionado.

- **Archivos enviados**: contiene registros de muestras que se enviaron a ESET LiveGuard.

- **HIPS**: contiene historiales de las reglas HIPS específicas que están marcadas para incluirse en el registro. El protocolo muestra la aplicación que desencadenó la operación, el resultado (si la regla se permitió o prohibió) 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 red**: el registro de protección de red muestra todos los ataques remotos detectados por el firewall, la protección de ataques de red (IDS) y la protección contra botnets. Aquí encontrará información sobre todos los ataques a su equipo. En la columna Evento se muestra una lista de los ataques detectados. La columna Origen da más información sobre el atacante. La columna Protocolo revela el protocolo de comunicación utilizado en el ataque. Un análisis del registro de protección de red puede ayudarlo a detectar a tiempo los intentos de infiltraciones en el sistema para prevenir el acceso no autorizado. Para obtener más información sobre los ataques de red, consulte IDS 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 o el control parental. Cada registro incluye la hora, la dirección URL, el usuario y la aplicación de creación de conexión con un sitio Web en particular.

- **Antispam del cliente de correo electrónico** – contiene historiales relacionados con los mensajes de correo electrónico que se marcaron como spam.

- **Control parental**: muestra las páginas Web bloqueadas o permitidas por el control parental. Las columnas Coincidir tipo y Coincidir valores le indican cómo se aplicaron las reglas de filtrado.

- **Control del dispositivo**: contiene registros de medios o dispositivos extraíbles que se conectaron al equipo. Solo los dispositivos con reglas de control del dispositivo respectivo se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, se creará una entrada del registro para un dispositivo conectado. También puede ver detalles tales como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).

- **Protección de cámara web**: contiene registros de aplicaciones bloqueadas por la protección de cámara web.

Seleccione los contenidos de cualquier registro y presione **CTRL + C** para copiarlo al portapapeles. Mantenga presionado **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 secundario en un registro específico para abrir el menú contextual. Las siguientes opciones se encuentran disponibles en el menú contextual:

- **Mostrar**– muestra información más detallada acerca del registro seleccionado en una ventana nueva.

- **Filtrar los mismos historiales** – luego de activar este filtro, solo verá los historiales del mismo tipo (diagnósticos, advertencias, ...).

- **Filtrar** – Después de hacer clic en esta opción, la ventana Filtrado de registros le permitirá definir los criterios de filtrado para entradas de registros específicas.

- **Habilitar filtro** – activa las configuraciones de los filtros.

- **Deshabilitar el filtro** – borra todas las configuraciones del filtro (descritas arriba).

- **Copiar/Copiar todo:** copia información sobre los registros seleccionados.

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

• **Quitar/Quitar todo:** quita los registros seleccionados o todos los registros mostrados. Esta acción requiere privilegios de administrador.

• **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 la detección con un asistente (no disponible para la detección de malware).

• **Agregar a la lista de permitidos de protección del navegador**: abre la ventana Lista de permitidos de protección del navegador y agrega el elemento a la lista.

Filtrado de registros

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

La característica de filtrado de registros lo ayudará a encontrar la información que busca, en particular, cuando hay muchos registros. Le permite acotar los registros, por ejemplo, si busca un tipo de evento, un estado o un periodo de tiempo específicos. Puede filtrar los registros al especificar ciertas opciones de búsqueda y solo se mostrarán los registros que sean pertinentes (en función de dichas opciones de búsqueda) en la ventana Archivos de registro.

Escriba la palabra clave que está buscando en el campo **Buscar texto**. Utilice el menú desplegable **Buscar en columnas** para acotar la búsqueda. Elija uno o más registros del menú desplegable **Tipos de registro**. Defina el **periodo de tiempo** para el que quiere que se muestren los resultados. También puede usar otras opciones de búsqueda, como **Solo coincidir palabras completas** o **Coincidir mayúsculas y minúsculas**.

Buscar el texto

Escriba una cadena (palabra o una parte de una palabra). Solo se mostrarán los registros que contengan dicha cadena. Se omitirán otros registros.

Buscar en columnas

Seleccione qué columnas se tomarán en cuenta en la búsqueda. Puede marcar una o más columnas para utilizar en la búsqueda.

Tipos de historiales

Elija uno o más tipos de registro del menú desplegable:

• **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.

• **Informativo** – registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.

• **Advertencias** – registra los errores críticos y los mensajes de advertencia.

• **Errores** – se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.

• **Crítico** – registra solo los errores críticos (error al iniciar la protección antivirus,

Período de tiempo

Defina el momento a partir del cual desea que se muestren los resultados.

• **Sin especificar** (predeterminado): no busca en un periodo de tiempo, sino en todo el registro.

• **Ayer**

• **Última semana**

• **El mes pasado**

• **Período de tiempo**: puede especificar el periodo de tiempo exacto (Desde: y Hasta:) para filtrar únicamente los registros del periodo de tiempo especificado.

Solo coincidir palabras completas

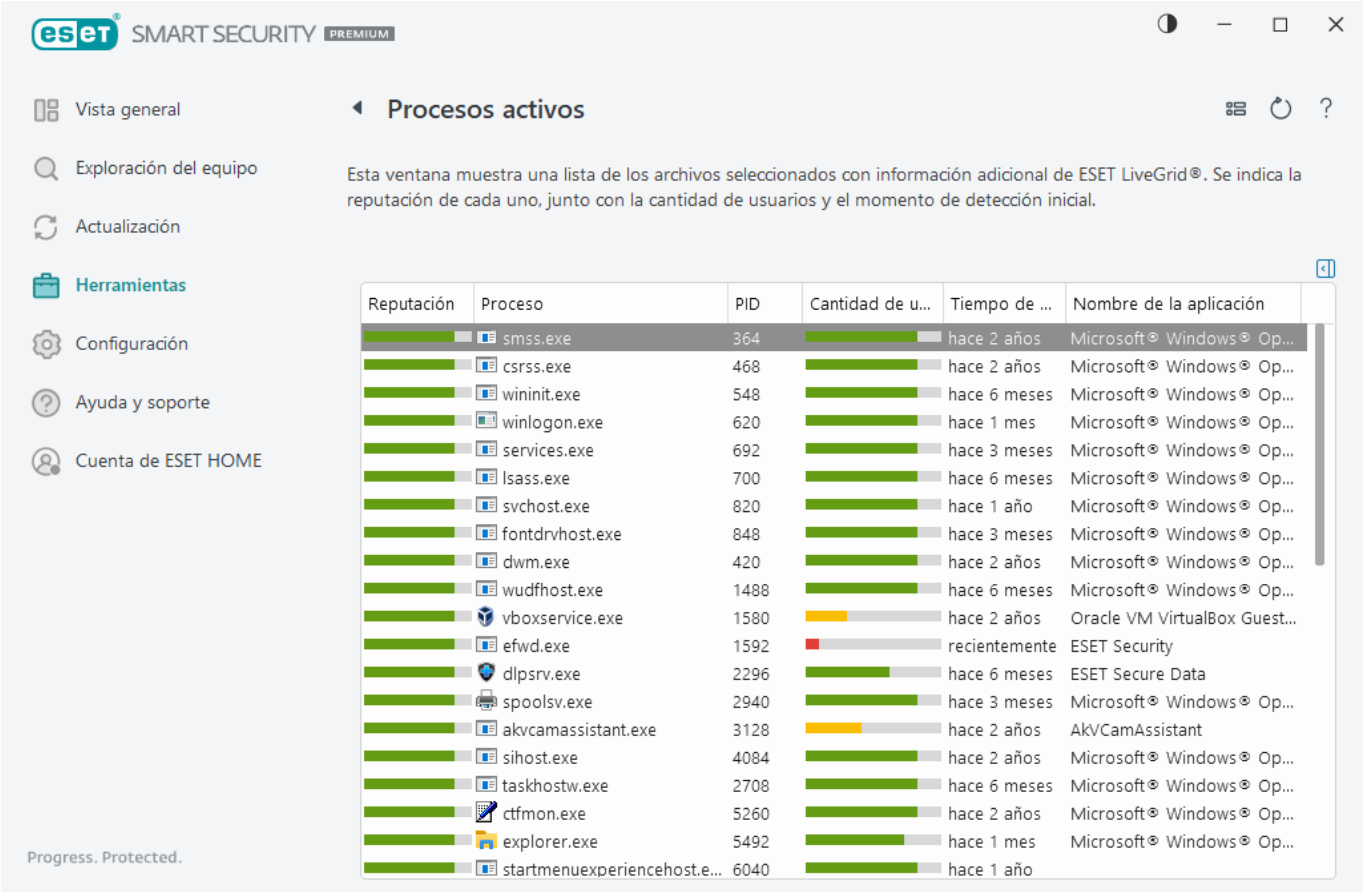
Utilice la casilla de verificación si quiere buscar palabras completas para resultados más precisos.

Coincidir mayúsculas y minúsculas

Habilite esta opción si es importante para usted usar letras mayúsculas o minúsculas al filtrar. Una vez que haya configurado las opciones de filtrado/búsqueda, haga clic en **Aceptar** para mostrar los registros filtrados o en **Buscar** para comenzar a buscar. Los archivos de registro se buscan de arriba hacia abajo, comenzado por su posición actual (el registro que está resaltado). La búsqueda se detiene cuando encuentra el primer registro coincidente. Presione **F3** para buscar el siguiente registro o haga clic con el botón secundario y seleccione **Buscar** para refinar las opciones de búsqueda.

Procesos en ejecución

Los procesos activos muestran los programas o procesos activos en su equipo y mantiene a ESET informado de manera instantánea y continua sobre las nuevas infiltraciones. ESET Security Ultimate proporciona información detallada sobre los procesos activos para proteger a los usuarios con la tecnología ESET LiveGrid®.



Reputación – en la mayoría de los casos, la tecnología ESET Security Ultimate y ESET LiveGrid® les asigna niveles de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para ello, utiliza una serie de reglas heurísticas que examinan las características de cada objeto y después estima su potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor 1: seguro (en color verde) hasta 9: peligroso (en color rojo).

Proceso – la imagen y el nombre del programa o proceso que se está ejecutando actualmente en el equipo. También puede usar el Administrador de tareas de Windows para ver todos los procesos activos en el equipo. Para abrir el Administrador de tareas, haga clic con el botón secundario en un área de la barra de tareas y luego haga clic en **Administrador de tareas**, o presione **Ctrl**+**Shift**+**Esc** en el teclado.

Las aplicaciones conocidas marcadas como Seguras (verde)están definitivamente limpias (están en la lista blanca) y se excluirán de la exploración para mejorar el rendimiento.

PID : el número del identificador de procesos se puede usar como parámetro en diversas llamadas de funciones como ajustar la prioridad del proceso.

Cantidad de usuarios – la cantidad de usuarios que usan una aplicación específica. Estos datos se recopilan con la tecnología ESET LiveGrid®.

Tiempo de descubrimiento – periodo transcurrido desde que la tecnología ESET LiveGrid® descubrió la aplicación.

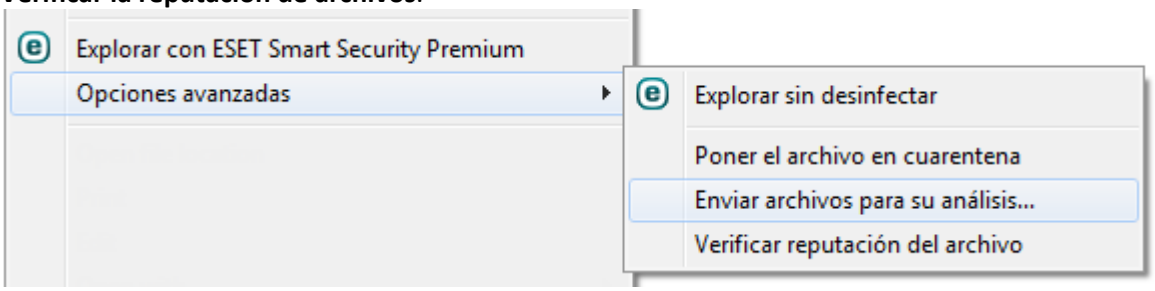
La aplicación marcada como Desconocida (naranja) no es necesariamente software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, puede enviar el archivo para su análisis al laboratorio de investigación de ESET. Si el archivo resulta ser una aplicación maliciosa, se agregará su detección a una de las próximas actualizaciones.

Nombre de la aplicación – el nombre dado a un programa o proceso.

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

- **Ruta** – ubicación de una aplicación en su equipo.
- **Tamaño** – tamaño del archivo ya sea en kB (kilobytes) o MB (megabytes).
- **Descripción** – características del archivo según la descripción proporcionada por el sistema operativo.
- **Empresa** – nombre del proveedor o del proceso de la aplicación.
- **Versión** – información proporcionada por el desarrollador de la aplicación.
- **Producto** – nombre de la aplicación y/o nombre comercial.
- **Creado el/Modificado el**: fecha y hora de la creación (modificación).

También puede verificar la reputación de los archivos que no sean programas o procesos activos. Para ello, haga clic con el botón secundario en un explorador de archivos y seleccione **Opciones avanzadas** > **Verificar la reputación de archivos**.



Informe de seguridad

Esta función proporciona una descripción general de las estadísticas para las siguientes catgorías:

- **Páginas web bloqueadas** – Muestra el número de páginas web bloqueadas (URL en la lista negra para PUA, phishing, router hackeado, IP o certificado).
- **Objetos de correo electrónico infectados detectados** – Muestra el número de objetos de correo electrónico infectados que se han detectado.
- **Páginas web con Control parental bloqueadas** – Muestra el número de páginas web bloqueadas con el control parental.
- **PUA detectadas** – Muestra el número de aplicaciones potencialmente no deseadas (PUA).
- **Spam de correo electrónico detectado** – Muestra el número de correos electrónicos de spam detectados.
- **Accesos bloqueados a cámara web**: muestra el número de accesos bloqueados a la cámara web.
- **Documentos explorados**: muestra el número de objetos de documento explorados.
- **Aplicaciones exploradas**: muestra el número de objetos ejecutables explorados.
- **Otros objetos explorados**: muestra el número de otros objetos explorados.

- **Objetos de páginas web explorados**: muestra el número de objetos explorados de la página web.
- **Objetos del correo electrónico analizados**: muestra el número de objetos del correo electrónico analizados.
- **Archivos analizados por ESET LiveGuard**: muestra la cantidad de muestras analizadas por ESET LiveGuard.

El orden de estas categorías depende del valor numérico, desde el más alto hasta el más bajo. No se visualizan las categorías con valores cero. Haga clic en **Mostrar más** para expandir y mostrar categorías ocultas.

La última parte del Informe de seguridad le brinda la posibilidad de activar las siguientes funciones:

- ESET LiveGuard
- Secure Data
- Control parental
- Anti-Theft

Una vez que la función está activada, ya no aparecerá como no funcional en el informe de seguridad.

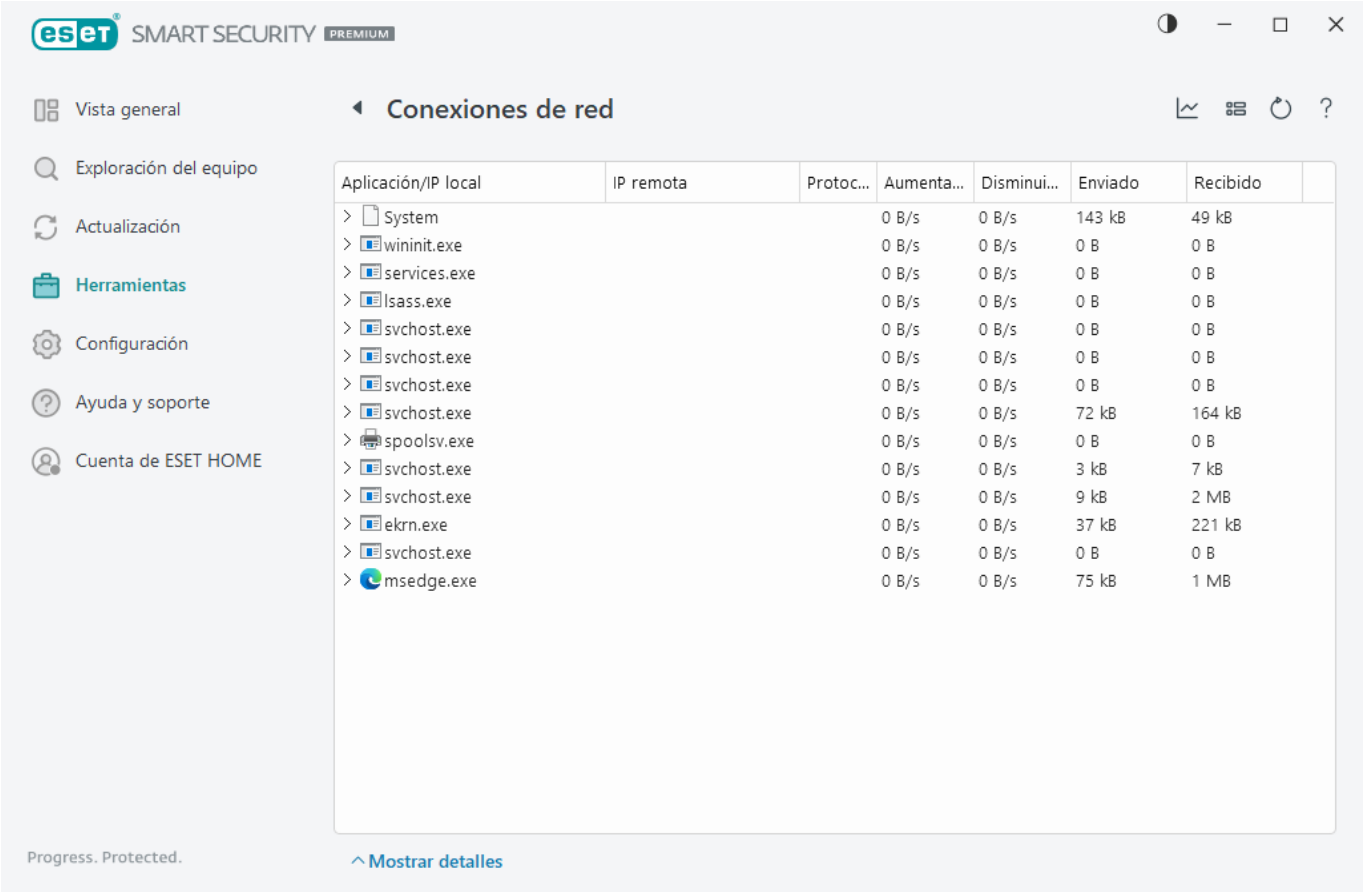
Haga clic en la rueda de engranaje en la esquina superior derecha, donde puede **Habilitar/deshabilitar las notificaciones del informe de seguridad** o puede seleccionar si los datos que se mostrarán serán de los últimos 30 días o desde que se activó el producto. Si ESET Security Ultimate tiene menos de 30 días de instalación, sólo se puede seleccionar el número de días desde la instalación. El período de 30 días se establece de forma predeterminada.

Restablecer los datos eliminará todas las estadísticas así como los datos existentes para el informe de seguridad.

Esta acción debe confirmarse, a menos que se desactive 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, verá una lista de las conexiones activas y pendientes. Sirve para controlar todas las aplicaciones que establecen conexiones salientes.



Haga clic en el ícono del gráfico para abrir 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 realizadas por la aplicación (e información más detallada), 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 del equipo remoto específico.

Protocolo – protocolo de transferencia utilizado.

Aumentar velocidad/Disminuir velocidad – la velocidad actual de los datos salientes y entrantes.

Enviado/Recibido – cantidad de datos intercambiados en la conexión.

Mostrar detalles – elija esta opción para mostrar información detallada sobre la conexión seleccionada.

Haga un clic derecho en una conexión para ver opciones adicionales, entre las que se incluyen:

Resolver nombres de host – si es posible, todas las direcciones de red se muestran en el formato de nombre DNS, no en el formato numérico de dirección IP.

Mostrar solo las conexiones TCP – la lista muestra únicamente las conexiones pertenecientes al grupo de protocolos TCP.

Mostrar las conexiones de escucha – seleccione esta opción para mostrar únicamente aquellas conexiones para las que aún no se estableció comunicación alguna, pero para las que el sistema ha abierto un puerto y está esperando establecer una conexión.

Mostrar las conexiones dentro del equipo – seleccione esta opción para mostrar únicamente aquellas conexiones en las que el lado remoto es un sistema local; es decir, las llamadas conexiones localhost.

Actualizar la velocidad – elija la frecuencia para actualizar las conexiones activas.

Actualizar ahora – actualiza la ventana de **Conexiones de red**.

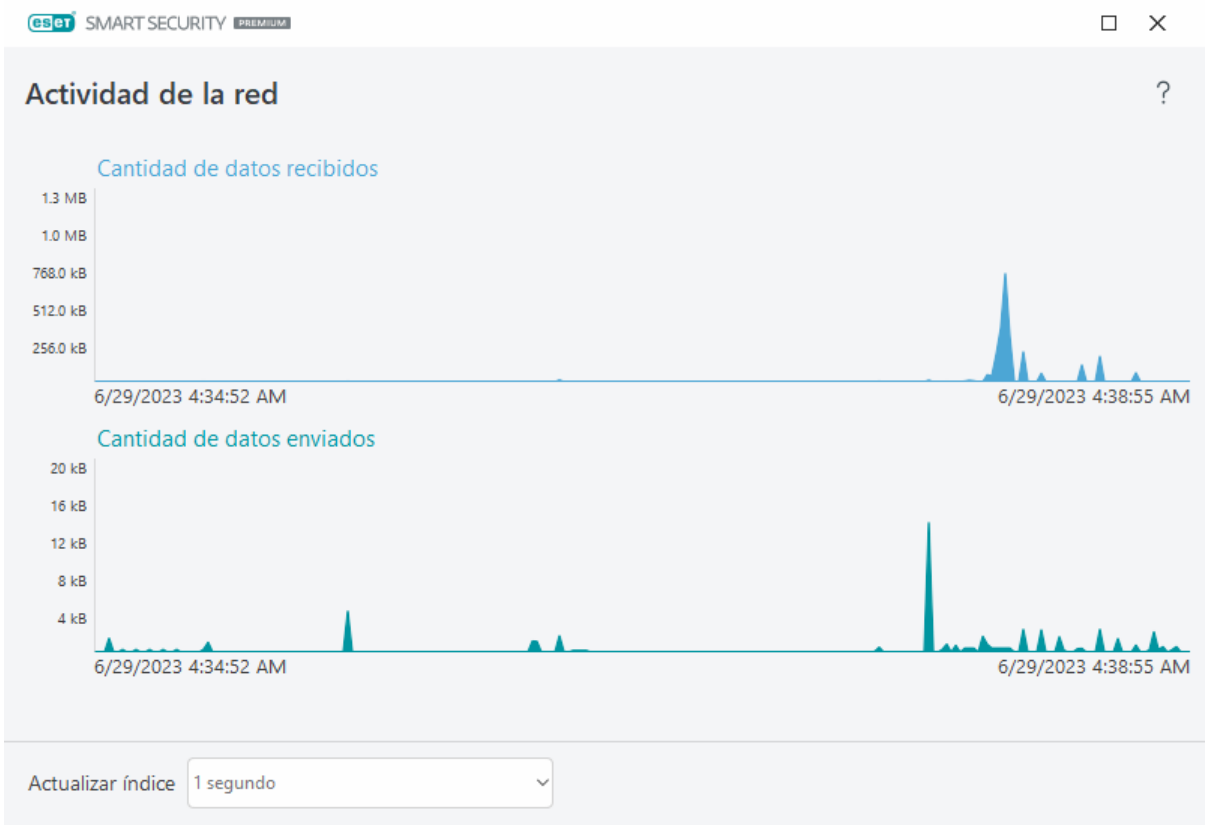
Las siguientes opciones están disponibles solo luego de hacer clic en una aplicación o proceso, no en una conexión activa:

Denegar temporalmente las comunicaciones para el proceso – rechaza las conexiones actuales de la aplicación determinada. Si se establece una nueva conexión, el firewall usa una regla predefinida. Puede encontrar una descripción de la configuración en la sección Reglas de Firewall.

Permitir temporalmente las comunicaciones para el proceso – permite las conexiones actuales de la aplicación determinada. Si se establece una nueva conexión, el firewall usa una regla predefinida. Puede encontrar una descripción de la configuración en la sección Reglas de Firewall.

Actividad de la red

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



Se encuentran disponibles las siguientes opciones:

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

El eje vertical del gráfico representa la cantidad de datos recibidos o enviados. Coloque el puntero del mouse 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 minuciosamente su equipo, recopila información detallada sobre los componentes del sistema como las aplicaciones y los controladores, las conexiones de red o las entradas de registro importantes, y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa del comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de códigos maliciosos. Para aprender a usar ESET SysInspector, consulte la Ayuda en línea de ESET SysInspector.

La ventana ESET SysInspector muestra la siguiente información de los registros:

- **Hora** – la hora de creación del registro.
- **Comentario** – un breve comentario.
- **Usuario** – el nombre del usuario que creó el registro.

- **Estado** – el estado de la creación del registro.

Están disponibles las siguientes opciones:

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

- **Crear** – crea un nuevo registro. 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 los registros seleccionados de la lista.

Los siguientes elementos están disponibles en el menú contextual cuando se seleccionan uno o más archivos de registro:

- **Mostrar** – abre el registro seleccionado en ESET SysInspector (equivale a hacer doble clic en el registro).

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

- **Eliminar** – elimina los registros seleccionados de la lista.

- **Eliminar todo** – elimina todos los registros.

- **Exportar** – exporta el registro a un archivo .xml o .xml comprimido.

Tareas programadas

Desde la sección de tareas programadas, se gestionan y ejecutan tareas programadas según la configuración y las propiedades predefinidas.

Para acceder a las tareas programadas, diríjase a la ventana principal del programa ESET Security Ultimate y haga clic en **Herramientas** > **Tareas programadas**. La sección **Tareas programadas** contiene una lista de todas las tareas programadas y propiedades de configuración, como la fecha y la hora predefinidas y el perfil de exploración utilizado.

Esta sección sirve para programar las siguientes tareas: la actualización de módulos, la tarea de exploración, la verificación de archivos de inicio del sistema y el mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana principal de Tareas programadas (haga clic en **Agregar tarea** o **Eliminar** en el sector inferior). Puede restaurar la lista de tareas programadas a los valores predeterminados y eliminar todos los cambios haciendo clic en **Predeterminado**. Haga un clic con el botón secundario en cualquier parte de la ventana Tareas programadas para realizar una de las siguientes acciones: mostrar información detallada, ejecutar la tarea de inmediato, agregar una nueva tarea y eliminar una tarea existente. Use las casillas de verificación al comienzo de cada entrada para activar o desactivar las tareas.

En forma predeterminada, se muestran las siguientes **tareas programadas**:

- **Mantenimiento de registros**

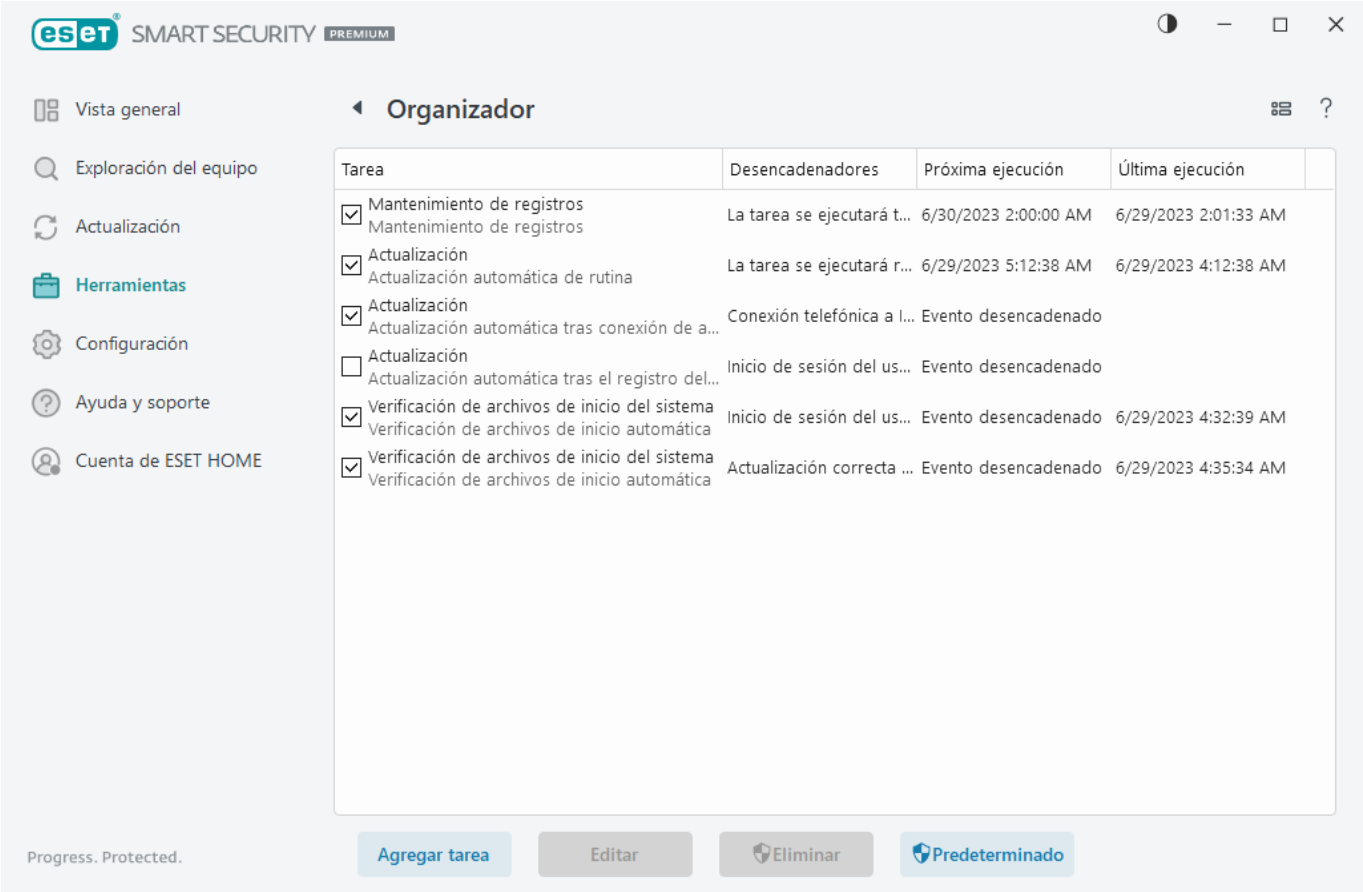
- **Actualización automática de rutina**

- **Actualización automática luego del registro del usuario**

• **Verificación de archivos de inicio automática** (después del registro del usuario)

• **Exploración automática de archivos durante el inicio del sistema** (tras la actualización correcta del motor de detección)

Para editar la configuración de una tarea programada existente (ya sea predeterminada o definida por el usuario), haga clic con el botón secundario en la tarea y luego en **Editar** o seleccione la tarea que quiere modificar y haga clic en el botón **Editar**.



Agregar una nueva tarea

1. Haga clic en **Agregar tarea** en el sector inferior de la ventana.

2. Ingrese el nombre de la tarea.

3. Seleccione la tarea deseada desde el menú desplegable:

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

• **Mantenimiento de registros**: los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.

• **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.

• **Crear una instantánea de estado del equipo**: crea una instantánea del equipo de ESET SysInspector, que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores,

aplicaciones) y evalúa el nivel de riesgo de cada componente.

- **Exploración del equipo a pedido**: realiza una exploración del equipo de los archivos y las carpetas de su equipo.

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

4. Habilite el interruptor junto a **Habilitado** para activar la tarea (puede hacerlo luego al seleccionar/anular la selección de 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 realizará en la fecha y a la hora predefinidas.

- **Reiteradamente** – la tarea se realizará con el intervalo de tiempo especificado.

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

- **Semanalmente** – la tarea se ejecutará en el día y a la hora especificados.

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

5. Seleccione **Omitir tarea al ejecutar con alimentación de la batería** para reducir los recursos del sistema mientras un equipo portátil se ejecuta con alimentación de la batería. La tarea se ejecutará en la fecha y hora especificadas en los campos de **Ejecución de la tarea**. Si la tarea no se pudo ejecutar en el momento predefinido, puede especificar cuándo se realizará nuevamente:

- **A la próxima hora programada**

- **Lo antes posible**

- **Inmediatamente, si la hora 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 la hora con el siguiente control de giro.

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 exploración programada

En esta ventana, puede especificar opciones avanzadas para una tarea de exploración programada del equipo.

Para ejecutar una exploración sin acciones de limpieza, haga clic en **Configuración avanzada** y seleccione **Explorar sin limpieza**. El historial de la exploración se guarda en el registro de la exploración.

Cuando se encuentra seleccionado **Ignorar exclusiones**, los archivos con extensiones que solían ser excluidas de la exploración serán analizadas sin excepción.

El menú desplegable **Acción después de la exploración** permite establecer una acción que se realice automáticamente tras finalizar una exploración:

- **Sin acción** – después de la finalización de la exploración, no se llevará a cabo ninguna acción.

- **Apagar** – el equipo se apaga después de la finalización de la exploración.

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

- **Reiniciar** – cierra todos los programas abiertos, y reinicia el equipo luego de la finalización de la exploración.

- **Reiniciar si es necesario**: el equipo fuerza el reinicio solo si es necesario para completar la limpieza de las amenazas detectadas.

- **Forzar reinicio**: fuerza el cierre de todos los programas abiertos sin esperar la intervención del usuario y reinicia el equipo cuando finaliza la exploración.

- **Suspender**– guarda su sesión y pone el equipo en un estado de energía baja para que pueda volver a trabajar rápidamente.

- **Hibernar**– toma todo lo que se está ejecutando en la memoria RAM y lo envía a un archivo especial de su disco duro. Su equipo se apaga, pero reanudará su estado anterior la próxima vez que lo inicie.

> Las acciones **Suspender** o **Hibernar** están disponibles en función de la configuración de Activar o Hibernar del sistema operativo o de las capacidades de su equipo/computadora portátil. Tenga en cuenta que un equipo en suspensión aún es un equipo en funcionamiento. Sigue ejecutando funciones básicas y utilizando electricidad cuando el equipo funciona con la alimentación de la batería. Para preservar la vida útil de la batería, como cuando viaja fuera de su oficina, recomendamos utilizar la opción Hibernar.

La acción seleccionada comenzará tras la finalización de las exploraciones en ejecución. Cuando seleccione **Apagar** o **Reiniciar**, aparecerá un cuadro de diálogo de confirmación con una cuenta regresiva de 30 segundos (haga clic en **Cancelar** para desactivar la acción solicitada).

Seleccione **No se puede cancelar la exploración** para denegarles a los usuarios sin privilegios la capacidad de detener las medidas tomadas luego de la exploración.

Seleccione la opción **El usuario puede pausar la exploración durante (min.)** si desea permitir que el usuario limitado pause la exploración del equipo durante un periodo especificado.

Consulte también Progreso de la exploración.

Resumen general de tareas programadas

Esta ventana de diálogo muestra información detallada acerca de la tarea programada seleccionada cuando hace doble clic en una tarea personalizada o clic derecho en una tarea programada personalizada y, luego, clic en **Mostrar detalles de la tarea**.

Detalles de tarea

Escriba el **Nombre de la tarea**, seleccione una de las opciones del **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 remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.

• **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.

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

• **Exploración del equipo a pedido**: realiza una exploración del equipo de los archivos y las carpetas de su equipo.

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

Programación de tarea

La tarea se realizará reiteradamente en el intervalo de tiempo especificado. Seleccione una de las opciones de programación:

• **Una vez**: la tarea se realizará una sola vez, en la fecha y a la hora predefinidas.

• **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado (en horas).

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

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

• **Cuando se cumpla la condición**: la tarea se ejecutará luego de un suceso especificado.

Omitir tarea al ejecutar con alimentación de la batería: la tarea no se ejecutará si su equipo recibe alimentación de la batería en el momento en que la tarea debería iniciarse. Esto también es así en los equipos que reciben alimentación de un SAI.

Sincronización de la tarea: una vez

Ejecución de la tarea: la tarea especificada se ejecutará una sola vez en la fecha y a la 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 horarios seleccionados.

Sincronización de la tarea: desencadenada por un suceso

La tarea se accionará por uno de los siguientes sucesos:

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

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

Omisión de una tarea

Una tarea se puede omitir cuando el equipo está funcionando con baterías o si está desconectado. Seleccione cuándo debería ejecutarse la tarea entre una de estas opciones y haga clic en **Siguiente**:

- **En la siguiente hora programada**: la tarea se ejecutará si el equipo está activado en la siguiente hora programada.
- **Lo antes posible**: la tarea se ejecutará cuando el equipo esté activado.
- **Inmediatamente, si la hora 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.

De inmediato, en caso de que se supere el tiempo establecido desde la última ejecución programada (en horas) – ejemplos

Se configura una tarea de ejemplo para que se ejecute reiteradamente cada hora. La opción **Inmediatamente, si la hora desde la última ejecución programada excede (horas)** se selecciona y el tiempo superado se establece en dos horas. La tarea se ejecuta a las 13:00 y, cuando finaliza, el equipo queda en suspensión:

- El equipo se reactiva 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 equipo se reactiva 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: actualizar

Si desea actualizar el programa desde dos servidores de actualización, será necesario crear dos perfiles de actualización diferentes. Si el primero no logra descargar los archivos de actualización, el programa cambia automáticamente al perfil alternativo. Esto es conveniente, por ejemplo, para equipos portátiles, que suelen actualizarse desde un servidor de actualización de la red de área local, pero cuyos dueños normalmente se conectan a Internet por medio de otras redes. Por lo tanto, si falla el primer perfil, el segundo descargará automáticamente los archivos de actualización desde los servidores de actualización de ESET.

Detalles de la tarea: ejecutar aplicación

En esta tarea se programa la ejecución de una aplicación externa.

Archivo ejecutable – elija un archivo ejecutable desde el árbol del directorio, haga clic en la opción **...** e ingrese la ruta en forma manual.

Carpeta de trabajo – defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **Archivo ejecutable** seleccionado se crearán dentro de este directorio.

Parámetros – parámetros de la línea de comandos de la aplicación (opcional).

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

Limpiador de sistema

El limpiador del sistema es una herramienta que lo ayuda a restaurar el equipo a un estado utilizable luego de eliminar la amenaza. El malware puede desactivar utilidades como el Editor de registro, el Administrador de tareas o las Actualizaciones de Windows. El limpiador de sistema restaura los valores predeterminados y las configuraciones para un sistema determinado con un solo clic.

El limpiador de sistema informa problemas de cinco categorías de configuración:

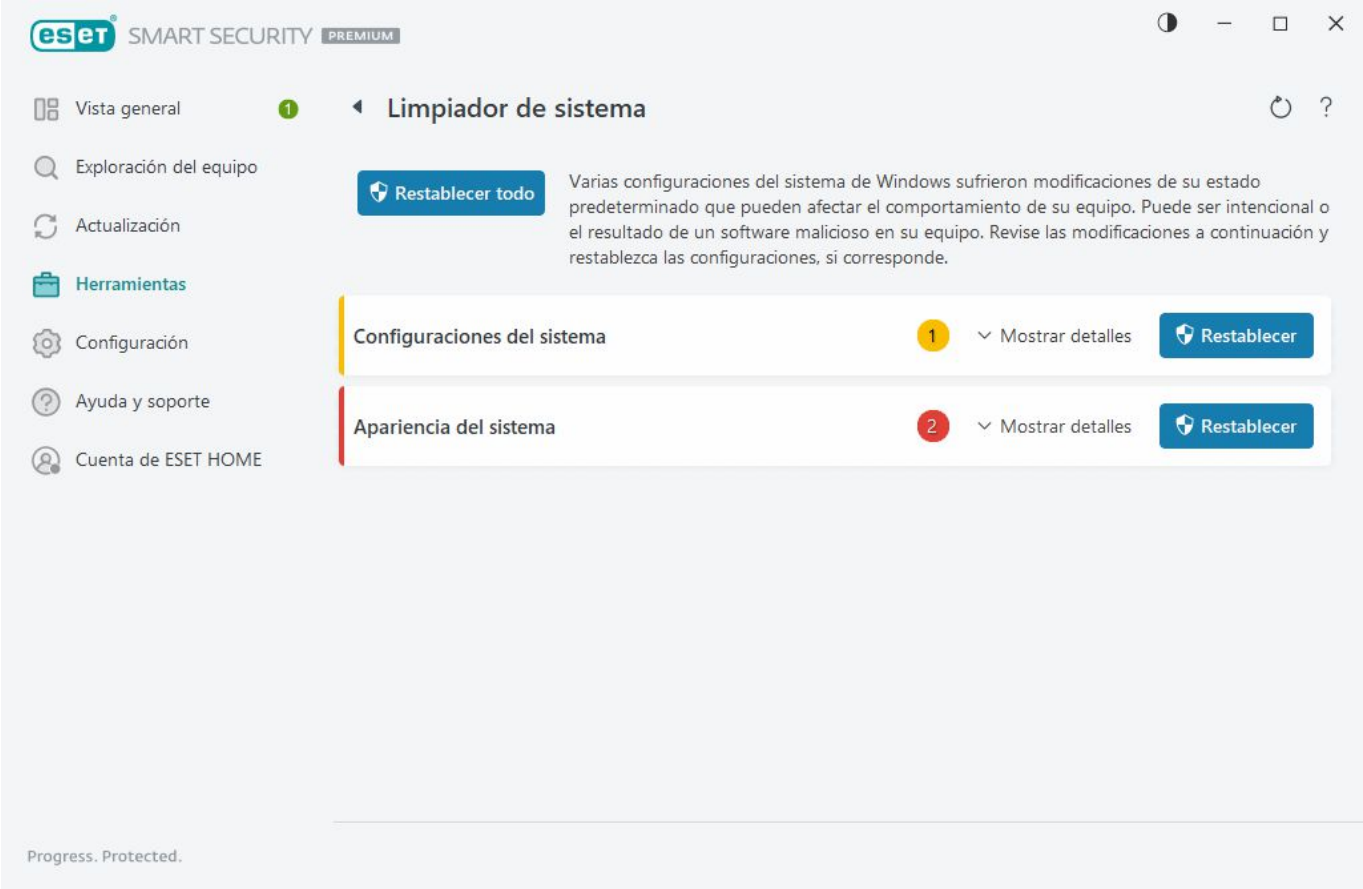
- **Configuración de seguridad**: cambios en la configuración que pueden causar una mayor vulnerabilidad de su equipo, como actualizaciones de Windows.
- **Configuración del sistema**: cambios en la configuración del sistema que pueden cambiar el comportamiento de su equipo, como asociaciones de archivos.
- **Aspecto del sistema**: configuración que afecta el aspecto de su sistema, como su fondo de escritorio.
- **Funciones desactivadas**: funciones importantes y aplicaciones que pueden estar deshabilitadas.
- **Restauración del sistema de Windows**: configuraciones para la función Restaurar sistema de Windows, que le permite restaurar su sistema a un estado anterior.

Se puede solicitar la limpieza del sistema:

- cuando se encuentra una amenaza

- cuando un usuario hace clic en **Restablecer**

Puede revisar los cambios y restablecer las configuraciones si fuese necesario.



Solo un usuario con derechos de administrador puede realizar acciones en el Limpiador del sistema.

Inspector de red

Inspector de red puede ayudar a identificar vulnerabilidades en la red confiable (red doméstica o red de oficina) (por ejemplo, puertos abiertos o una contraseña de router débil). También le brinda una lista de dispositivos conectados, categorizados por tipo de dispositivo (por ejemplo, impresora, router, dispositivo móvil, etc.) para mostrar qué está conectado a su red (por ejemplo, consolas de videojuegos, dispositivos de IoT u otros dispositivos inteligentes del hogar).

Inspector de red le ayuda a identificar las vulnerabilidades de un enrutador y aumenta el nivel de protección cuando se conecta con una red.

El Inspector de red no reconfigura el router por usted. Usted mismo hará los cambios mediante la interfaz especializada de su router. Los routers domésticos pueden ser muy vulnerables al malware que se usa para el lanzamiento de ataques de denegación distribuida de servicio (DDoS). Si el usuario no ha cambiado la contraseña del router de la predeterminada, es fácil de adivinar para los piratas informáticos, quienes luego pueden iniciar sesión en su router y reconfigurarlo o poner en peligro su red.

Recomendamos encarecidamente que cree una contraseña fuerte que sea lo suficientemente larga e incluya números, símbolos o letras mayúscula. Para que la contraseña sea más difícil de romper, utilice una mezcla de diferentes tipos de caracteres.

Si la red a la que está conectado está configurada como confiable, 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 todo ESET Security Ultimate a fin de 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 con información básica en una vista de lista. Haga clic en el dispositivo específico para editar el dispositivo o ver su 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 específica
- Dispositivos conectados a **Todas las redes**
- Dispositivos sin categoría

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

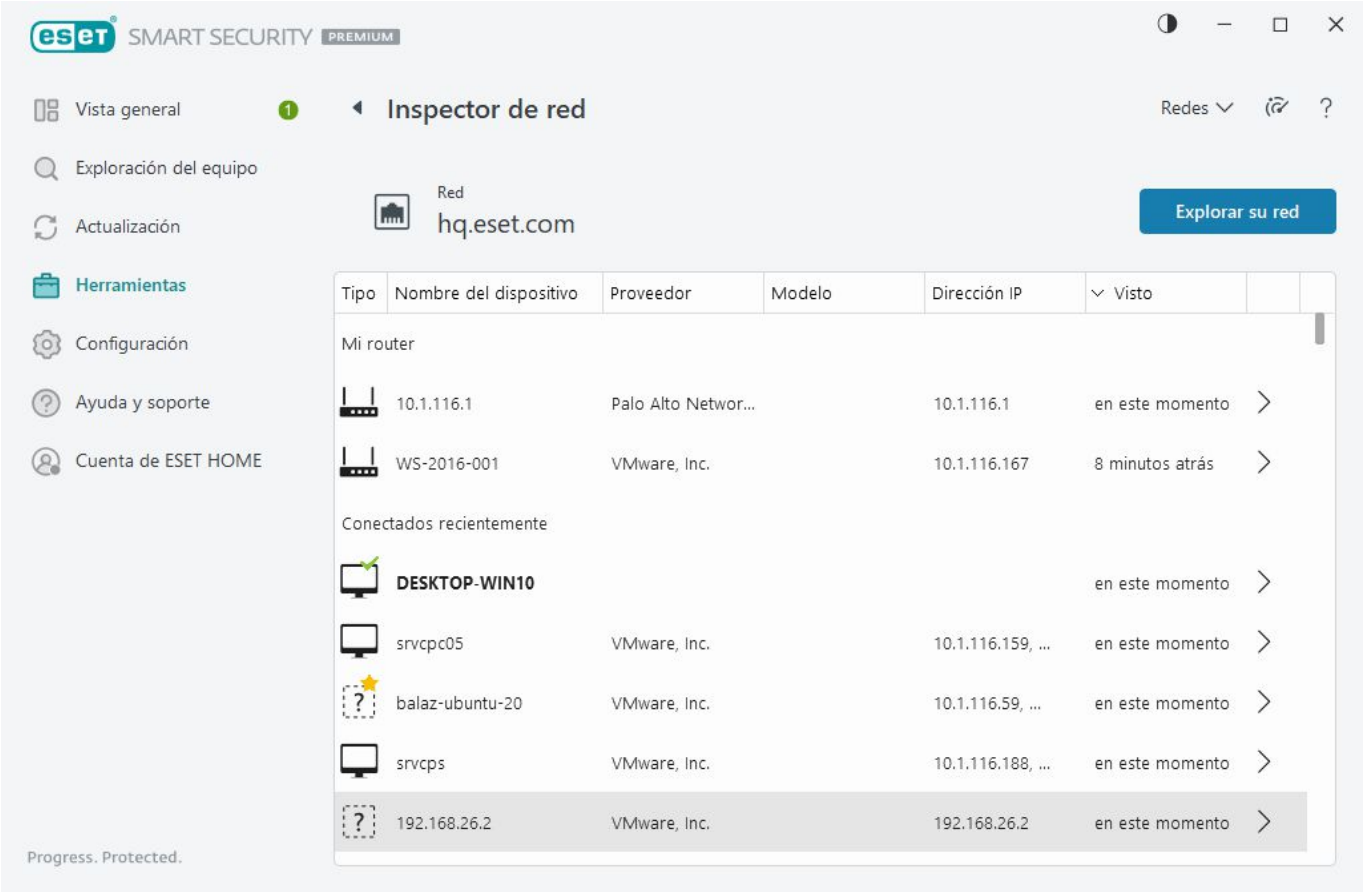
Haga clic en la rueda dentada ⚙ ubicada en la esquina superior derecha para seleccionar si desea notificar cuando se detecte un nuevo dispositivo en la red.

Haga clic en **Explorar la red** para realizar una exploración manual de la red a la que está conectado. **Explorar la red** solo está disponible para una red confiable. Consulte Perfiles de conexión de red para revisar o editar la configuración de red.

Puede elegir entre las siguientes opciones de exploración:

- Escanear todo
- Escanear solo router
- Escanear solo dispositivos

⚠ Realice exploraciones de red solo en redes confiables. Si lo hace en red no confiable, podría ser peligroso.



Una vez finalizada la exploración, se mostrará una notificación con un enlace a la información básica del dispositivo o puede hacer doble clic en el dispositivo sospechoso en la vista de lista o sonar. Haga clic en **Resolución de problemas** para ver las comunicaciones recientemente bloqueadas. Más información sobre la resolución de problemas con el cortafuegos.

Existen dos tipos de notificaciones que muestra el módulo del Inspector de red:

- **Nuevo dispositivo conectado a la red**: se muestra si un dispositivo desconocido se conecta a la red mientras el usuario está conectado.
- **Se encontraron nuevos dispositivos de red**: se muestra si se vuelve a conectar a su red confiable y hay un dispositivo desconocido.

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

¿Qué significan los íconos en los dispositivos del Inspector de red?

	El ícono de estrella amarilla indica que los dispositivos son nuevos en la red o que ESET los ha detectado por primera vez.
	El ícono de precaución amarillo indica que es posible que su enrutador presente vulnerabilidades. Haga clic en el ícono del producto para obtener información más detallada sobre el problema.
	El ícono de precaución rojo les indica a los dispositivos que su enrutador presenta vulnerabilidades y podría estar infectado. Haga clic en el ícono del producto para obtener información más detallada sobre el problema.

El ícono azul puede aparecer cuando su producto ESET contiene información adicional para su enrutador, pero no requiere de atención inmediata porque no hay riesgos de seguridad presentes. Haga clic en el ícono del producto para obtener información más detallada.

Dispositivo de red en el Inspector de red

Aquí puede encontrar información detallada sobre el dispositivo, incluidos los siguientes:

- Nombre del dispositivo
- Tipo de dispositivo
- Última vez visto
- Nombre de la red
- Dirección IP
- Dirección MAC
- Sistema operativo

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

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 este 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 interfaz del router**. Si posee un router que proporcionó su proveedor de servicios de Internet, tal vez deba comunicarse con el servicio de soporte de su proveedor de servicios de Internet o del fabricante del router para resolver los problemas de seguridad detectados. Siga siempre las medidas de seguridad adecuadas según se indican en la guía de usuario del router.
Protección Para proteger su router y red de ataques a la ciberseguridad, siga estas recomendaciones básicas.

Dispositivo de red

Identificación del dispositivo: si no está seguro acerca del dispositivo conectado a su red, verifique el nombre del proveedor o fabricante debajo del nombre del dispositivo. Puede ayudarle a identificar qué tipo de dispositivo es. Puede cambiar el nombre del dispositivo para referencia futura.
Desconexión del dispositivo: si no está seguro de que un dispositivo conectado es seguro para sus dispositivos o la red, administre el acceso a la red para este dispositivo en la configuración del router o cambie la contraseña de su red.
Protección: para proteger su dispositivo contra ataques y software malicioso, instale la protección de ciberseguridad en su dispositivo y siempre mantenga actualizados su sistema operativo y el software instalado. Para permanecer protegido, no se conecte a redes Wi-Fi no seguras.

Este dispositivo

Este dispositivo representa su equipo en la red.
Adaptadores de red: muestra la información de sus adaptadores de red.

Notificaciones | Inspector de red

Las siguientes son varias notificaciones que pueden mostrarse cuando ESET Security Ultimate detecta algún problema de vulnerabilidad en el router. Cada notificación contiene una descripción breve y provee una solución o pasos que deben seguirse para minimizar el riesgo de vulnerabilidad del router. Si no está familiarizado con los cambios de router, le recomendamos que se ponga en contacto con el fabricante del router o con el proveedor de internet.

Se encontró una posible vulnerabilidad
Es posible que el router contenga vulnerabilidades conocidas que podrían facilitar su ataque y explotación. Actualice el firmware del router.

Se encontró una vulnerabilidad
El router contiene vulnerabilidades conocidas que facilitan su ataque y explotación. Actualice el firmware del router.

Amenaza detectada
El router está infectado con malware. Reinicie el equipo y repita la exploración.

La contraseña del router es débil
La contraseña del router es insegura y cualquier persona puede adivinarla. Cambie la contraseña del router.

Redirección de red maliciosa
El tráfico de Internet parece ser redireccionado a sitios Web maliciosos. Esto podría significar que el enrutador esté comprometido. Cambie la configuración del servidor DNS del router.

Servicios de red abierta
El enrutador ejecuta servicios de red que podrían ser explotados por otros. Esto puede deberse a una configuración deficiente o un enrutador comprometido. Verifique la configuración del router.

Servicios de red abierta sensibles
El enrutador ejecuta servicios de red sensibles que podrían ser explotados por otros. Esto puede deberse a una configuración deficiente o un enrutador comprometido. Verifique la configuración del router.

Firmware desactualizado
El firmware del router está desactualizado y puede contener vulnerabilidades. Actualice el firmware del router.

Configuración de router maliciosa
Este servidor DNS que utiliza es malicioso y puede enviarlo a sitios Web peligrosos. Esto podría significar que el enrutador esté comprometido. Cambie la configuración del servidor DNS del router.

Servicios de red
El enrutador ejecuta servicios de red comunes. Son necesarios para la red y probablemente sean seguros. Verifique la configuración del router.

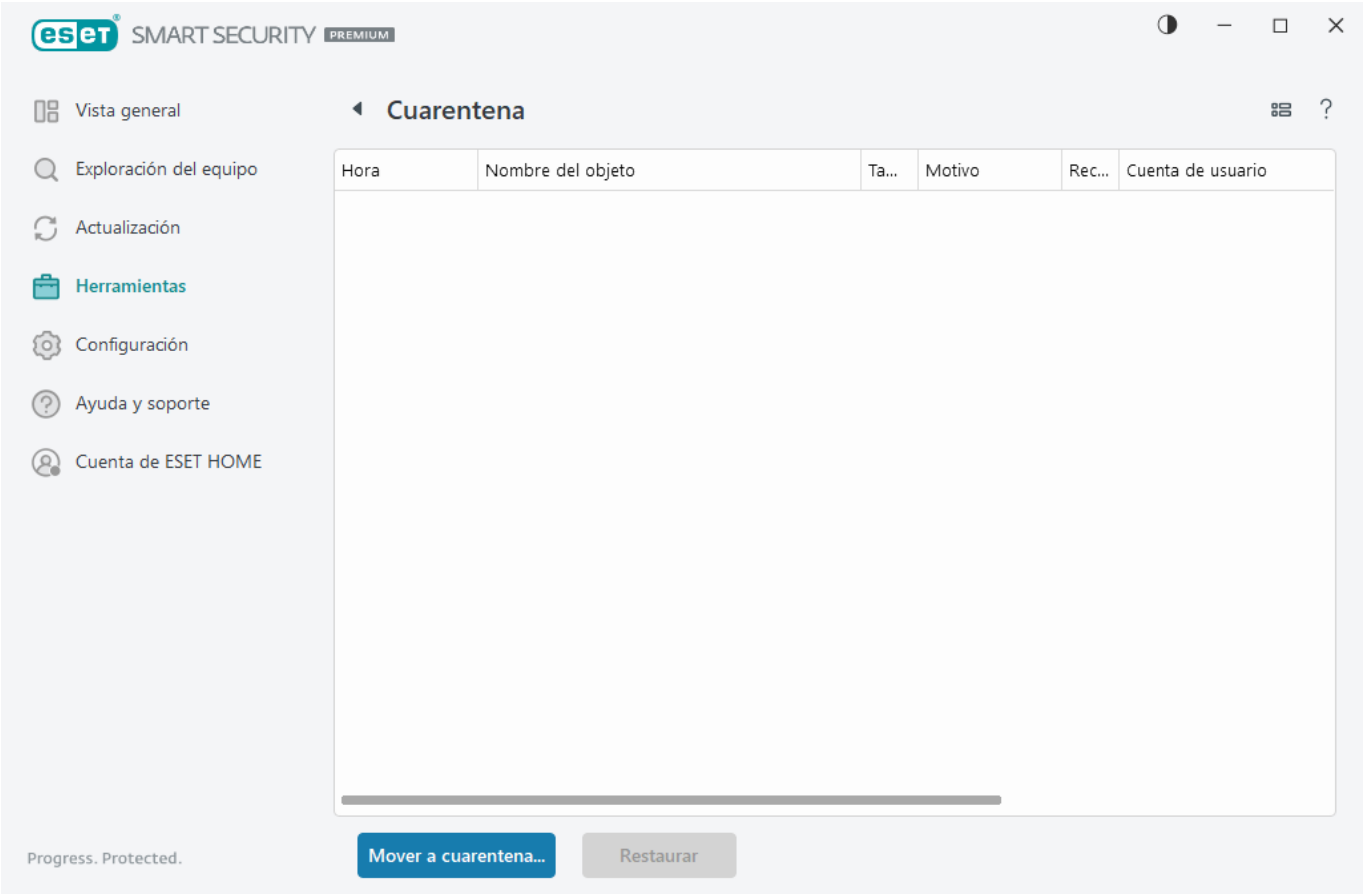
Cuarentena

La principal función de la cuarentena es almacenar de forma segura los objetos informados (como malware, archivos infectados o aplicaciones potencialmente no deseadas).

Para acceder a la cuarentena, diríjase a la ventana principal del programa ESET Security Ultimate y haga clic en **Herramientas** > **Cuarentena**.

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

- la fecha y la hora en que se pusieron en cuarentena,
- la ruta a la ubicación original del archivo,
- su tamaño en bytes,
- el motivo (por ejemplo, objeto agregado por el usuario),
- y la cantidad de amenazas (por ejemplo, detecciones duplicadas del mismo archivo o si un archivo contiene varias infiltraciones).



Envío de archivos a cuarentena

ESET Security Ultimate dispone los archivos eliminados en cuarentena de manera automática (si usted no canceló esta opción en la ventana de alerta).

Los archivos adicionales deberían ponerse en cuarentena si:

a.no pueden limpiarse,

b.no es seguro o recomendable eliminarlos,

c.ESET Security Ultimate los detecta de manera falsa,

d.o si un archivo presenta un comportamiento sospechoso pero Protecciones no lo detecta.

Para poner un archivo en cuarentena, cuenta con varias opciones:

a.Use la función Arrastrar y soltar para poner un archivo en cuarentena manualmente al hacer clic en el archivo, mover el puntero del mouse hacia el área marcada al mismo tiempo que mantiene el botón pulsado, y luego lo suelta. Después de eso, la aplicación se mueve al primer plano.

b.Haga clic derecho en el archivo > haga clic en **Opciones avanzadas** > **Archivo en cuarentena**.

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

d.También puede usarse el menú contextual para este fin. Haga clic con el botón secundario en la ventana **Cuarentena** y seleccione **Cuarentena**.

Restauración desde Cuarentena

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

- Para tal fin, use la función **Restaurar**, que se encuentra disponible en el menú contextual, al hacer clic con el botón secundario en un archivo específico en Cuarentena.

- Si un archivo está marcado como aplicación potencialmente no deseada, se habilita la opción **Restaurar y excluir de la exploración**. Consulte también Exclusiones.

- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar un archivo de una ubicación que no sea aquella en la que se lo eliminó.

- La funcionalidad de restauración no se encuentra disponible en algunos casos, por ejemplo, para archivos ubicados en una unidad de uso compartido de solo lectura.

Eliminar de la cuarentena

Haga clic con el botón secundario en un elemento determinado y seleccione **Eliminar de la Cuarentena**, o seleccione el elemento que desea eliminar y presione **Eliminar** en su teclado. Si desea seleccionar y eliminar todos los elementos de Cuarentena, puede presionar **Ctrl + A** y luego **Delete** en el teclado. Los elementos eliminados se eliminarán en forma permanente de su dispositivo y cuarentena.

Envío de un archivo desde cuarentena

Si puso en cuarentena un archivo sospechoso que el programa no detectó o si un archivo se determinó erróneamente como infectado (por ejemplo, tras la exploración heurística del código) y luego se puso en cuarentena, envíe el archivo al laboratorio de amenazas de ESET. Para enviar un archivoa, haga un clic derecho en el archivo y seleccione **Enviar para su análisis** desde el menú contextual.

Descripción de la detección

Haga clic derecho en un elemento y 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 ilustradas

Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- Restaurar un archivo en cuarentena en ESET Security Ultimate
- Eliminar un archivo en cuarentena en ESET Security Ultimate
- Mi producto ESET me envió una notificación sobre una detección. ¿Qué debo hacer?

Error en la cuarentena

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

- **No tiene los permisos de lectura:** significa que no puede ver el contenido de un archivo.
- **No tiene los 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:** debe reducir el tamaño del archivo.

Cuando reciba el mensaje de error "Ha fallado la 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 el archivo no puede ponerse en cuarentena.

Seleccionar muestra para su análisis

Si encuentra un archivo de conducta sospechosa en su equipo o un sitio sospechoso en Internet, puede enviarlo al laboratorio de investigación de ESET para su análisis (es posible que no esté disponible según la configuración de ESET LiveGrid® que usted tenga).

Antes de enviar muestras a ESET

No envíe una muestra excepto que cumpla con, al menos, uno de los siguientes criterios:

- Su producto ESET no detecta la muestra en absoluto
- El programa detecta erróneamente la muestra como una amenaza
- No aceptamos sus archivos personales (aquellos que le gustaría que ESET explore para detectar malware) como muestras (el Laboratorio de investigación de ESET no realiza exploraciones a pedido de los usuarios)
- Recuerde utilizar un tema descriptivo e incluir la mayor cantidad de información posible sobre el archivo (por ejemplo, una captura de pantalla o el sitio Web desde donde realizó la descarga).

Puede realizar el envío de una muestra (un archivo o un sitio web) para que ESET lo analice por medio de uno de estos métodos:

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

2. Como alternativa, puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima el archivo utilizando WinRAR/WinZIP, proteja el archivo con la contraseña “infected” y envíelo a samples@eset.com.

3. Para denunciar spam, falsos positivos de spam o sitios web mal categorizados por el módulo de control parental, consulte nuestro artículo incluido en la base de conocimientos de ESET.

En el formulario **Seleccionar muestra para su análisis**, seleccione la descripción del menú desplegable **Motivo por**

el cual se envía la muestra que mejor se adapte a su mensaje:

- Archivo sospechoso
- Sitio sospechoso (un sitio web que se encuentra infectado por algún malware),
- Sitio falso positivo
- Archivo falso positivo (un archivo que se detecta como una infección pero no está infectado),
- Otro

Archivo/sitio – la ruta al archivo o sitio web que desea enviar.

Correo electrónico de contacto – el correo electrónico de contacto se envía junto con los archivos sospechosos a ESET y puede utilizarse para contactarlo en caso de que se requiera información adicional para el análisis. El ingreso del correo electrónico de contacto es opcional. Seleccione **Enviar de manera anónima** para dejarlo vacío.

> **Es posible que no obtenga respuesta de ESET.**
> No obtendrá una respuesta de ESET a menos que se requiera más información. Ya que nuestros servidores reciben decenas de miles de archivos por día, lo que hace imposible responder a todos los envíos.
> Si la muestra resulta ser una aplicación maliciosa o sitio malicioso, se agregará su detección a una de las próximas actualizaciones de ESET.

Seleccionar muestra para su análisis: archivo sospechoso

Signos y síntomas observados de infección de malware – ingrese una descripción sobre la conducta de los archivos sospechosos observada en el equipo.

Origen del archivo (dirección URL o proveedor): ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Notas e información adicional – aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

> Aunque solo el primer parámetro, **Signos y síntomas observados de infección de malware**, es obligatorio, el suministro de información adicional ayudará en forma significativa a nuestros laboratorios en la etapa de identificación y en el procesamiento de muestras.

Seleccionar muestra para su análisis: sitio sospechoso

Seleccione uno de los siguientes del menú desplegable **Problemas del sitio**:

- **Infectado** – un sitio web que contiene virus u otro malware distribuidos por varios métodos.
- El **phishing** utilizarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, PIN, etc. Lea más información sobre este tipo de ataque en el glosario.

- **Fraudulento** – un sitio web fraudulento o engañoso, especialmente para obtener una ganancia rápida.
- Seleccione **Otro** si las opciones mencionadas previamente no se aplican al sitio que va a enviar.

Notas e información adicional – aquí puede agregar información adicional o una descripción que ayudarán a analizar el sitio web sospechoso.

Seleccionar muestra para su análisis: archivo con falso positivo

Le solicitamos que envíe los archivos detectados como una infección pero que no se encuentran infectados para mejorar nuestro motor antivirus y antispyware y ayudar a otros a estar protegidos. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en un motor de detección.

Nombre y versión de la aplicación – el título del programa y su versión (por ejemplo, número, alias o nombre del código).

Origen del archivo (dirección URL o proveedor) – ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Propósito de la aplicación – la descripción general de la aplicación, el tipo de aplicación (por ej., navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional – aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

> Los primeros tres parámetros son obligatorios para identificar aplicaciones legítimas y distinguirlas del código malicioso. Al proporcionar información adicional, ayudará significativamente a nuestros laboratorios en el proceso de identificación y en el procesamiento de las muestras.

Seleccionar muestra para su análisis: sitio de falso positivo

Le solicitamos que envíe los sitios que se detectan como infectados, fraudulentos o phishing pero no lo son. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en un motor de detección. Envíenos esta página web para mejorar nuestro motor antivirus y antiphishing y ayudar a proteger a los demás.

Notas e información adicional: aquí puede agregar información adicional o descripciones útiles que ayudarán durante el procesamiento del sitio web sospechoso.

Seleccionar muestra para su análisis: otros

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

Motivo por el cual se envía el archivo – ingrese una descripción detallada y el motivo por el cual envía el archivo.

Configuración

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

El menú **Configuración** se divide en los siguientes grupos:

Protección del equipo

Protección de Internet

Protección de la red

Herramientas de seguridad

Hay opciones adicionales disponibles en la parte inferior de la ventana de configuración. Haga clic en Configuración avanzada para configurar parámetros más detallados para cada módulo. Para cargar los parámetros de configuración mediante un archivo de configuración .xml o para guardar los parámetros de configuración actuales en un archivo de configuración, use la opción Importar/Exportar configuraciones.

Protección del equipo

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

- Protección del sistema de archivos en tiempo real – Se exploran todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan.
- ESET LiveGuard: agrega una capa de protección en la nube diseñada específicamente para mitigar amenazas nunca vistas.
- Protección proactiva: bloquea la ejecución de archivos nuevos hasta que se reciben los resultados del análisis de ESET LiveGuard. Si desea desbloquear el archivo que se está analizando, haga clic derecho en el archivo y, a continuación, haga clic en **Desbloquear archivo analizado por ESET LiveGuard**.
- Control de dispositivos: este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y seleccionar la forma en que el usuario puede acceder y utilizar un dispositivo determinado (CD/DVD/USB...).
- HIPS: HIPS monitorea los sucesos dentro del sistema operativo y reacciona a ellos según un grupo de reglas personalizado.
- Modo de juego: habilita o deshabilita el Modo de juego. Tras habilitar el modo de juego, recibirá un mensaje de advertencia (riesgo potencial en la seguridad) y la ventana principal se pondrá de color naranja.
- Protección de la cámara Web: controla los procesos y las aplicaciones que acceden a la cámara.

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de interruptor  .

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

Haga clic en el icono del engranaje junto a un módulo de protección para acceder a las configuraciones avanzadas de dicho módulo.

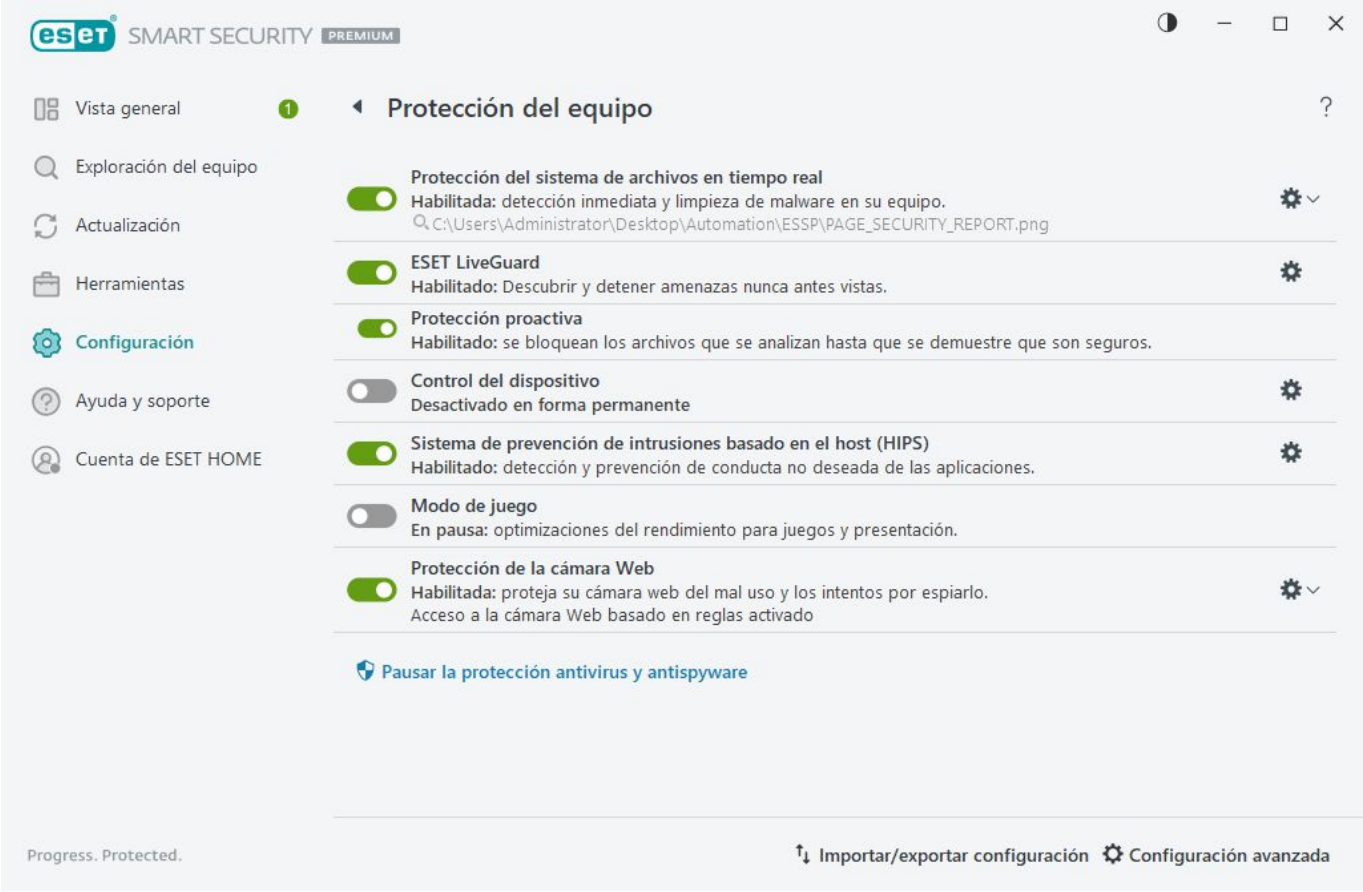
Para la **protección del sistema de archivos en tiempo real**, haga clic en el ícono del engranaje y elija una de las siguientes opciones:

- **Configurar:** abre la Configuración avanzada de la protección del sistema de archivos en tiempo real.
- **Editar exclusiones:** abre la ventana Configuración de exclusiones para poder excluir archivos y carpetas de la exploración.

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

- **Configurar:** abre la configuración avanzada de la protección de la cámara web.
- **Bloquear todo el acceso hasta el reinicio:** bloquea todo el acceso a la cámara web hasta el reinicio del equipo.
- **Bloquear todo el acceso de forma permanente:** bloquea todo el acceso a la cámara web hasta que se desactiva esta configuración.

• **Detener bloqueo de todo el acceso**: desactiva la capacidad de bloquear el acceso a la cámara web. Esta opción solo está disponible si se bloquea el acceso a la cámara web.



Pausar la protección antivirus y antispyware: deshabilita todos los módulos de protección antivirus y antispyware. Al deshabilitar la protección, se abrirá una ventana donde puede determinar durante cuánto tiempo se encontrará deshabilitada la protección mediante el menú desplegable **Intervalo temporal**. Solo use esta opción si es un usuario experimentado o si se lo indica el soporte técnico de ESET.

Infiltración detectada

Las infiltraciones pueden llegar al sistema desde diversos puntos de entrada, como páginas Web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, etc.).

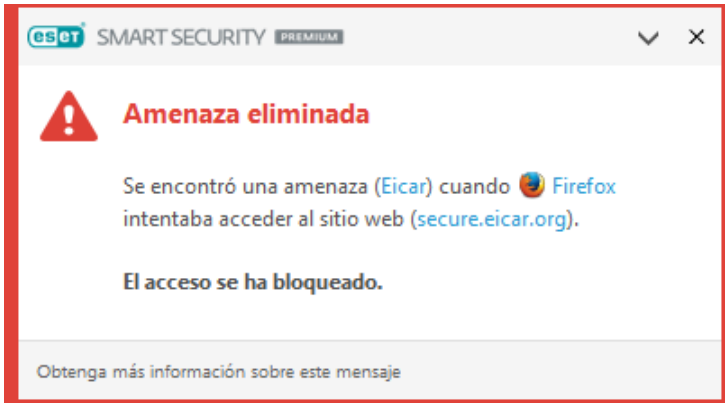
Conducta estándar

Como ejemplo general de la forma en que ESET Security Ultimate maneja las infiltraciones, las infiltraciones se pueden detectar mediante:

- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección del cliente de correo electrónico
- Exploración del equipo a petición

Cada uno utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o

finalizar la conexión. Una ventana de notificación se muestra en el área de notificaciones en la esquina inferior derecha de la pantalla. Para obtener información detallada sobre los objetos detectados/desinfectados, consulte Archivos de registro. Para obtener más información sobre los niveles de desinfección y conducta, consulte Nivel de desinfección.



Explorando el equipo para detectar archivos infectados

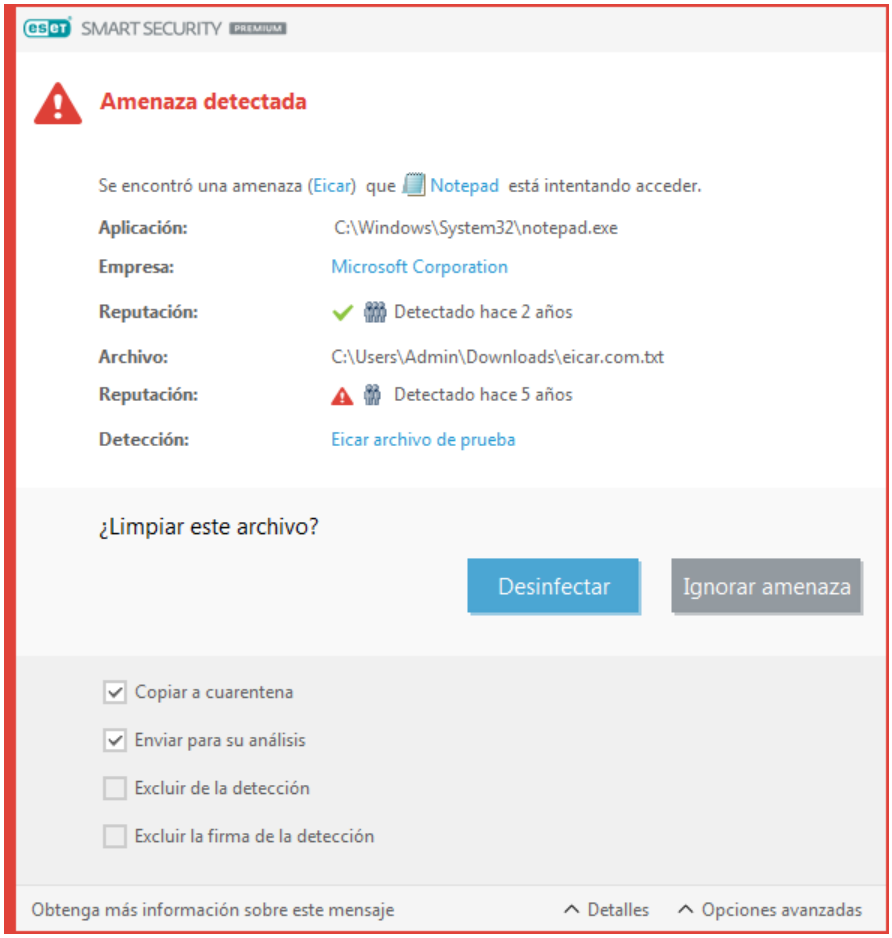
Si su equipo muestra signos de infección por malware, por ej., funciona más lento, con frecuencia no responde, etc., se recomienda hacer lo siguiente:

1. Abra ESET Security Ultimate y haga clic en **Exploración del equipo**.
2. Haga clic en **Explorar el equipo** (para obtener más información, consulte en Exploración del equipo).
3. Una vez finalizada la exploración, consulte el registro para verificar la cantidad de archivos explorados, infectados y desinfectados.

Si solo quiere explorar una parte determinada del disco, haga clic en **Exploración personalizada** y seleccione los objetos para explorar en busca de virus.

Desinfección y eliminación:

Si no hay ninguna acción predefinida para la protección del sistema de archivos en tiempo real, el programa le pedirá que seleccione una opción en una ventana de alerta. Por lo general están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acción**. No se recomienda seleccionar **Sin acción**, ya que esto dejará los archivos infectados sin desinfectar. La excepción a este consejo es cuando usted está seguro de que un archivo es inofensivo y fue detectado por error.



Aplique la opción de desinfección si un virus atacó un archivo y le adjuntó códigos maliciosos. En este caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo está compuesto exclusivamente por códigos maliciosos, será eliminado.

Si un archivo infectado está “bloqueado” u otro proceso del sistema lo está usando, por lo general se elimina cuando es liberado (normalmente luego del reinicio del sistema).

Restauración desde Cuarentena

Para acceder a la cuarentena, diríjase a la ventana principal del programa ESET Security Ultimate y haga clic en **Herramientas** > **Cuarentena**.

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

- Para tal fin, use la función **Restaurar**, que se encuentra disponible en el menú contextual, al hacer clic con el botón secundario en un archivo específico en Cuarentena.
- Si un archivo está marcado como aplicación potencialmente no deseada, se habilita la opción **Restaurar y excluir de la exploración**. Consulte también Exclusiones.
- El menú contextual también ofrece la opción **Restaurar a**, que le permite restaurar un archivo de una ubicación que no sea aquella en la que se lo eliminó.
- La funcionalidad de restauración no se encuentra disponible en algunos casos, por ejemplo, para archivos ubicados en una unidad de uso compartido de solo lectura.

Varias amenazas

Si algún archivo infectado no se desinfectó durante la exploración del equipo (o el Nivel de desinfección estaba configurado en **Sin desinfección**), se muestra una ventana de alerta que le solicitará seleccionar las acciones para dichos archivos. Seleccione las acciones para los archivos (las acciones se establecen en forma individual para cada archivo de la lista) y luego haga clic en **Finalizar**.

Eliminación de archivos en archivos comprimidos

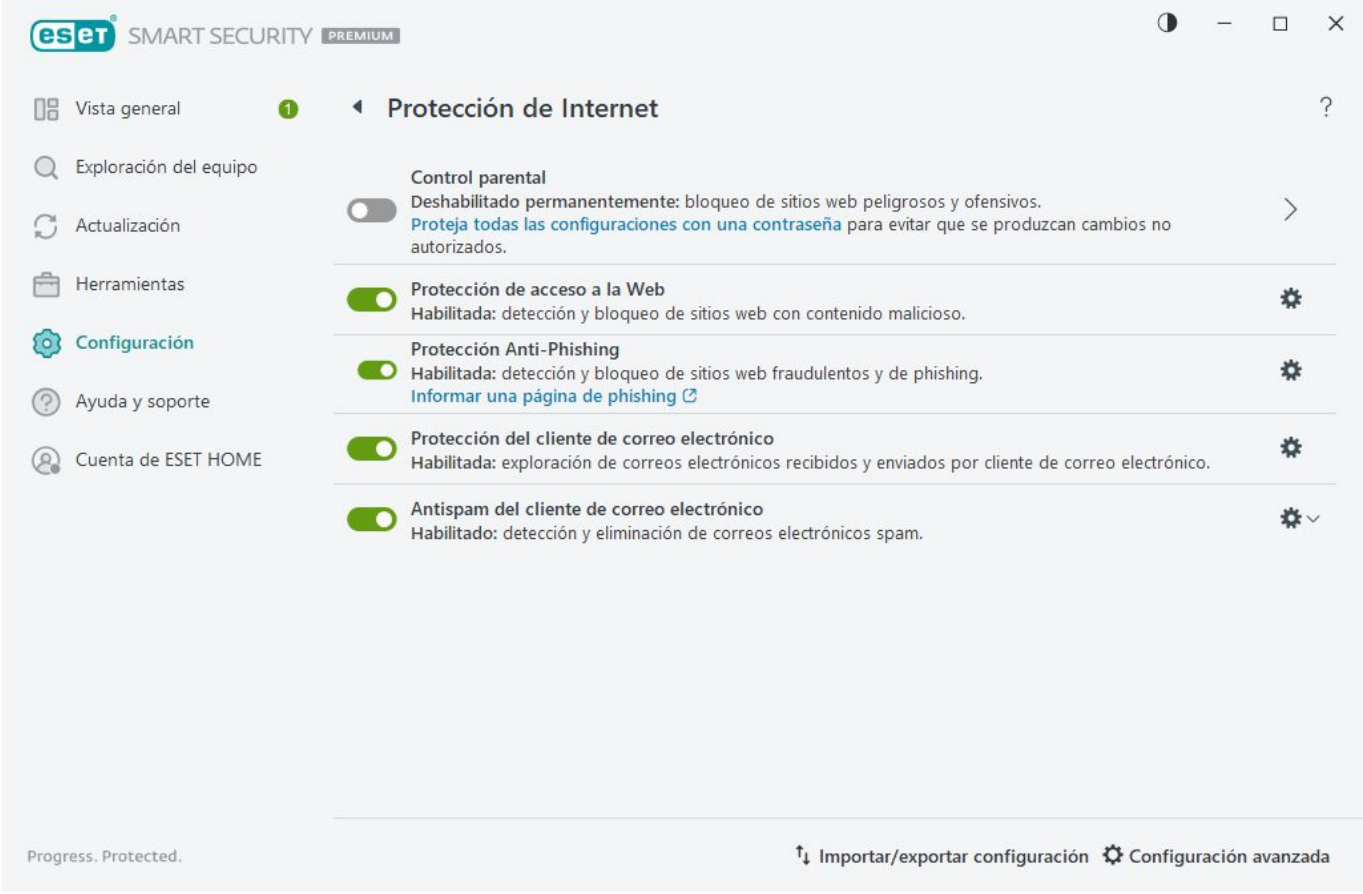
En el modo de desinfección predeterminado, se eliminará el archivo comprimido completo solo si todos los archivos que lo componen están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos inofensivos no infectados. Tenga precaución al realizar una exploración con Desinfección estricta: si la Desinfección estricta está habilitada, un archivo se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.

Protección de Internet

La conectividad a Internet es una función estándar del equipo personal. Lamentablemente, también se convirtió en el medio principal para transferir códigos maliciosos. Abra la ventana del programa principal > **Configuración** > **Protección de Internet** para configurar las características ESET Security Ultimate que aumentan su protección de Internet.

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de interruptor .

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



Haga clic en el icono del engranaje junto a un módulo de protección para acceder a las configuraciones avanzadas de dicho módulo.

El módulo de Control parental protege a sus hijos al bloquear los contenidos inapropiados o dañinos en Internet.

La protección de acceso a la Web explora la comunicación HTTP/HTTPS para detectar malware y phishing. La protección de acceso a la web solo debe desactivarse para solucionar problemas.

Protección antiphishing le permite bloquear las páginas Web conocidas por distribuir contenido phishing. Se recomienda firmemente que deje Anti-Phishing habilitada.

Informar una página de phishing: informa un sitio web malicioso/de phishing a ESET para su análisis.

> Antes de enviar un sitio Web a ESET, asegúrese de que cumpla con uno o más de los siguientes criterios:
> • El programa directamente no detecta el sitio Web.
> • El programa detecta erróneamente el sitio Web como una amenaza. En ese caso, puede Informar una página bloqueada incorrectamente.

Protección del cliente de correo electrónico: proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S). Mediante el complemento del programa para su cliente de correo electrónico, ESET Security Ultimate proporciona el control de todas las comunicaciones desde el cliente de correo electrónico.

El 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 ícono del engranaje y elija una de las siguientes opciones:

- **Configurar** – abre las configuraciones avanzadas para el antispam del cliente de correo electrónico.

- **Lista de direcciones del usuario** (si está activada): abre una ventana de cuadro de diálogo donde puede agregar, editar o eliminar direcciones para definir las reglas antispam. Las reglas de esta lista se aplicarán al usuario actual.

- **Lista de direcciones de direcciones** (si está activada): abre una ventana de cuadro de diálogo donde puede agregar, editar o eliminar direcciones para definir las reglas antispam. Las reglas de esta lista se aplicarán a todos los usuarios.

Protección antiphishing

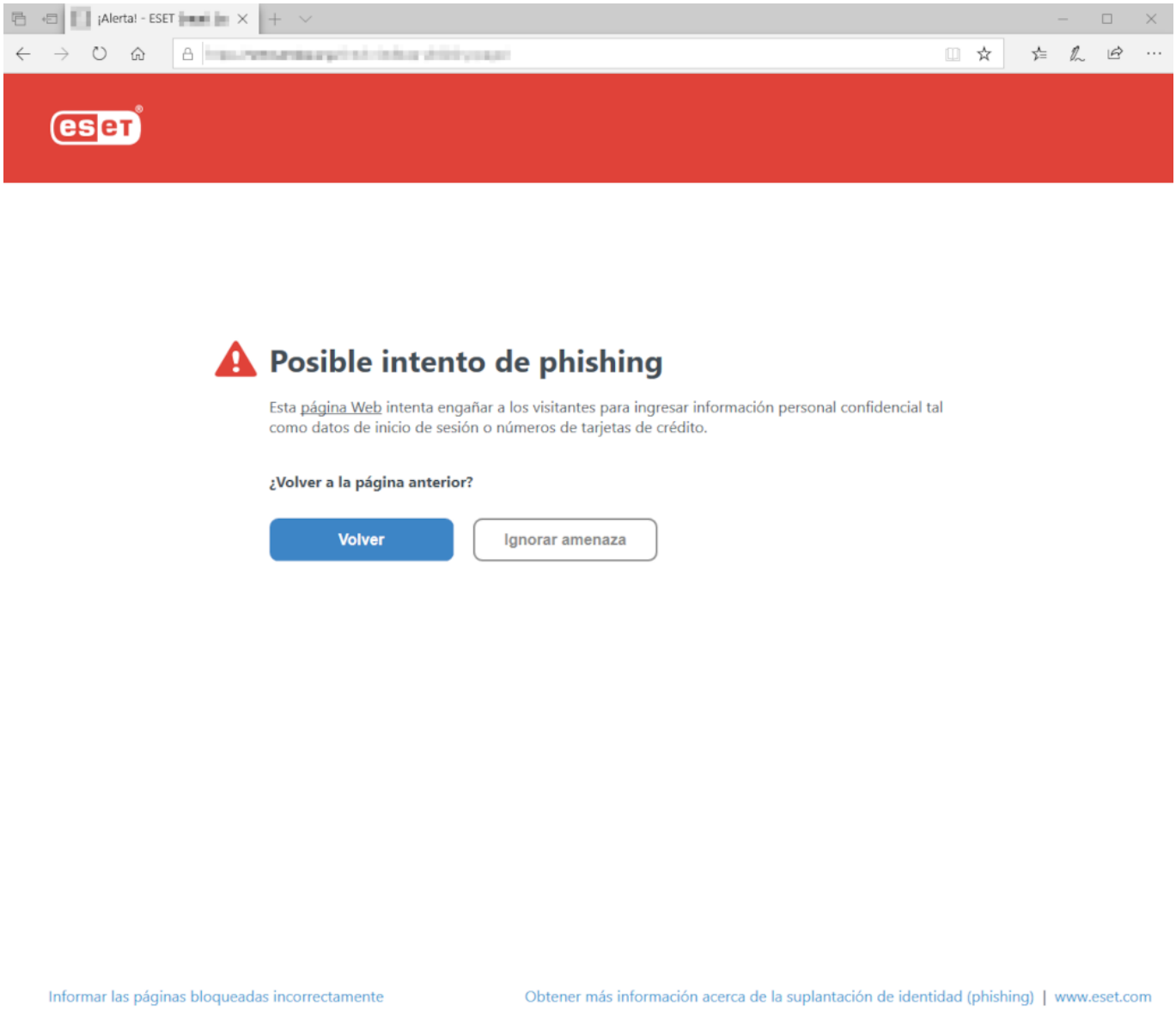
El phishing es una actividad delictiva que usa la ingeniería social (manipulación de usuarios para obtener información confidencial). El phishing se utiliza para acceder a datos confidenciales, como números de cuentas bancarias, códigos PIN, etc. Obtenga más información sobre esta actividad en el glosario. ESET Security Ultimate incluye protección antiphishing, 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 acerca de la protección antiphishing en ESET Security Ultimate.

Acceso a un sitio Web de phishing

Cuando ingrese a un sitio web de phishing reconocido, su navegador web mostrará el siguiente cuadro de diálogo. Si aún desea acceder al sitio web, haga clic en **Ignorar amenaza** (no recomendado).



Los posibles sitios Web de phishing de la lista blanca se vencerán, de forma predeterminada, luego de algunas horas. Para permitir un sitio Web de manera permanente, use la herramienta Administración de direcciones URL. En Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Administración de direcciones URL** > **Lista de direcciones** > **Editar** agregue a la lista el sitio web que desea editar.

Informar una página de phishing

El enlace **Informar una página bloqueada incorrectamente** le permite informar un sitio Web que se detecta incorrectamente como una amenaza.

Como alternativa, puede enviar el sitio Web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Recuerde usar un asunto descriptivo y proporcionar la mayor cantidad de información posible sobre el sitio web (por ejemplo, el sitio web que se lo recomendó, cómo se enteró de este sitio web, etc.).

Control parental

El módulo Control parental permite configurar las opciones del parental control, que les proporciona a los padres herramientas automatizadas para ayudar a proteger a sus hijos y establecer restricciones para dispositivos y servicios. El objetivo es prevenir que los niños y jóvenes accedan a páginas con contenido inapropiado o perjudicial.

El control parental le permite bloquear las páginas web que puedan contener material potencialmente ofensivo. Además, puede prohibir el acceso a más de 40 categorías de sitios Web predefinidos y más de 140 subcategorías.

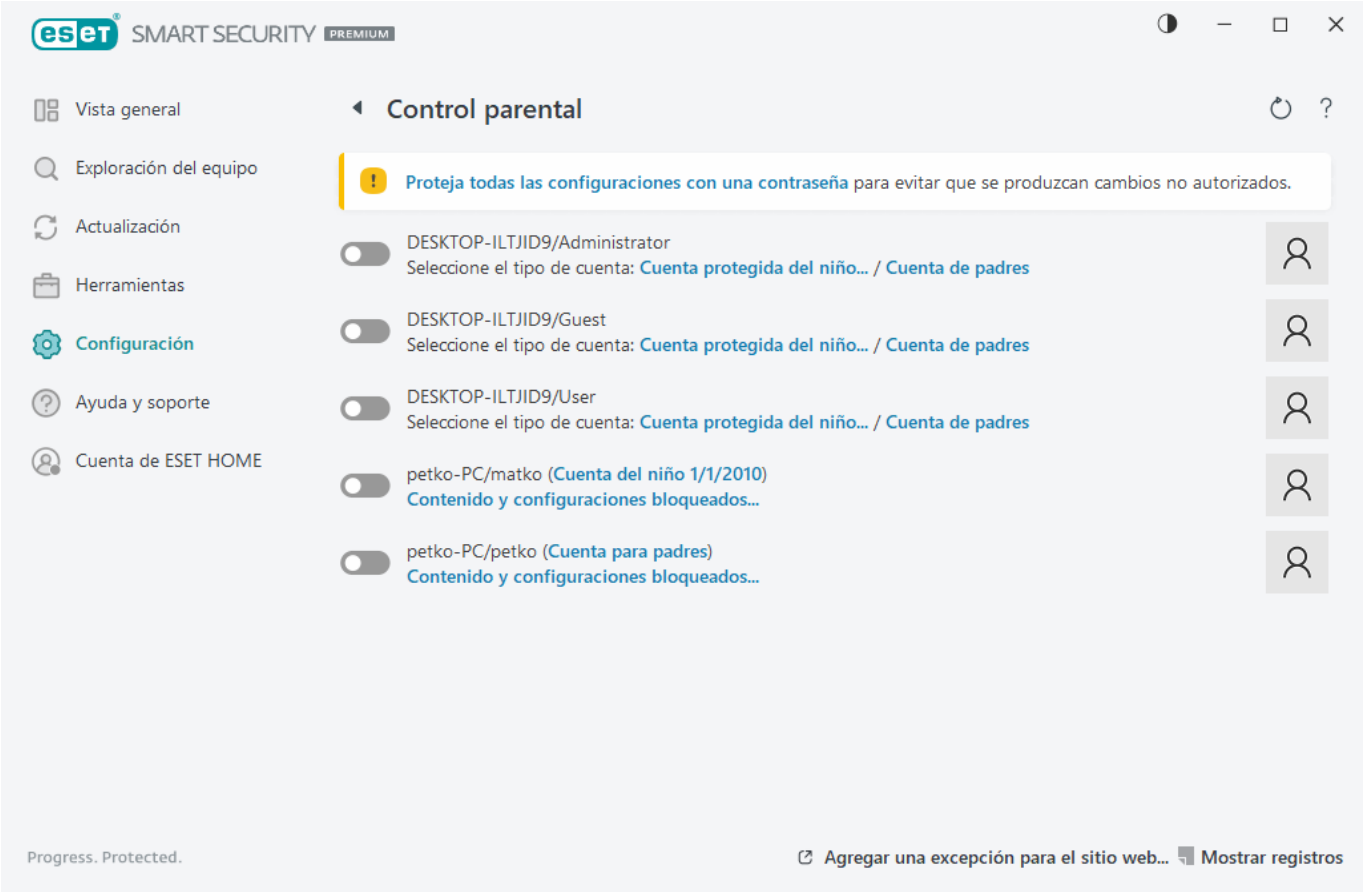
Para activar el control parental en una cuenta de usuario específica, siga los pasos a continuación:

1. De manera predeterminada, el control parental está deshabilitado en ESET Security Ultimate. Existen dos métodos para activar el Control parental:

   • Haga clic en el ícono interruptor  en **Configuración** > **Protección de internet** > **Control parental** de la ventana principal del programa y cambie el estado del Control parental a habilitado.

   • Abra Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Control parental** y, a continuación, habilite el interruptor junto a **Habilitar control parental**.

2. Haga clic en **Configuración** > **Protección de internet** > **Control parental** de la ventana principal del programa. Incluso si aparece **Habilitado** junto al **Control parental**, debe configurar ese control para la cuenta deseada; para ello, haga clic en el símbolo de la flecha y luego, en la siguiente ventana, debe seleccionar **Proteger cuenta para niños** o **Cuenta primaria**. En la siguiente ventana, seleccione la fecha de nacimiento para determinar el nivel de acceso y las páginas web recomendadas para la edad. El Control parental ahora estará habilitado para la cuenta especificada del usuario. Haga clic en **Contenido y configuración bloqueados** debajo del nombre de la cuenta para personalizar las categorías que desea permitir o bloquear en la pestaña Categorías. Para permitir o bloquear páginas web personalizadas que no coincidan con ninguna categoría, haga clic en la pestaña Excepciones.



Si hace clic en **Configuración** > **Protección de internet** > **Control parental** desde la ventana principal del producto de ESET Security Ultimate, verá que la ventana principal consta de:

Cuentas de usuarios de Windows

Si ha creado un rol para una cuenta existente aparecerá aquí. Haga clic en el interruptor para que muestre una marca verde junto al Control parental de la cuenta. En la cuenta activa, haga clic en Contenido y configuraciones bloqueadas para ver la lista de categorías permitidas de páginas Web para esta cuenta y las páginas Web bloqueadas y permitidas.

En la parte inferior de la ventana se encuentra

Agregar una excepción para el sitio web - El sitio web específico puede ser permitido o bloqueado de acuerdo a sus preferencias para cada cuenta parental por separado.

Mostrar el registro: muestra un registro detallado de la actividad del Control parental (las páginas bloqueadas, la cuenta para la cual se bloqueó cada página, categoría, etc.). También puede filtrar este registro al hacer clic en **Filtrar** basándose en los criterios que elija.

Control parental

Luego de deshabilitar el Control parental, se mostrará una ventana de **Deshabilitar parental control**. Ahí podrá configurar el intervalo de tiempo durante el cual estará deshabilitada la protección. Luego, la opción pasa a **Pausada** o **Deshabilitada permanentemente**.

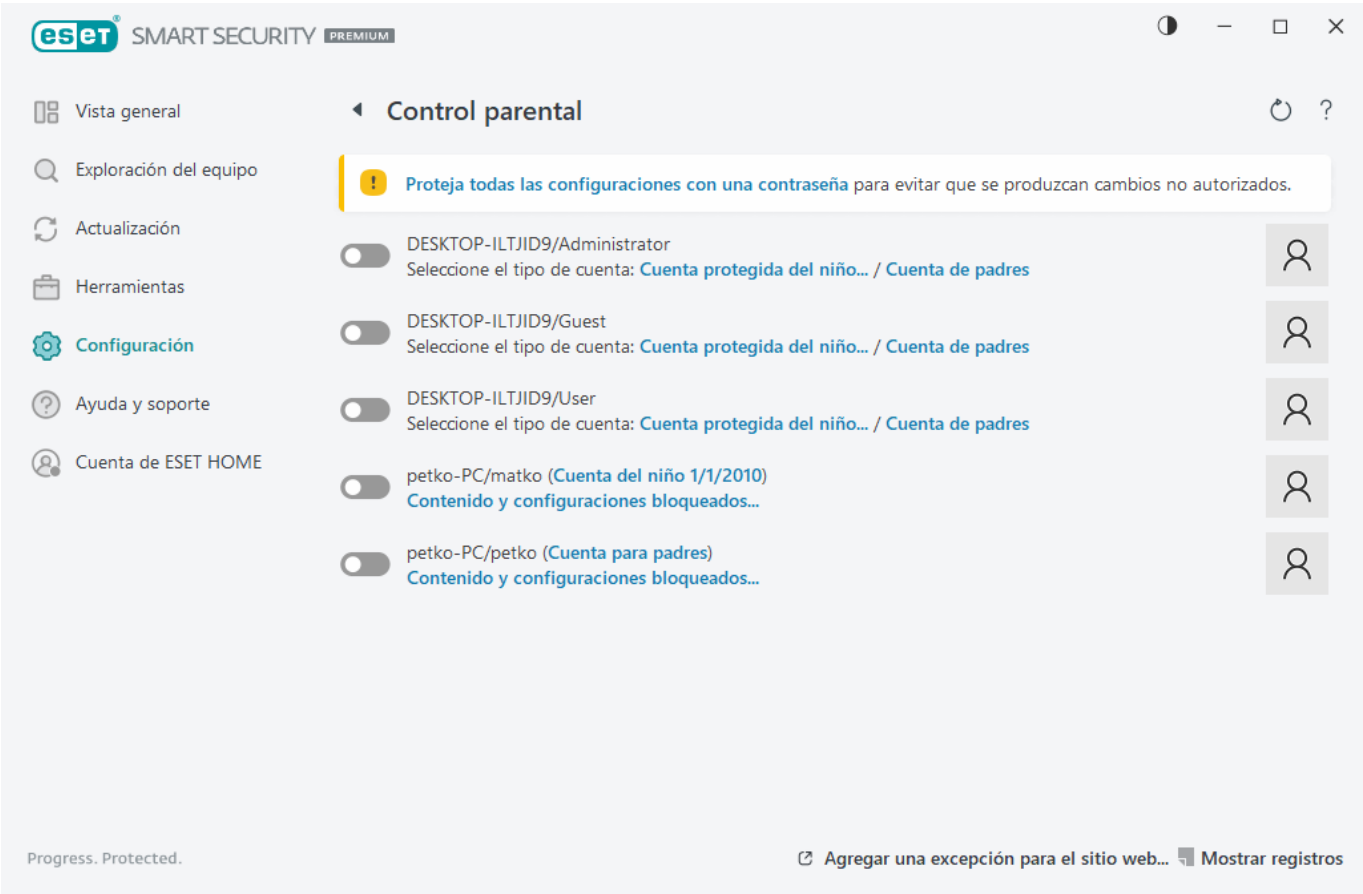
Es importante proteger la configuración de ESET Security Ultimate con una contraseña. Dicha contraseña se

establece en la sección Configuración del acceso. Se mostrará una advertencia si no se establece una contraseña: **Proteger todas las configuraciones con una contraseña** para evitar cambios no autorizados. Las restricciones establecidas en Control parental solamente afectan las cuentas de usuario estándar. Dado que un administrador puede anular cualquier restricción, las restricciones no tendrán ningún efecto en dichas cuentas.

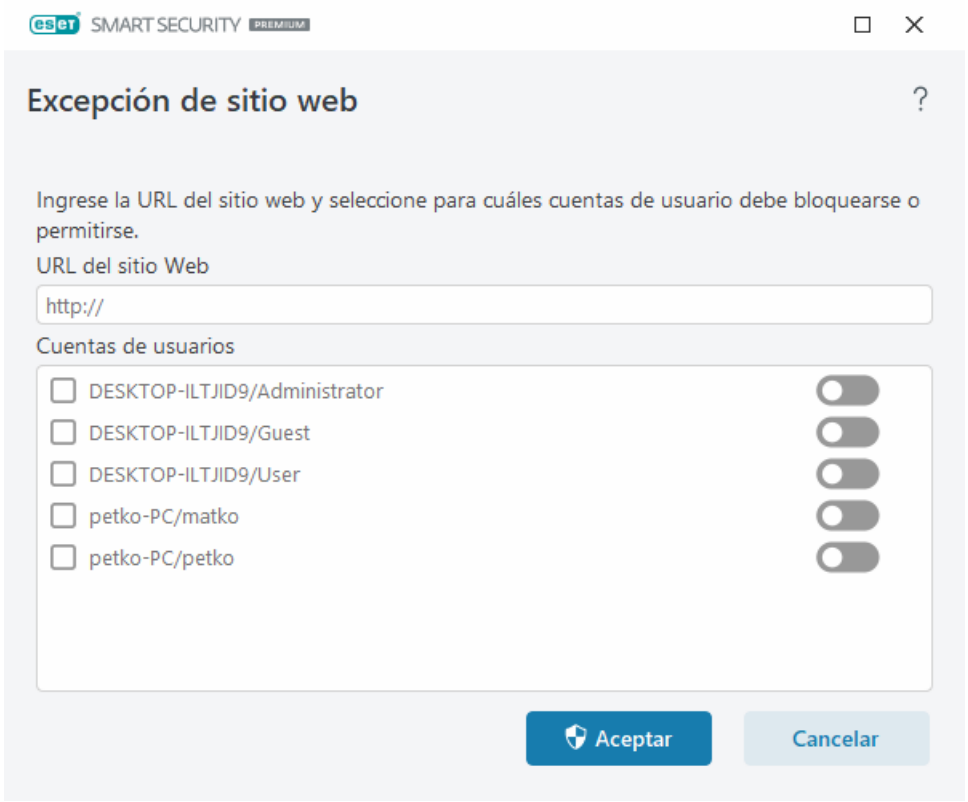
> El control parental requiere que el explorador de tráfico de red, la exploración de tráfico HTTP(S) y el firewall estén habilitados para funcionar correctamente. Todas estas funcionalidades están habilitadas de forma predeterminada.

Excepciones de sitio web

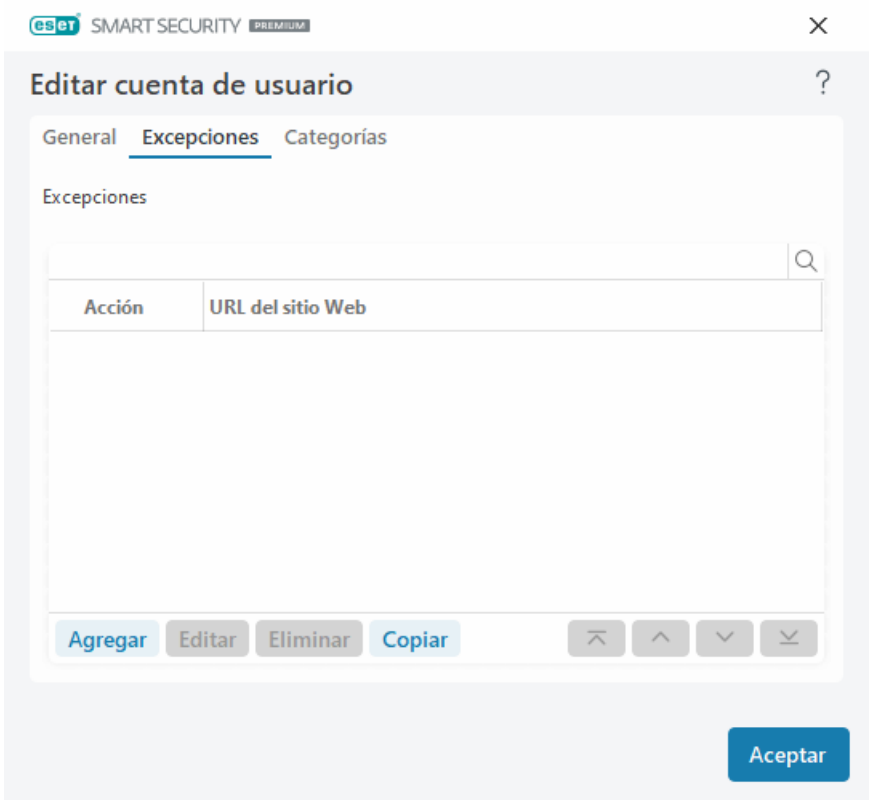
Para agregar una excepción de un sitio web, haga clic en **Configuración** > **Protección de internet** > **Control parental** y luego haga clic en **Agregar una excepción para un sitio Web**.



Ingrese una URL en el campo **URL de sitio Web**, seleccione (permitido) o (bloqueado) para cada cuenta de usuario específica y luego haga clic en **Aceptar** para agregarla a la lista.



Para eliminar una dirección URL de la lista, haga clic en **Configuración** > **Protección de internet** > **Control parental** > haga clic en **Contenido permitido y prohibido** dentro de la cuenta de usuario deseado, haga clic en la pestaña **Excepciones,** seleccione la excepción y haga clic en **Eliminar**.



En la lista de direcciones URL, no pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). Por ejemplo, las direcciones de página Web con varios TLD se deben ingresar manualmente (*examplepage.com*, *examplepage.sk*, etc.). Cuando agregue un dominio a la lista, todo el contenido ubicado en este dominio y todos los subdominios (por ejemplo, *sub.examplepage.com*) se bloquearán o permitirán en

función de su elección de acción basada en URL.

El hecho de bloquear o permitir una página Web específica puede ser más preciso que bloquear o permitir una categoría de páginas Web. Tenga precaución al modificar estas opciones y agregar una categoría o página Web a la lista.

Copiar excepción del usuario

Seleccione un usuario del menú desplegable desde el cual desea copiar una excepción creada.

Copiar categorías de la cuenta

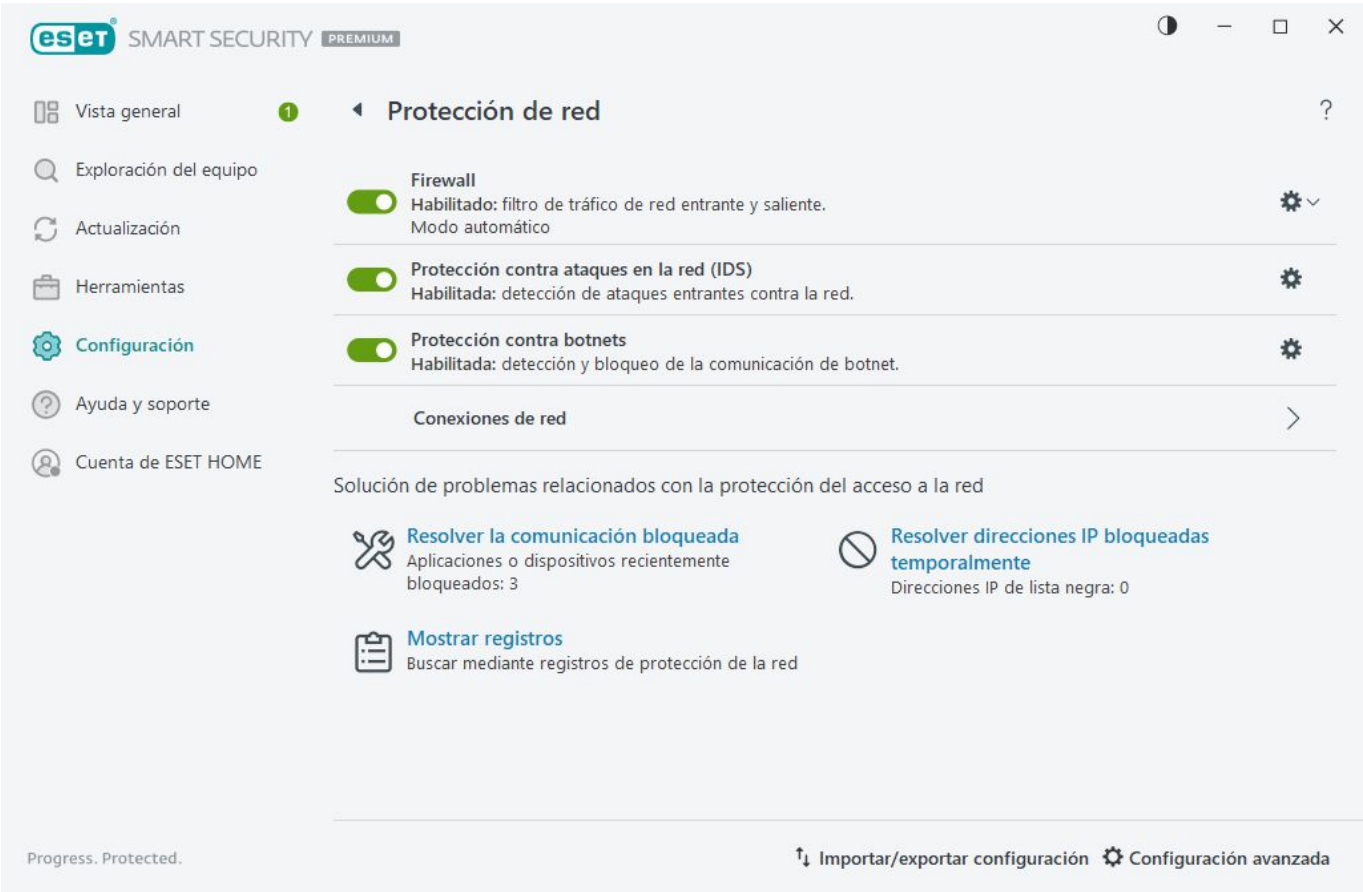
Le permite copiar una lista de categorías bloqueadas o permitidas de una cuenta modificada existente.

Protección de la red

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

Para pausar o desactivar módulos de protección individuales, haga clic en el ícono de interruptor .

Desactivar los módulos de protección puede disminuir el nivel de protección del equipo.



Haga clic en el icono del engranaje junto a un módulo de protección para acceder a las configuraciones

avanzadas de dicho módulo.

Firewall: filtra toda la comunicación de red en función de la configuración de ESET Security Ultimate.

Configurar – abre la Configuración avanzada del firewall donde puede definir cómo el firewall manejará la comunicación de redes.

Pausar firewall (permitir todo tráfico): se desactivan todas las opciones de filtrado del firewall y se permiten todas las conexiones entrantes y salientes. Haga clic en **Habilitar el firewall** para restablecer el firewall mientras el filtrado del tráfico de red está en este modo.

Bloquear todo el tráfico – todas las comunicaciones entrantes y salientes serán bloqueadas por el Firewall. Use esta opción solo si sospecha que existe un riesgo crítico de seguridad que requiere desconectar el sistema de la red. Mientras el filtrado del tráfico de red está en modo **Bloquear todo el tráfico**, haga clic en **Detener el bloqueo de todo el tráfico** para restablecer el firewall a su funcionamiento normal.

Modo automático – (cuando otro modo de filtrado está habilitado) – Haga clic para cambiar del modo de filtrado al modo de filtrado automático (con reglas definidas por el usuario).

Modo interactivo – (cuando otro modo de filtrado está habilitado) – Haga clic para cambiar del modo de filtrado al modo de filtrado interactivo.

Protección contra ataques a la red (IDS) – Analiza el contenido del tráfico de red y protege de ataques en la red. Todo tráfico considerado perjudicial será bloqueado. ESET Security Ultimate le informará cuando se conecte a una red inalámbrica desprotegida o a una red con protección débil.

Protección contra Botnet: detecta de manera rápida y precisa el malware en el sistema.

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 resolver los problemas de conectividad causados por el firewall de ESET. Para obtener información más detallada, consulte el Asistente para la resolución de problemas.

Resolver direcciones IP bloqueadas temporalmente – ver una lista de direcciones IP que han sido detectadas como la fuente de ataques y agregadas a la lista negra para bloquear la conexión durante cierto período de tiempo.

Mostrar registros: abre el archivo Registro de la Protección de 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 del programa principal > **Configuración** > **Protección de red** > **Conexiones de red**.

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

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

- **Editar**: abre la ventana Configurar protección de red, donde puede asignar un perfil de protección de red a una red específica.

- **Olvidar**: restablece la configuración de la conexión de red a la predeterminada
- **Analizar red con Inspector de red**: abre el Inspector de red para ejecutar una exploración de red.
- **Marcar como "Mi red"**: agrega una etiqueta "Mi red" a la red; esta etiqueta se mostrará junto a la red en todo ESET Security Ultimate a fin de mejorar la identificación y la visión general de seguridad.
- **Desmarcar como "Mi red"**: elimina la etiqueta "Mi red"; sólo disponible si la red ya está etiquetada

Detalles de conexión de la red

Haga doble clic en una conexión de la lista de Conexiones de red para mostrar sus 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 conexión de la red:

- Estado de la conexión de red
- Fecha y hora de la primera detección de red
- Última vez 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 red (si la red es de confianza)

Detalles del adaptador de red:

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

Solución de problemas de acceso a la red

El Asistente para la resolución de problemas le ayuda a resolver problemas de conectividad causados por el Firewall. **La solución de problemas de acceso a la red** se puede encontrar en la ventana del programa principal > **Configuración** > **Protección de red** > **Resolver comunicación bloqueada**.

Seleccione si desea mostrar la comunicación bloqueada para **aplicaciones locales** o la comunicación bloqueada desde **dispositivos remotos**.

Desde el menú desplegable, seleccione el tiempo durante el que la comunicación se ha bloqueado. El listado de comunicaciones bloqueadas recientemente le brinda una vista general del tipo de aplicación o dispositivo, reputación y cantidad total de aplicaciones y dispositivos bloqueados durante dicho período. Para más detalles sobre comunicaciones bloqueadas, haga clic en **Detalles**. El siguiente paso es desbloquear la aplicación o dispositivo con el que está experimentando problemas de conectividad.

Al hacer clic en **Desbloquear**, se permitirá la comunicación que estaba bloqueada. Si los problemas con una aplicación continúan o si su dispositivo no funciona como debería, haga clic en **crear otra regla** y se permitirán todas las comunicaciones para ese dispositivo que estaban bloqueadas. Si el problema persiste, reinicie el equipo.

Haga clic en **Abrir reglas de firewall** para ver las reglas creadas por el asistente. Asimismo, puede ver las reglas creadas por el asistente en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Firewall** > **Reglas** > **Editar**.

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

Lista negra temporal de direcciones IP

Las direcciones IP que han sido detectadas como fuentes de ataques son agregadas a la Lista negra para prevenir la conexión durante un cierto período de tiempo, abra ventana del programa principal > **Configuración** > **Protección de red** > **Resolver direcciones IP bloqueadas temporalmente**. Las direcciones IP bloqueadas de manera temporal se bloquean durante 1 hora.

Columnas

Direcciones IP: muestra las direcciones IP que han sido bloqueadas.

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

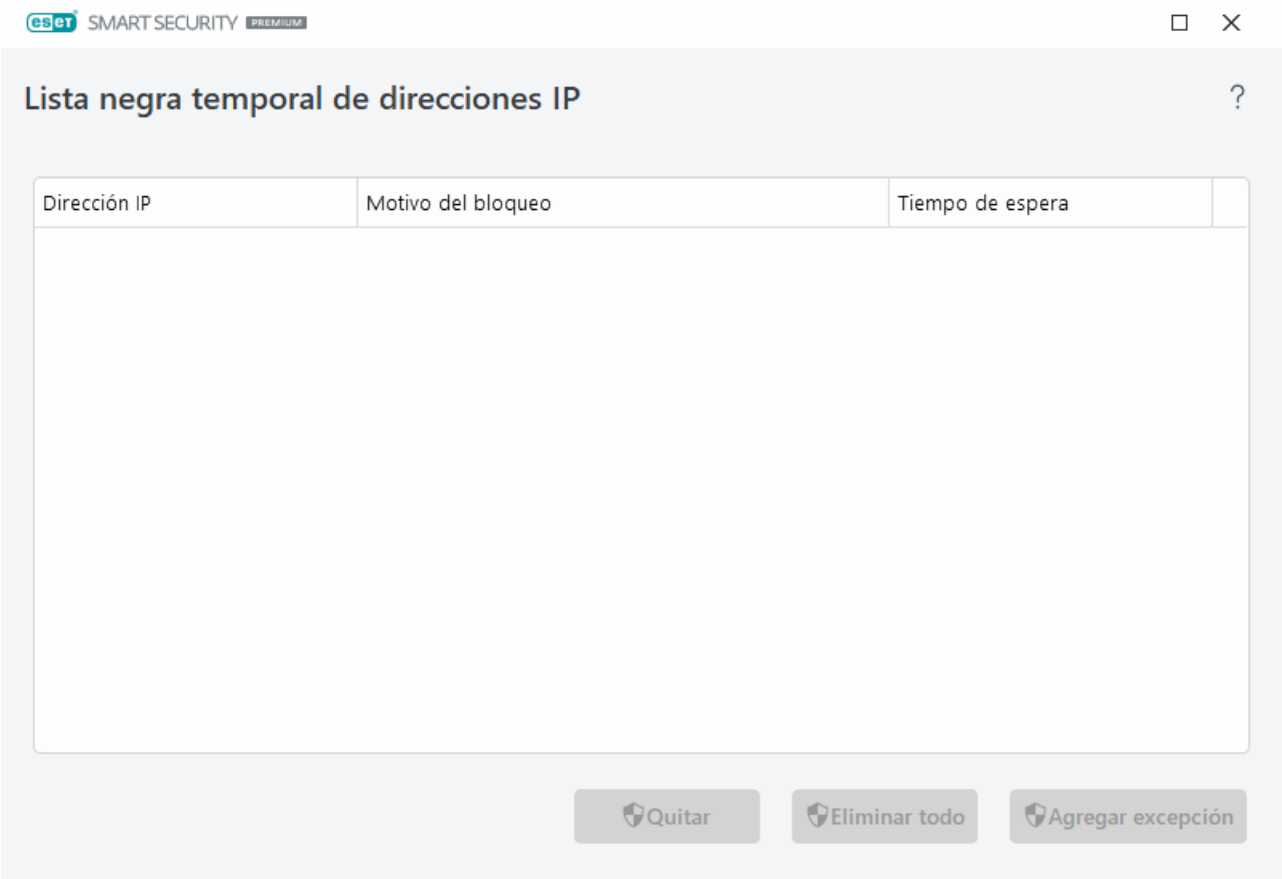
Tiempo de espera: muestra la hora y fecha en la cual la dirección expirará de la lista negra.

Elementos de control

Eliminar: haga clic para eliminar una dirección de la lista negra antes de que expire.

Quitar todas: haga clic para quitar todas las direcciones de la lista negra inmediatamente.

Agregar excepción: haga clic para agregar una excepción del firewall al filtrado de IDS.



Registros de protección de red

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

Los archivos de registro se pueden usar para detectar errores y revelar intrusiones en el sistema. Los registros de protección de red contienen los siguientes datos:

- Fecha y la hora del suceso
- Nombre del suceso
- Fuente
- Dirección de red de destino
- Protocolo de comunicación de red
- La regla aplicada o, si se identificó el gusano, su nombre
- Ruta de la aplicación y nombre
- Hash
- Usuario
- Firmante de la aplicación (editor)

- Nombre del paquete
- Nombre del servicio

Un análisis completo de estos datos puede ayudar a detectar intentos de comprometer la seguridad del sistema. Existen muchos otros factores que indican riesgos de seguridad potenciales y permiten minimizar su impacto: conexiones frecuentes desde ubicaciones remotas, intentos reiterados de establecer conexiones, comunicaciones de aplicaciones desconocidas o el uso de números de puerto inusuales.

> **Explotación de la vulnerabilidad de la seguridad**
> El mensaje de ataque de vulnerabilidad a la seguridad se registra incluso cuando se soluciona la vulnerabilidad específica, ya que se detecta el intento de ataque y se lo bloquea a nivel de la red antes de que el ataque real pueda tener lugar.

Resolución de problemas con el Firewall

Si experimenta problemas de conectividad con ESET Security Ultimate instalado, existen varias maneras de identificar si el Firewall es el causante del problema. Además, el Firewall puede ayudarle a crear nuevas reglas o excepciones para resolver los problemas de conectividad.

Consulte los siguientes temas de ayuda para resolver los problemas con el Firewall:

- Solución de problemas de acceso a la red
- Registro y creación de reglas o excepciones desde el registro
- Crear excepciones desde las notificaciones del firewall
- Registro avanzado de protección de red
- Resolución de problemas con el explorador de tráfico de red

Registro y creación de reglas o excepciones desde el registro

De forma predeterminada, el Firewall de ESET no registra todas las conexiones bloqueadas. Si desea ver lo que bloqueó la protección de red, abra Configuración avanzada > **Herramientas** > **Diagnósticos** > **Registro avanzado** y habilite **Habilitar el registro avanzado de la protección de red**. Si ve algo en el registro que no desea que el Firewall bloquee, puede crear una regla o una regla del sistema de detección de intrusiones al hacer clic derecho en ese elemento y seleccionar **No bloquear eventos similares en el futuro**. Tenga en cuenta que el registro de todas las conexiones bloqueadas puede contener miles de elementos y es posible que sea difícil encontrar una conexión específica en este registro. Puede desactivar el registro luego de haber solucionado su problema.

Para obtener más información acerca del registro consulte los Archivos de registro.

> Use los registros para ver el orden en que el Protección de red bloqueó las conexiones específicas. Además, la creación de reglas desde los registros le permite crear reglas que hagan exactamente lo que usted desee.

Crear regla a partir del registro

La nueva versión de ESET Security Ultimate le permite crear una regla a partir del registro. Desde el menú principal, haga clic en **Herramientas** > **Archivos de registro**. Elija **Protección de la red** del menú desplegable, haga clic derecho en la entrada de registro deseada y seleccione **No bloquear sucesos similares en el futuro** del menú contextual. Una ventana de notificación mostrará su regla nueva.

Para permitir la creación de reglas nuevas a partir del registro, ESET Security Ultimate debe establecerse con las siguientes configuraciones:

1. Ajustar el nivel de detalle mínimo para los registros a **Diagnóstico** en Configuración avanzada > **Herramientas** > **Archivos de registro**.

2. Active **Mostrar notificaciones para ataques entrantes frente a agujeros de seguridad** en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques a la red** > **Opciones avanzadas** > **Detección de intrusiones**.

Crear excepciones desde las notificaciones del firewall

Cuando el Firewall de ESET detecte actividad de red maliciosa, aparecerá una ventana de notificación con la descripción del suceso. Esta notificación contiene un enlace que le permitirá obtener más información acerca del suceso para, así, establecer una regla para este suceso si lo desea.

> Si una aplicación de red o dispositivo no implementa las normas de red correctamente, puede disparar reiteradas notificaciones del sistema de detección de intrusiones del firewall. Puede crear una excepción directamente desde la notificación para evitar que el Firewall de ESET detecte esta aplicación o dispositivo.

Registro avanzado de protección de red

Esta característica tiene como propósito brindar archivos de registro más complejos para el soporte técnico de ESET. Use esta característica solo cuando el soporte al cliente de ESET se lo solicite, ya que puede generar un archivo de registro inmenso y así ralentizar su equipo.

1. Abra Configuración avanzada > **Herramientas** > **Diagnósticos** > **Registro avanzado** y active **Habilitar el registro avanzado de protección de red**.

2. Intente reproducir el problema que está experimentando.

3. Deshabilite el registro avanzado de protección de red.

4. El archivo de registro PCAP creado por el registro avanzado de protección de red se puede encontrar en el mismo directorio donde se generan los volcados de memoria de diagnóstico: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Resolución de problemas con el explorador de tráfico de red

Si experimenta problemas con su navegador o cliente de correo electrónico, el primer paso es determinar si el responsable es el explorador de tráfico de red. Para hacer eso, intente deshabilitar temporalmente la exploración del tráfico de red en Configuración avanzada > **Motor de detección** > **Explorador de tráfico de red** (recuerde activarlo nuevamente una vez finalizado ya que, de lo contrario, su navegador y cliente de correo electrónico permanecerán desprotegidos). Si el problema desaparece una vez desactivado, aquí hay una lista de problemas comunes y formas para resolverlos:

Actualizar o asegurar problemas de comunicación

Si su aplicación se queja de la incapacidad de actualizar o de que un canal de comunicación no es seguro:

- Si tiene SSL/TLS habilitado, intente desactivarlo temporalmente. Si eso ayuda, puede continuar utilizando SSL/TLS y hacer que la actualización funcione al excluir la comunicación problemática:
  Deshabilitar SSL/TLS. Vuelva a ejecutar la actualización. Debería aparecer un cuadro de diálogo para informarle acerca del tráfico de red cifrado. Asegúrese de que la aplicación se ajuste a la que está intentando resolver y que el certificado parezca que proviene del servidor del que se está actualizando. Luego, elija recordar la acción para este certificado y haga clic en ignorar. Si no se muestran más cuadros de diálogo relevantes, puede cambiar el modo de filtrado a automático y el problema debería resolverse.

- Si la aplicación en cuestión no es un navegador o cliente de correo electrónico, puede excluirla por completo de protección de acceso a la web (hacer esto en el navegador o cliente de correo electrónico lo dejaría expuesto). Cualquier aplicación cuya comunicación haya sido filtrada en el pasado debería estar en la lista provista a usted cuando agrega la excepción, por lo que agregar una de forma manual no debería ser necesario.

Problema para acceder a un dispositivo de su red

Si no puede usar ninguna funcionalidad de un dispositivo en su red (esto podría significar abrir una página web de su cámara web o reproducir un video en un reproductor multimedia doméstico), intente agregar sus direcciones IPv4 y IPv6 a la lista de direcciones excluidas.

Problemas con un sitio Web específico

Puede excluir sitios Web específicos de la protección de acceso a la web con la gestión de direcciones URL. Por ejemplo, si no puede acceder a https://www.gmail.com/intl/en/mail/help/about.html, intente agregar *gmail.com* a la lista de direcciones excluidas.

Error “Algunas de las aplicaciones aptas para importar el certificado raíz siguen activas”

Cuando habilita SSL/TLS, ESET Security Ultimate se asegura de que las aplicaciones instaladas confían en la forma en que se filtra e protocolo SSL al importar un certificado a su almacén de certificados. Es posible que algunas aplicaciones requieran un reinicio para importar un certificado. Esto incluye a Firefox y Opera. Asegúrese de que ninguna de ellas esté activa (la mejor manera de hacer esto es abrir el Administrador de tareas y asegurarse de que firefox.exe u opera.exe no estén en la pestaña de Procesos), luego vuelva a intentarlo.

Error acerca de un emisor no confiable o de una firma no válida

Lo más probable es que esto signifique que falló la importación antes mencionada. Primero, asegúrese de que ninguna de las aplicaciones mencionadas esté activa. A continuación, desactive SSL/TLS y vuelva a activarlo. Esto vuelve a ejecutar la importación.

Consulte el artículo de la base de conocimiento para obtener información sobre Cómo gestionar el explorador de tráfico de red en el producto ESET para Windows home.

Se bloqueó una amenaza de red

Esta situación puede ocurrir cuando una aplicación en su equipo está intentando transmitir tráfico malicioso a otro dispositivo en la red, está explotando una vulnerabilidad de seguridad o incluso si se detecta un intento de exploración de los puertos en su sistema.

Puede encontrar el tipo de amenaza y la dirección IP del dispositivo relacionado en la notificación. Haga clic en **Cambiar el manejo de esta amenaza** para mostrar las siguientes opciones:

Continuar con el bloqueo: bloquea la amenaza detectada. Si desea dejar de recibir notificaciones sobre este tipo de amenaza desde la dirección remota específica, seleccione el botón de opción situado junto a **No notificar** antes de hacer clic en **Continuar con el bloqueo**. Al hacerlo, se creará una regla de servicio de detección de intrusiones (IDS) con la siguiente configuración: **Bloquear** - predeterminado, **Notificar** - no, **Registrar** - no.

Permitir:crea una regla de 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:

- **Notificar únicamente cuando se bloquea esta amenaza** — Configuración de la regla: **Bloquear** - no, **Notificar** - no, **Registrar** - no.
- **Notificar siempre que esta amenaza ocurra** — Configuración de la regla: **Bloquear** - no, **Notificar** - predeterminado, **Registrar** - predeterminado.
- **No notificar** — Configuración de la regla: **Bloquear** - no, **Notificar** - no, **Registrar** - no.

La información que se muestre en la ventana de notificación puede variar en base al tipo de amenaza detectada.
Para obtener más información acerca de las amenazas y otros términos relacionados, consulte Tipos de ataques remotos o Tipos de detecciones.
Para resolver el evento **Direcciones de IP duplicadas en la red**, consulte nuestro artículo de la Base de conocimiento de ESET.

Detección de una red nueva

De manera predeterminada, ESET Security Ultimate 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 red a **Preguntar**. La configuración de la protección de red se mostrará cada vez que el equipo se conecte a una nueva red.

Puede seleccionar entre los siguientes perfiles de conexión de red:

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

Privado: para redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de 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.

Público: para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a 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 está disponible solo si ha creado al menos un perfil personalizado.

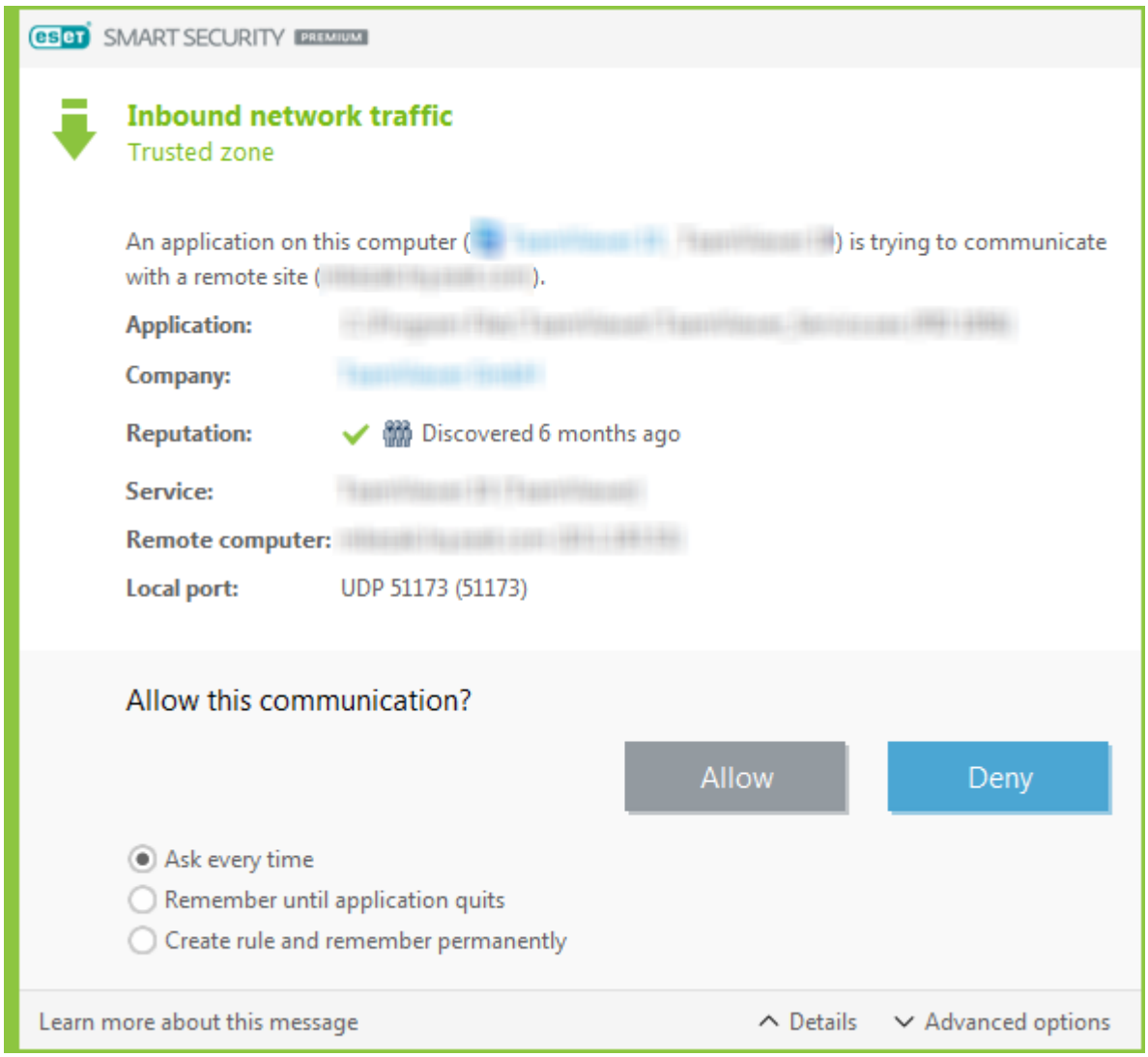
⚠ Una configuración de red incorrecta puede suponer un riesgo para la seguridad de su equipo.

Establecimiento de una conexión: detección

El firewall detecta cada nueva conexión de red que se crea. El modo de firewall activo determina las acciones que se llevan a cabo para la nueva regla. Si el **Modo automático** o el **Modo basado en políticas** está activado, el firewall realizará acciones predefinidas sin la interacción del usuario.

El **modo interactivo** muestra una ventana informativa para indicar que se detectó una nueva conexión de red, complementada con información detallada sobre la conexión. Puede optar por **Permitir** o **Rechazar** (bloquear) la conexión. Si permite la misma conexión en forma reiterada en la ventana de diálogo, es recomendable crear una nueva regla para esa conexión. Seleccione **Crear regla y recordar permanentemente** y guarde la acción como una

nueva regla para el Firewall. Si en el futuro el firewall reconoce la misma conexión, aplicará la regla existente sin requerir la interacción del usuario.



Cuando cree reglas nuevas, solo permita las conexiones que usted reconoce como seguras. Si se permiten todas las conexiones, el firewall deja de cumplir su propósito. Estos son los 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. Las conexiones tienen un nivel de riesgo: Aceptable (verde), Desconocido (naranja) o Peligroso (rojo), y cada nivel se establece mediante una serie de reglas heurísticas que examinan las características de cada conexión, el número de usuarios y la hora de detección. Estos datos se recopilan con la tecnología ESET LiveGrid®.

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

Equipo remoto: dirección del dispositivo remoto. Solo permite las conexiones de direcciones de confianza y conocidas.

Puerto remoto: puerto de comunicación. La comunicación en puertos comunes (p. ej., tráfico de red, número de puerto 80 443) deberían permitirse bajo circunstancias normales.

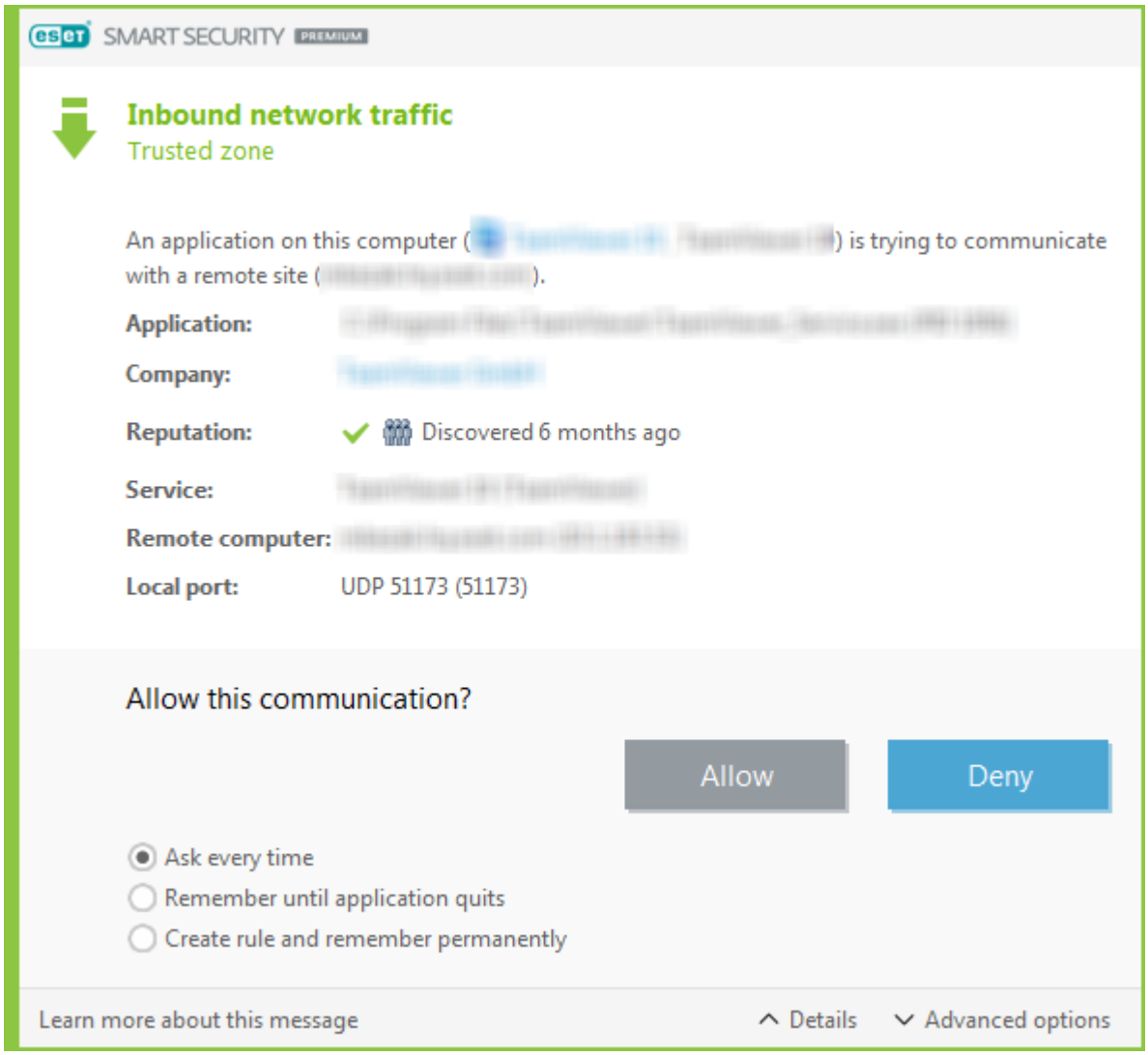
Las infiltraciones informáticas suelen usar Internet y conexiones ocultas, que las ayudan a infectar sistemas remotos. Si las reglas están configuradas correctamente, el firewall se convierte en una herramienta útil para la protección ante una diversidad de ataques de códigos maliciosos.

Modificación de aplicaciones

El firewall detectó un cambio en una aplicación que se usa para establecer conexiones salientes desde el equipo. Es posible que la aplicación simplemente se haya actualizado a una versión posterior. Por otro lado, la modificación también puede haberse provocado por una aplicación maliciosa. Si no percibe ningún cambio legítimo, es recomendable que deniegue la conexión y explore el equipo con la base de datos de firmas de virus más reciente.

Comunicación de confianza entrante

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



Aplicación: la aplicación contactada por un dispositivo remoto.

Ruta 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: reputación de la aplicación obtenida por la tecnología ESET LiveGrid®.

Proceso: nombre del proceso que se está ejecutando actualmente en el equipo.

Equipo remoto: equipo remoto que intenta establecer una comunicación con la aplicación del equipo local.

Puerto remoto: puerto usado para la comunicación.

Preguntar siempre: Si la acción predeterminada para una regla está configurada en **Preguntar**, una ventana de diálogo aparecerá cada vez que se active la regla.

Recordar hasta salir de la aplicación: ESET Security Ultimate se recordará la acción seleccionada hasta el próximo reinicio.

Crear regla y recordar permanentemente: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Security Ultimate recordará la acción y la usará si el equipo remoto vuelve a ponerse en contacto con la aplicación.

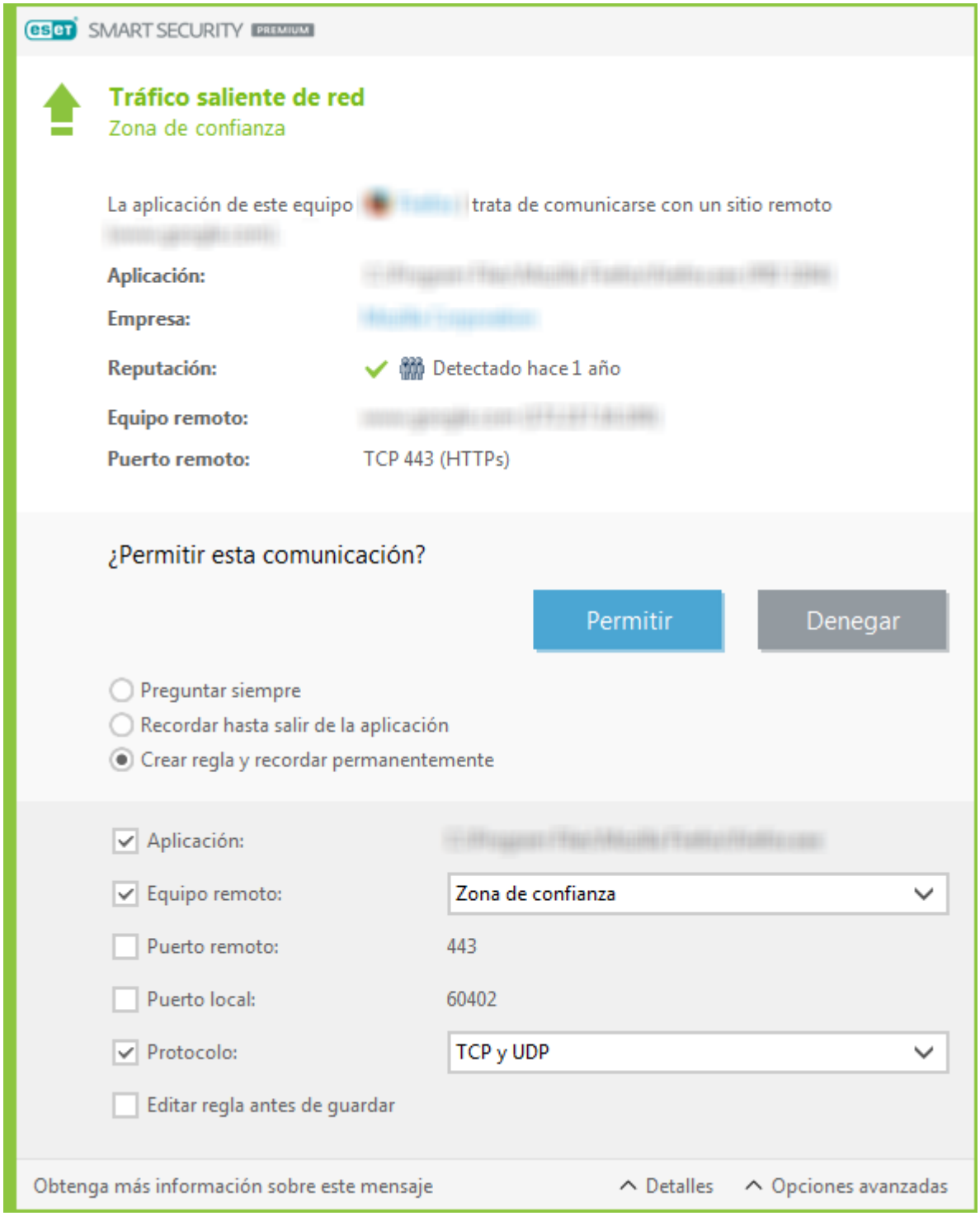
Permitir: permite la comunicación entrante.

Denegar: deniega la comunicación entrante.

Editar regla: permite personalizar las propiedades de la regla mediante el editor de reglas de firewall.

Comunicación de confianza saliente

Ejemplo de una conexión saliente dentro de la zona de confianza:
Una aplicación local que intenta establecer una conexión con otro equipo dentro de la red local o dentro de una red de la zona segura.



Aplicación: la aplicación contactada por un dispositivo remoto.

Ruta 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: reputación de la aplicación obtenida por la tecnología ESET LiveGrid®.

Proceso: nombre del proceso que se está ejecutando actualmente en el equipo.

Equipo remoto: equipo remoto que intenta establecer una comunicación con la aplicación del equipo local.

Puerto remoto: puerto usado para la comunicación.

Preguntar siempre: Si la acción predeterminada para una regla está configurada en **Preguntar**, una ventana de diálogo aparecerá cada vez que se active la regla.

Recordar hasta salir de la aplicación: ESET Security Ultimate se recordará la acción seleccionada hasta el próximo reinicio.

Crear regla y recordar permanentemente: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Security Ultimate recordará la acción y la usará si el equipo remoto vuelve a ponerse en contacto con la aplicación.

Permitir: permite la comunicación entrante.

Denegar: deniega la comunicación entrante.

Editar regla: permite personalizar las propiedades de la regla mediante el editor de reglas de firewall.

Comunicación entrante

Ejemplo de una conexión de Internet entrante:
Un equipo remoto que intenta comunicarse con una aplicación ejecutada en el equipo.

Aplicación: la aplicación contactada por un dispositivo remoto.

Ruta 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: reputación de la aplicación obtenida por la tecnología ESET LiveGrid®.

Proceso: nombre del proceso que se está ejecutando actualmente en el equipo.

Equipo remoto: equipo remoto que intenta establecer una comunicación con la aplicación del equipo local.

Puerto remoto: puerto usado para la comunicación.

Preguntar siempre: Si la acción predeterminada para una regla está configurada en **Preguntar**, una ventana de diálogo aparecerá cada vez que se active la regla.

Recordar hasta salir de la aplicación: ESET Security Ultimate se recordará la acción seleccionada hasta el próximo reinicio.

Crear regla y recordar permanentemente: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Security Ultimate recordará la acción y la usará si el equipo remoto vuelve a ponerse en contacto con la aplicación.

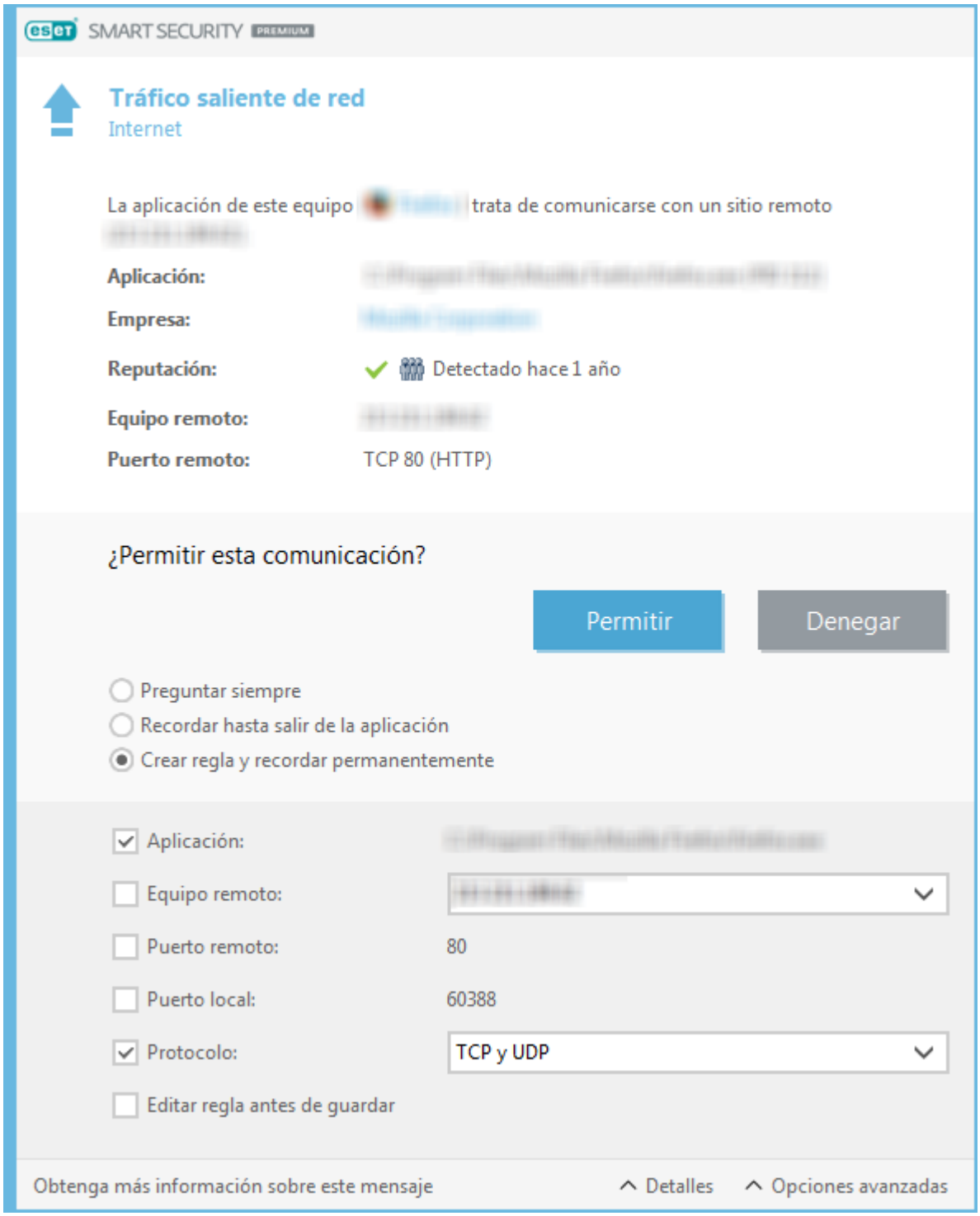
Permitir: permite la comunicación entrante.

Denegar: deniega la comunicación entrante.

Editar regla: permite personalizar las propiedades de la regla mediante el editor de reglas de firewall.

Comunicación saliente

Ejemplo de una conexión de Internet saliente:
Una aplicación local que intenta establecer una conexión a Internet.



Aplicación: la aplicación contactada por un dispositivo remoto.

Ruta 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: reputación de la aplicación obtenida por la tecnología ESET LiveGrid®.

Proceso: nombre del proceso que se está ejecutando actualmente en el equipo.

Equipo remoto: equipo remoto que intenta establecer una comunicación con la aplicación del equipo local.

Puerto remoto: puerto usado para la comunicación.

Preguntar siempre: Si la acción predeterminada para una regla está configurada en **Preguntar**, una ventana de diálogo aparecerá cada vez que se active la regla.

Recordar hasta salir de la aplicación: ESET Security Ultimate se recordará la acción seleccionada hasta el próximo reinicio.

Crear regla y recordar permanentemente: si selecciona esta opción antes de permitir o denegar una comunicación, ESET Security Ultimate recordará la acción y la usará si el equipo remoto vuelve a ponerse en contacto con la aplicación.

Permitir: permite la comunicación entrante.

Denegar: deniega la comunicación entrante.

Editar regla: permite personalizar las propiedades de la regla mediante el editor de reglas de firewall.

Configuración de la vista de la conexión

Haga un clic derecho en una conexión para ver opciones adicionales, entre las que se incluyen:

Resolver nombres de host – si es posible, todas las direcciones de red se muestran en el formato de nombre DNS, no en el formato numérico de dirección IP.

Mostrar solo las conexiones TCP – la lista muestra únicamente las conexiones pertenecientes al grupo de protocolos TCP.

Mostrar las conexiones de escucha – seleccione esta opción para mostrar únicamente aquellas conexiones para las que aún no se estableció comunicación alguna, pero para las que el sistema ha abierto un puerto y está esperando establecer una conexión.

Mostrar las conexiones dentro del equipo – seleccione esta opción para mostrar únicamente aquellas conexiones en las que el lado remoto es un sistema local; es decir, las llamadas conexiones localhost.

Actualizar la velocidad – elija la frecuencia para actualizar las conexiones activas.

Actualizar ahora – actualiza la ventana de **Conexiones de red**.

Herramientas de seguridad

Abra la ventana del programa principal > **Configurar** > **Herramientas de seguridad** para ajustar los siguientes módulos:

Banca y navegación seguras: añade un nivel de protección de navegadores diseñado para proteger su información financiera durante las transacciones en línea. Habilite **Proteger todos los navegadores** en la configuración avanzada de Banca y navegación seguras para iniciar todos los navegadores web compatibles en un modo seguro.

Seguridad y privacidad del navegador: mantiene su actividad en línea privada y segura sin dejar una huella digital.

Anti-Theft: active Anti-Theft para proteger su equipo 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 protege y almacena sus contraseñas y datos personales.

VPN – Proteja sus datos y evada el seguimiento no deseado con una dirección IP anónima.

Identity Protection: protege su información personal, crediticia y financiera.

Banca y navegación seguras

Banca y navegación seguras es una capa de protección adicional diseñada para proteger sus datos financieros durante las transacciones en línea.

De forma predeterminada, los navegadores compatibles comenzarán en modo seguro. Esto le permite navegar por Internet, acceder a la banca por Internet y realizar compras y transacciones en línea en un navegador seguro automáticamente.

El sistema de reputación de ESET LiveGrid® debe estar habilitado (de forma predeterminada) para garantizar que Banca y navegación seguras funcione correctamente.

Para configurar el comportamiento de navegador seguro, consulte Configuración avanzada de Banca y navegación seguras. Si desactiva la opción **Proteger todos los navegadores**, puede acceder al navegador seguro en la ventana principal del programa > **Descripción general** > **Banca y navegación seguras** o haciendo clic en el ícono del escritorio **Banca y navegación seguras**. El navegador, establecido como predeterminado en Windows, se inicia en un modo seguro.

Es necesario el uso de la comunicación cifrada HTTPS para realizar la navegación 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+

Solo Firefox y Microsoft Edge son compatibles con dispositivos con procesadores ARM.

Para obtener más información sobre las funciones de Banca y navegación seguras, lea los siguientes artículos de la base de conocimientos de ESET que están disponibles en inglés y otros idiomas:

- ¿Cómo uso Banca y navegación seguras de ESET?
- Pausar o deshabilitar Banca y navegación seguras en los productos hogareños de ESET Windows
- Banca y navegación seguras de ESET: errores comunes
- Glosario de ESET | Banca y navegación seguras

Notificación en el navegador

El navegador seguro le informa de su estado actual mediante notificaciones en el navegador y el color del marco 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 ícono de cierre.

Solo pueden descartarse la notificación informativa y el marco verde del navegador.

Notificaciones en el navegador

Tipo de notificación	Estado
Notificación informativa y marco verde del navegador	Se garantiza la máxima protección y se minimiza la notificación en el 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 seguro requiere su atención para un problema no grave. Para obtener más información sobre el problema o una solución, siga las instrucciones de la notificación del navegador.
Alerta de seguridad y marco rojo del navegador	El navegador no está protegido por Banca y navegación seguras de ESET. Reinicie el navegador para asegurarse de que la protección está activa. Para resolver un conflicto con los archivos cargados en el navegador, abra Archivos de registro > **Banca y navegación seguras** y asegúrese de que los archivos registrados no se carguen la próxima vez que inicie el navegador. Si el problema persiste, póngase en contacto con el soporte técnico de ESET según las instrucciones del artículo de nuestra base de conocimiento.

Seguridad y privacidad del navegador

Puede habilitar la función de Seguridad y privacidad del navegador a través de una extensión personalizada disponible en navegadores compatibles (Google Chrome, Mozilla Firefox y Microsoft Edge solamente).

Para instalar y habilitar la extensión:

1. Asegúrese de usar la última versión de ESET Security Ultimate y reinicie correctamente su equipo después de la actualización.
2. Abra su navegador.
3. La extensión está instalada en su navegador.
4. Habilite la extensión y se mostrará la página de información del navegador con la extensión.

El menú principal de la extensión Seguridad y privacidad del navegador se divide en las siguientes secciones:

Visión general

Búsqueda segura

Haga clic en el ícono de alternancia  junto a **Explorar resultados de búsqueda** para habilitar la característica y ver en qué resultados es seguro hacer clic. La búsqueda segura evalúa las direcciones de enlace enumeradas y no significa necesariamente que el sitio web no contenga malware. Nuestro motor de detección detecta cualquier malware en el sitio web.

Limpieza del navegador

Quite sus datos de navegación o configure limpiezas periódicas. Puede agregar sitios web donde desee aceptar cookies y mantener abierta la sesión incluso después de realizar la limpieza del navegador **si los agrega a la lista**.

- **Limpieza única:**seleccione el intervalo de tiempo en el menú desplegable y el tipo de datos que desea quitar. Puede elegir entre las opciones todos los datos, selecciones privadas y personalizadas.

- **Limpieza regular**: haga clic en el ícono de alternancia  junto a **Limpieza regular** para habilitar la función. Seleccione el intervalo de tiempo en el menú desplegable y el tipo de datos que desea quitar regularmente. Puede elegir entre las opciones todos los datos, selecciones privadas y personalizadas.

La opción **Datos personalizados** contiene las siguientes categorías:

- Historial de exploración
- Historial de descargas
- Cookies y datos de sitios web
- Imágenes y archivos en caché
- Contraseñas y datos de inicio de sesión
- Datos de autocompletar formularios

Limpieza de metadatos

La característica Limpieza de metadatos controla los datos de privacidad potencialmente exponibles a través de metadatos EXIF compartidos en archivos multimedia, documentos y otros formatos de archivo compatibles. Haga clic en el ícono de alternancia  junto a **Limpiar metadatos cada vez que sube una imagen** para habilitar la eliminación de metadatos.

Debe reiniciar el navegador para asegurarse de que la **Limpieza de metadatos** funcione correctamente.

Haga clic en el ícono de alternancia  junto a **Obtener notificaciones en el navegador** para habilitar la visualización de notificaciones después de la limpieza de metadatos.

Revisión de las configuraciones de los sitios web sitios web

Consulte y administre los permisos de sitios web para controlar qué información pueden usar los sitios web.

- **Notificaciones**: revise de qué sitios web desea **Permitir/Bloquear** las notificaciones o si desea que la extensión del navegador le **Pregunte cada vez**.

Configuración avanzada

Limpieza del navegador

Configuración avanzada de cookies

Lista de sitios web donde desea aceptar cookies y mantener abierta la sesión incluso después de realizar la limpieza del navegador. Introduzca la dirección URL en el campo de texto y haga clic en **Agregar**. Puede quitarla en cualquier momento de la lista haciendo clic en el ícono menos  junto al sitio web específico.

En la parte inferior de la página se encuentra la lista de dominios sugeridos actualmente abiertos en el navegador. Si no puede ver el sitio web específico, haga clic en **actualizar la lista** y agréguelo a la lista de cookies aceptadas haciendo clic en el ícono más  .

Revisión de las configuraciones de los sitios web sitios web

Consulte y administre los permisos de sitios web para controlar qué información pueden usar los sitios web.

- **Notificaciones**: revise de qué sitios web desea **Permitir/Bloquear** las notificaciones o si desea que la extensión del navegador le **Pregunte cada vez**.

Apariencia

Personalice el esquema de colores de la interfaz para que se adapte a sus preferencias. Puede elegir la combinación de colores que prefiera si selecciona la casilla de verificación **Claro** u **Oscuro**.

Anti-Theft

Los dispositivos personales corren constantemente el riesgo de perderse o ser robados en nuestros desplazamientos diarios del hogar al trabajo o a otros lugares públicos. Anti-Theft es una característica que amplía la seguridad en el nivel de usuario en caso de pérdida o robo del dispositivo. Anti-Theft le permite supervisar el

uso del dispositivo y rastrear el dispositivo perdido mediante la localización por dirección IP en ESET HOME, lo cual lo ayuda a recuperar el dispositivo y a proteger sus datos personales.

En el uso de las tecnologías modernas, como la búsqueda de dirección IP geográfica, la captura de imágenes con la cámara Web, la protección de la cuenta del usuario y la supervisión del dispositivo, Anti-Theft puede ayudar a usted y a una organización encargada del cumplimiento de la ley a ubicar su equipo o dispositivo si lo perdió o se lo robaron. En ESET HOME, puede ver la actividad que tiene lugar en el equipo o el dispositivo.

Para obtener más información sobre Anti-Theft en ESET HOME, consulte la Ayuda en línea de ESET HOME.

Es posible que Anti-Theft no funcione correctamente en los equipos de los dominios debido a restricciones en la administración de cuentas de usuario.

Tras activar Anti-Theft, puede optimizar la seguridad del dispositivo desde la ventana principal del programa en > **Configuración** > **Herramientas de seguridad** > **Anti-Theft**.

Opciones de optimización

No se creó una cuenta fantasma

La creación de una cuenta fantasma aumenta la posibilidad de localizar un dispositivo perdido o robado. Si marca su dispositivo como perdido, Anti-Theft bloqueará el acceso a sus cuentas de usuario activas para proteger sus 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 el dispositivo se marque como recuperado, lo que impedirá que alguien inicie sesión en otras cuentas de usuario o acceda a los datos de usuario.

Siempre que alguien inicie sesión en la cuenta fantasma cuando el equipo se encuentra en estado normal, se le enviará una notificación por correo electrónico con información sobre las actividades sospechosas en el equipo. Tras recibir la notificación por correo electrónico, puede decidir si desea marcar el equipo 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 o eliminar la cuenta.

Protección con 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 equipo resolverá este problema.

Para crear una contraseña para la cuenta de usuario, haga clic en **Administrar cuentas de Windows** y cambie la contraseña o siga las instrucciones que se indican a continuación:

1. Presione 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 presione **Intro**.

Inicio de sesión automático de cuentas de Windows

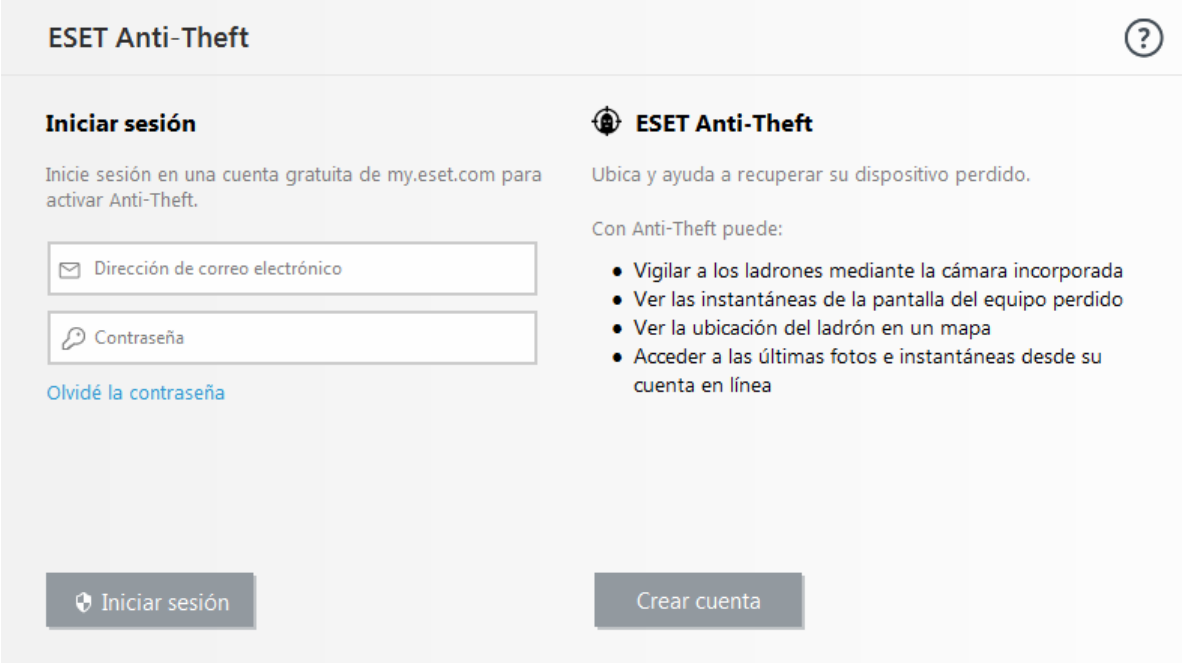
Su cuenta de usuario tiene activado el inicio de sesión automático; por lo tanto, la cuenta no está protegida frente a accesos no autorizados. Recibirá esta advertencia de optimización si al menos una cuenta de usuario tiene activado el inicio de sesión automático. Haga clic en **Desactivar inicio de sesión automático** para resolver este problema de optimización.

Inicio de sesión automático de la cuenta fantasma

El inicio de sesión automático está activado para la **cuenta fantasma** en su dispositivo. Cuando el dispositivo se encuentra 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 equipo. Haga clic en **Desactivar inicio de sesión automático** para resolver este problema de optimización.

Ingrese a su cuenta ESET HOME.

Para activar o desactivar Anti-Theft 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 ESET HOME:

- **Usar su dirección de correo electrónico y contraseña de ESET HOME**: escriba la **dirección de correo electrónico** y la **contraseña** que usó para crear su cuenta ESET HOME y haga clic en **Iniciar sesión**.

- **Usar su** cuenta de **Google/AppleID**: haga clic en **Continuar con Google** o **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se lo redirigirá a la página web de confirmación de ESET HOME. Para continuar, vuelva a la ventana de su producto de ESET. Para obtener más información sobre la cuenta de Google o el inicio sesión de AppleID, consulte las instrucciones de la Ayuda en línea de ESET HOME.

- **Analizar código QR**: haga clic en **Analizar código QR** para ver el código QR. Abra su aplicación móvil ESET HOME y escanee el código QR o apunte la cámara del dispositivo al 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 ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de ESET HOME.
Si olvidó su contraseña, haga clic en **Olvidé mi contraseña** y siga los pasos de la pantalla o consulte las instrucciones de la Ayuda en línea de ESET HOME.

Anti-Theft no admite Microsoft Windows Home Server.

Configure un nombre del dispositivo

El campo **Nombre del dispositivo** representa el nombre de su equipo (dispositivo) que se mostrará como identificador en todos los servicios de ESET HOME. El nombre del equipo se utiliza de forma predeterminada. Escriba el nombre del dispositivo o utilice el predeterminado y haga clic en **Continuar**.

Anti-Theft activado o desactivado

Esta ventana contiene un mensaje de confirmación cuando activa o desactiva Anti-Theft:

- Activado: su dispositivo ya está protegido por Anti-Theft, y puede administrar su seguridad de forma remota en el portal de ESET HOME mediante su cuenta.
- Desactivado: Anti-Theft está desactivado en este dispositivo, y todos los datos relacionados con <%ESET_ANTTHEFT%> correspondientes a este dispositivo se eliminan del portal de ESET HOME.

Error al agregar el nuevo dispositivo

Recibió un error durante la activación de Anti-Theft.

Las situaciones más habituales son:

- Error al iniciar sesión en ESET HOME
- No hay conectividad a Internet (o Internet no funciona por el momento)

Si no puede resolver el problema, póngase en contacto con el soporte técnico de ESET.

Secure Data

Secure Data es una característica de ESET Security Ultimate que le permite cifrar datos en su equipo y unidades extraíbles para proteger sus datos privados y evitar un uso incorrecto. Consulte las preguntas frecuentes sobre Secure Data ESET para obtener más información.

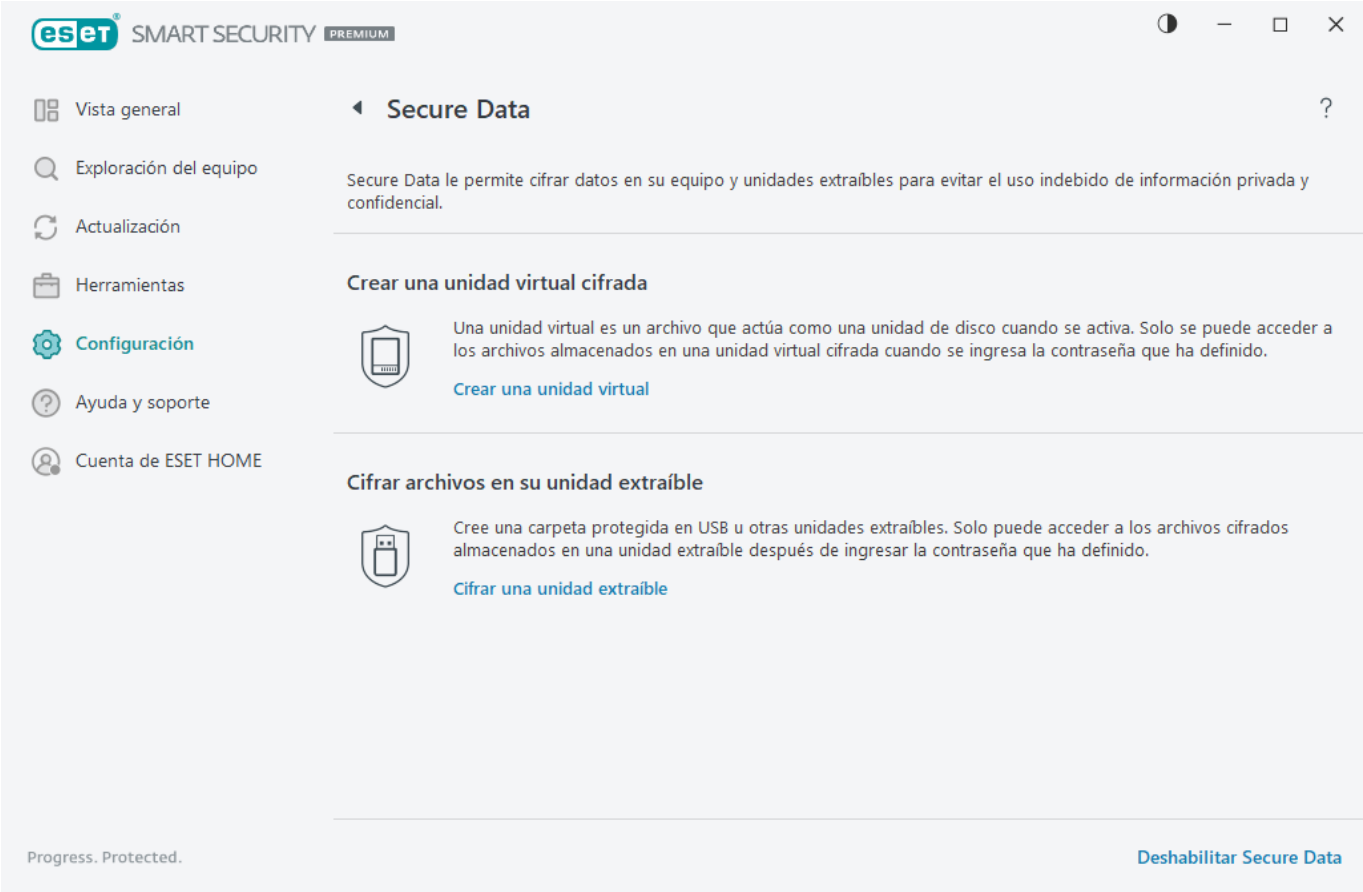
Para activar Secure Data, elija una de las siguientes opciones:

- En la ventana principal del programa > **Vista general**, haga clic en **CONFIGURAR** junto a **Secure Data**.
- En la ventana principal del programa > **Configuración** > **Herramientas de seguridad**, habilite el interruptor  **Secure Data**.

No se puede instalar ESET Endpoint Encryption en el mismo equipo en el que ya está instalado Secure Data.

Cuando Secure Data está activada, en la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad** > **Secure Data** y elija una de las siguientes opciones de cifrado:

- Crear una unidad virtual cifrada
- Cifrar archivos en su unidad extraíble



Crear una unidad virtual cifrada

Puede usar Secure Data para crear unidades virtuales cifradas. No hay límite para la cantidad de unidades que puede crear, siempre que tenga espacio en el disco duro. Siga los siguientes pasos 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 donde guardará la unidad virtual.

3. Ingrese un nombre para la unidad virtual y haga clic en **Guardar**.

4. Use el menú desplegable **Capacidad máxima** para definir el tamaño de la unidad virtual y haga clic en **Continuar**.

5. Establezca la contraseña deseada para la unidad virtual. Si no quiere que la unidad virtual se descifre automáticamente cuando inicia 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**. Se creó su unidad virtual y está lista para su uso. Se mostrará como un disco local si abre **Este equipo**.

Para acceder a la unidad cifrada después de reiniciar el equipo, busque el archivo de unidad cifrada (tipo de archivo `.eed`) que creó y ábralo con doble clic. Si se solicita, ingrese la contraseña que estableció al crear la unidad cifrada. La unidad se montará y se mostrará como un disco local en Este equipo. Cuando la unidad cifrada esté montada como un disco local, ese disco local y el contenido descifrado estarán disponibles para otros

usuarios de su equipo a menos que cierre sesión o lo reinicie.

> **¿Puedo quitar una unidad virtual?**
> Sí. Para quitar una unidad virtual cifrada, siga las instrucciones de nuestro artículo de Preguntas frecuentes de ESET Secure Data.

Cifrar archivos en su unidad extraíble

Secure Data le permite crear una carpeta cifrada en unidades extraíbles. Siga los pasos indicados a continuación para cifrar archivos en su unidad extraíble:

1. Inserte la unidad extraíble (unidad flash USB, disco duro USB) en el equipo.

2. En la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad** > **Secure Data** > **Cifrar una unidad extraíble**.

3. Seleccione el disco extraíble conectado que desea cifrar y haga clic en **Continuar**.
Haga clic en **Actualizar** para actualizar la lista de unidades que se pueden cifrar. Las unidades cifradas o no compatibles no se muestran en la lista.
Si desea descifrar la carpeta protegida en la unidad extraíble seleccionada en cualquier dispositivo Windows sin necesidad de instalar ESET Security Ultimate, seleccione **Descifrar la carpeta en cualquier dispositivo Windows**.

4. Establezca una contraseña para el directorio cifrado. Si no quiere que la unidad virtual se descifre automáticamente cuando inicia 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 está listo para su uso.

A partir de ahora, si conecta su disco extraíble en un equipo que no tiene instalado Secure Data, la carpeta cifrada no estará visible. Si se conecta la unidad extraíble en una computadora con Secure Data instalado, se le pedirá que ingrese la contraseña para descifrar la unidad extraíble. Si no ingresa ninguna contraseña, la carpeta cifrada será visible, pero no accesible.

Password Manager

Password Manager forma parte del paquete ESET Security Ultimate.

Es un gestor de contraseñas que protege y almacena sus contraseñas y datos personales. También incluye una característica de finalización de formulario que ahorra tiempo al rellenar los formularios web de manera automática y precisa.

Para obtener más información, consulte Password Manager Ayuda en línea.

- Password Manager instalación
- Comience a usar Password Manager.
- Administrar almacenamiento de Password Manager en ESET HOME

VPN

ESET VPN es parte del paquete de ESET Security Ultimate. VPN le permite mantener sus datos seguros, evitar el seguimiento no deseado y mejorar su privacidad mientras está en línea con la seguridad adicional de una dirección IP anónima.

Para comenzar a usar VPN, haga clic en **Descargar e instalar VPN.**

Para obtener más información, consulte ESET Virtual Private Network Ayuda en línea.

- VPN Introducción.
- VPN Instalación.
- Trabajar con VPN.

Identity Protection

ESET Identity Protection es la solución de seguridad que protege su información personal, crediticia y financiera. Identity Protection detecta la venta ilegal de su información personal proporcionando un monitoreo continuo. Con el Identity Protection, recibirá notificaciones en su teléfono móvil, equipo o tableta justo después de que su identidad esté en riesgo.

Para obtener más información, consulte ESET Identity Protection Ayuda en línea.

Importación y exportación de una configuración

Puede importar o exportar su archivo de configuración personalizado ESET Security Ultimate .xml desde el menú **Configuración**.

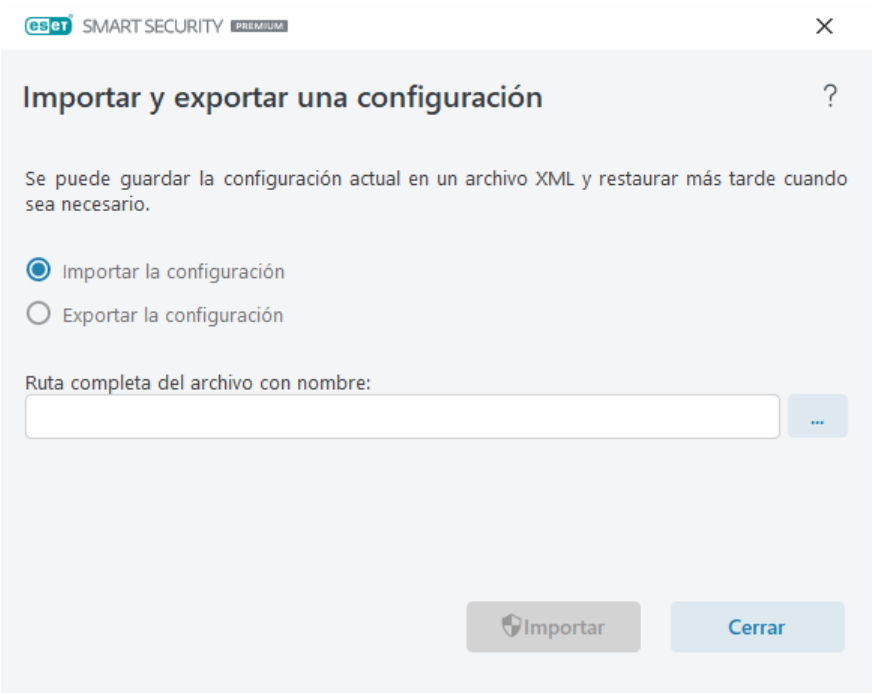
> **Instrucciones ilustradas**
> Consulte Importar o exportar los ajustes de configuración de ESET con un archivo .xml para obtener instrucciones ilustradas disponibles en inglés y en otros idiomas.

La importación y exportación de los archivos de configuración es útil si necesita hacer una copia de seguridad de la configuración actual de ESET Security Ultimate para usarla más adelante. La opción para exportar la configuración también es conveniente para usuarios que desean usar su configuración preferida en varios sistemas. Puede importar fácilmente un archivo .xml para transferir estas configuraciones.

Para importar una configuración, en la ventana principal del programa, haga clic en **Configuración** > **Importar/Exportar configuración** y seleccione **Importar configuración**. Ingrese el nombre del archivo de configuración o haga clic en el botón **...** para buscar el archivo de configuración que desea importar.

Para importar una configuración, en la ventana principal del programa, haga clic en **Configuración** > **Importar/Exportar configuración**. Seleccione **Importar configuración** e ingrese la ruta completa del archivo con el nombre. Haga clic en **...** para navegar hasta una ubicación en su equipo para guardar el archivo de configuración.

Es probable que encuentre un error mientras exporta las configuraciones, si no tiene suficientes derechos para escribir el archivo exportado en el directorio especificado.



Ayuda y soporte

Haga clic en **Ayuda y soporte** en la ventana del programa principal para mostrar información de soporte y herramientas de solución de problemas que le permitirán resolver los problemas que pueda encontrar.

Suscripción

- Solución de problemas de suscripción: haga clic en este enlace para buscar soluciones a problemas relacionados con la activación o el cambio de suscripción.
- Cambiar la suscripción: haga clic aquí para iniciar la ventana de activación y activar su producto. Si el dispositivo está conectado a ESET HOME, elija una suscripción de su cuenta ESET HOME o agregue una nueva.

Producto instalado

- Novedades: haga clic aquí para abrir la ventana de información sobre características nuevas y mejoradas.
- Acerca de ESET Security Ultimate – muestra información acerca de una copia de ESET Security Ultimate.
- Resolución de problemas del producto: haga clic en este enlace para buscar soluciones a los problemas más frecuentes.
- **Cambiar producto**: haga clic para ver si puede cambiar ESET Security Ultimate a una línea diferente de productos con la suscripción actual.

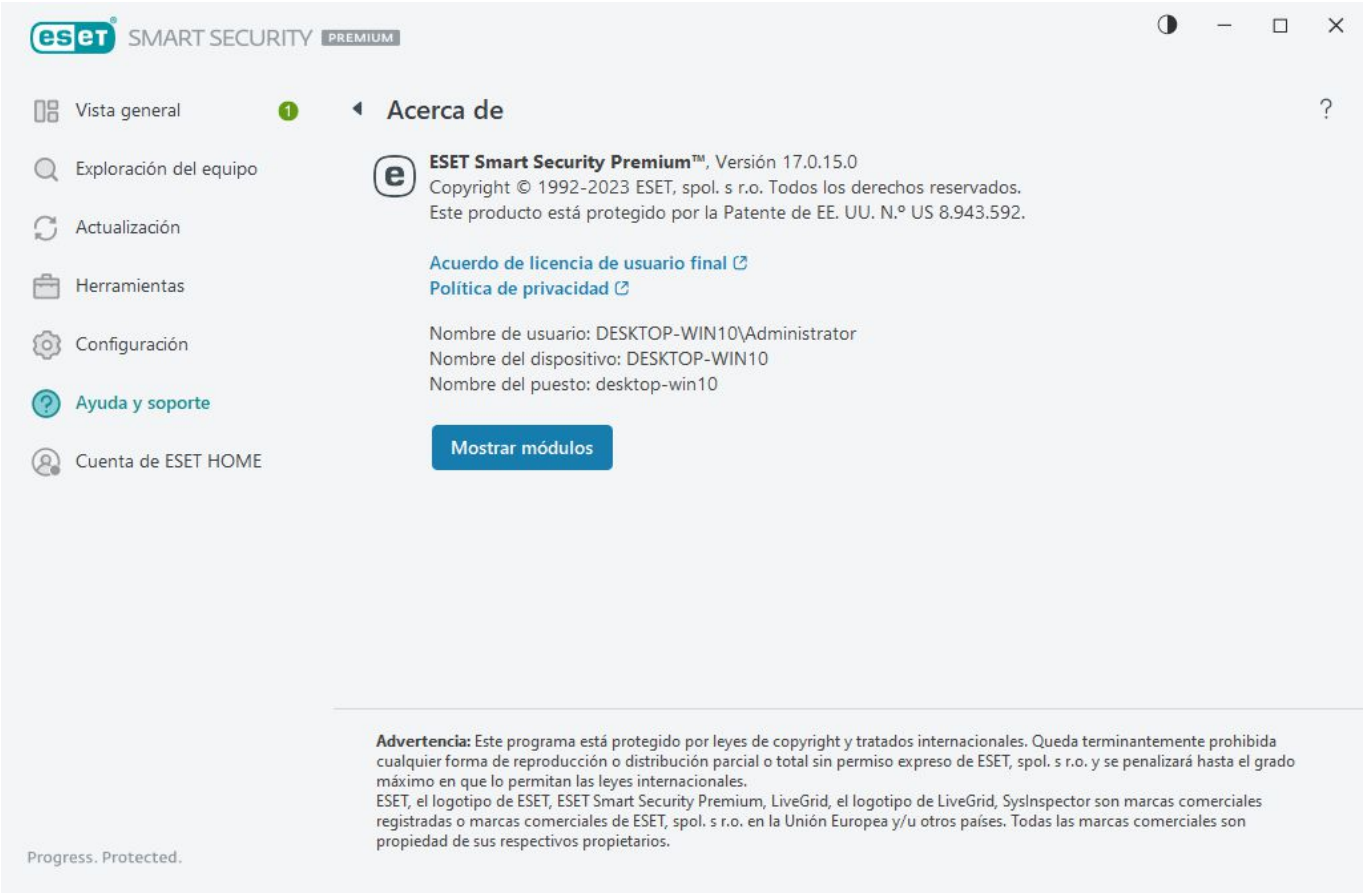
Página de ayuda – haga clic en este vínculo para abrir las páginas de ayuda de ESET Security Ultimate.

Soporte técnico

Base de conocimientos – la base de conocimiento de ESET contiene respuestas a las preguntas más frecuentes y soluciones recomendadas para varios problemas. La actualización regular por parte de los especialistas técnicos de ESET convierte a la base de conocimiento en la herramienta más potente para resolver varios problemas.

Acerca de ESET Security Ultimate

Esta ventana brinda detalles sobre la versión instalada de ESET Security Ultimate y su equipo.



Haga clic en **Mostrar módulos** para ver información sobre la lista de módulos del programa cargados.

- Puede copiar información sobre los módulos al portapapeles al hacer clic en **Copiar**. Esto puede resultar útil durante la resolución de problemas o al 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.

ESET Noticias

En esta ventana ESET Security Ultimate le informan las noticias de ESET de forma regular.

La mensajería del producto ha sido diseñada para informar a los usuarios de ESET acerca de noticias y otras comunicaciones. El envío de mensajes de marketing requiere el consentimiento de un usuario. Los mensajes de

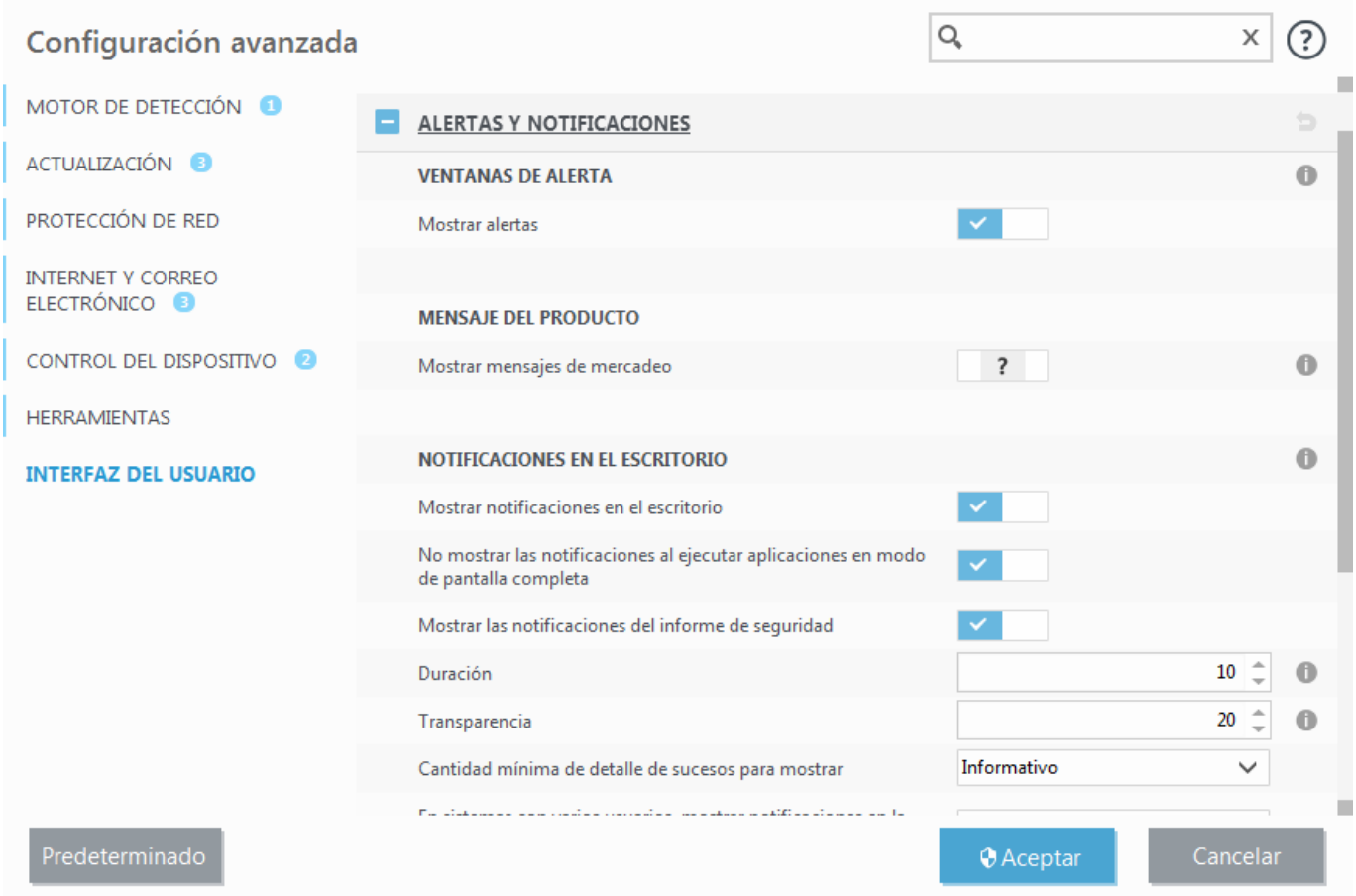
marketing no se envían a un usuario de forma predeterminada (se muestra como un signo de interrogación). Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no está interesado en recibir material de marketing de ESET, desactive la opción **Mostrar mensajes de marketing**.

Para activar o desactivar la recepción de mensajes de marketing mediante una ventana de notificación, siga las instrucciones a continuación.

1. Abre la configuración avanzada.

2. Haga clic en **Notificaciones** > **Alertas interactivas**.

3. Modificar la opción **Mostrar mensajes de marketing.**



Enviar datos de configuración del sistema

Con el fin de proporcionar asistencia lo más rápido y con la mayor exactitud posible, ESET solicita información sobre la configuración de ESET Security Ultimate, información detallada sobre el sistema y los procesos activos (Archivos de registro ESET SysInspector), y los datos de registro. ESET usará estos datos únicamente para proporcionar asistencia técnica al cliente.

Después de enviar el formulario web, los datos de configuración de su sistema se enviarán a ESET. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Al 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 Soporte 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 su ticket y se perderán los datos de configuración del sistema. Si no se pueden enviar los datos de configuración del sistema, complete el formulario web y espere las instrucciones del Soporte técnico.

Soporte técnico

En la ventana principal del programa, haga clic en **Ayuda y soporte** > **Soporte técnico**.

Comuníquese con el 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 Enviar los datos de configuración del sistema antes de rellenar el formulario web.

Obtener información para soporte técnico

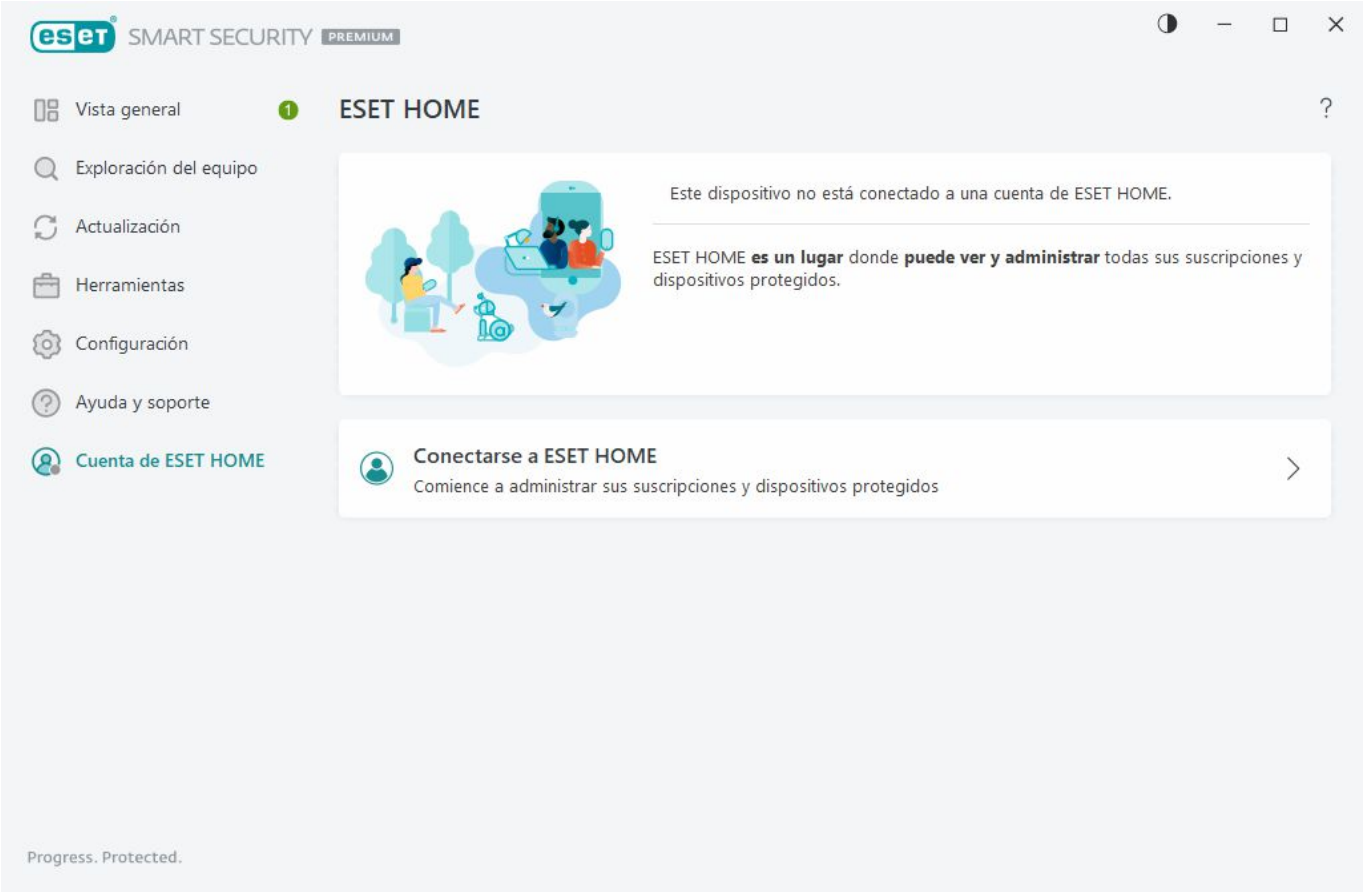
Detalles de soporte técnico: cuando se lo solicite, puede copiar y enviar información a Soporte técnico de ESET (como los detalles de la suscripción, el nombre del producto, la versión del producto, el sistema operativo y la información del equipo).

ESET Log Collector - enlaza al artículo de la Base de conocimiento de ESET, de donde puede descargar la utilidad ESET Log Collector, una aplicación que recopila información y registros automáticamente de un equipo para ayudar a resolver problemas más rápidamente. Para obtener más información, haga clic ESET Log Collector aquí.

Haga clic en Habilitar registros avanzados para crear registros avanzados de todas las funciones disponibles a fin de ayudar a los desarrolladores a diagnosticar y resolver problemas. El detalle mínimo para los registros está ajustado en el nivel de **Diagnóstico**. El registro avanzado se desactivará automáticamente después de dos horas, a menos que lo detenga antes haciendo clic en **Detener registro avanzado**. Cuando se crean todos los registros, se muestra la ventana de notificación que proporciona acceso directo a la carpeta de Diagnóstico con los registros creados.

Cuenta ESET HOME

Puede revisar el estado de conexión de la cuenta ESET HOME en la ventana principal del programa > **cuenta ESET HOME**.



Este dispositivo no está conectado a una cuenta ESET HOME

Haga clic en Conectar a ESET HOME para conectar su dispositivo a ESET HOME y administrar sus suscripciones y dispositivos protegidos. Puede renovar, actualizar o ampliar la suscripción y ver detalles importantes de ella. En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar diferentes suscripciones, descargar productos en sus dispositivos, comprobar el estado de seguridad del producto o compartir suscripciones por correo electrónico. Para obtener más información, visite ayuda en línea de ESET HOME.

Este dispositivo está conectado a una cuenta ESET HOME

Puede administrar la seguridad de su dispositivo de forma remota con el portal o la aplicación para dispositivos móviles de ESET HOME . Haga clic en **App Store** o **Google Play** para mostrar un código QR que puede analizar con su teléfono móvil para descargar la aplicación para dispositivos móviles de ESET HOME de App Store o Google Play.

Cuenta de ESET HOME—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 su ESET HOME cuenta, haga clic en **Desconectar de ESET HOME** > **Desconectar**. La suscripción que se usa para la activación permanecerá activa y su dispositivo estará protegido.

Conectarse a ESET HOME

Conecte su dispositivo a ESET HOME para ver y administrar todas las suscripciones y los dispositivos de ESET activados. Puede renovar, actualizar o ampliar la suscripción y ver detalles importantes de ella. En el portal de administración o la aplicación para dispositivos móviles de ESET HOME, puede agregar diferentes suscripciones, descargar productos en sus dispositivos, comprobar el estado de seguridad del producto o compartir suscripciones por correo electrónico. Para obtener más información, visite ayuda en línea de ESET HOME.

Conecte su dispositivo a ESET HOME:

Si se conecta a ESET HOME durante la instalación o al seleccionar **Usar 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 Security Ultimate con una suscripción añadida a su cuenta ESET HOME, puede conectar su dispositivo a ESET HOME mediante el portal ESET HOME: Siga las instrucciones en la ESET HOMEGuía de ayuda en línea y permita la conexión en ESET Security Ultimate.

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. Ingrese a su cuenta ESET HOME.

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

3. Defina un **Nombre del dispositivo y** haga clic en **Continuar**.

4. Tras una conexión correcta, se muestra una ventana de detalles. Haga clic en **Listo**.

Inicie sesión en ESET HOME

Hay varios métodos disponibles para iniciar sesión en su cuenta ESET HOME:

- **Usar su dirección de correo electrónico y contraseña de ESET HOME**: escriba la **dirección de correo electrónico** y la **contraseña** que usó para crear su cuenta ESET HOME y haga clic en **Iniciar sesión**.

- **Usar su** cuenta de **Google/AppleID**: haga clic en **Continuar con Google** o **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se lo redirigirá a la página web de confirmación de ESET HOME. Para continuar, vuelva a la ventana de su producto de ESET. Para obtener más información sobre la cuenta de Google o el inicio sesión de AppleID, consulte las instrucciones de la Ayuda en línea de ESET HOME.

- **Analizar código QR**: haga clic en **Analizar código QR** para ver el código QR. Abra su aplicación móvil ESET HOME y escanee el código QR o apunte la cámara del dispositivo al código QR. Para obtener más información, consulte las instrucciones de la Ayuda en línea de ESET HOME.

Si no tiene una cuenta ESET HOME, haga clic en **Crear cuenta** para registrarse o consulte las instrucciones de la Ayuda en línea de ESET HOME.
Si olvidó su contraseña, haga clic en **Olvidé 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 pudimos encontrar una cuenta que coincida con la dirección de correo electrónico ingresada

La dirección de correo electrónico que ha ingresado no coincide con ninguna cuenta ESET HOME. Haga clic en **Atrás** y escriba la dirección de correo electrónico y la contraseña correctas.

Para iniciar sesión debe crear una cuenta ESET HOME. Si no tiene una cuenta ESET HOME, haga clic en **Atrás** > **Crear cuenta** o consulte Crear una nueva cuenta ESET HOME.

El usuario y la contraseña no coinciden

La contraseña ingresada no coincide con la dirección de correo electrónico ingresada. Haga clic en **Atrás**, escriba la contraseña correcta y verifique que la dirección de correo electrónico escrita sea correcta. Si no puede iniciar sesión, haga clic en **Atrás** > **¿Olvidó su contraseña?** para restablecer su contraseña y siga los pasos de la pantalla o consulte Olvidé 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 redes sociales. Para iniciar sesión en ESET HOME, haga clic en **Continuar con Google** o **Continuar con Apple** e inicie sesión en la cuenta correspondiente. Tras iniciar sesión correctamente, se lo redirigirá a la página web de confirmación de ESET HOME. Puede desconectar su cuenta de redes sociales de su cuenta ESET HOME en el portal ESET HOME.

Contraseña incorrecta

Este error puede producirse si su ESET Security Ultimate ya está conectado a ESET HOME y está realizando cambios que requieren que inicie sesión (por ejemplo, desactivar Anti-Theft) y la contraseña que ingresó no coincide con su cuenta. Haga clic en **Atrás** y escriba la contraseña correcta. Si no puede iniciar sesión, haga clic en **Atrás** > **¿Olvidó su contraseña?** para restablecer su contraseña y siga los pasos de la pantalla o consulte Olvidé mi contraseña de ESET HOME.

Agregar dispositivo en ESET HOME

Si ya ha instalado y activado ESET Security Ultimate con una suscripción añadida a su cuenta 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 Security Ultimate muestra la ventana de diálogo **Conectar este dispositivo a una cuenta ESET HOME** con el nombre de su cuenta ESET HOME. Haga clic en **Permitir** para conectar el dispositivo a la cuenta ESET HOME mencionada.

> Si no hay interacción, la solicitud de conexión se cancelará automáticamente después de aproximadamente 30 minutos.

Configuración avanzada

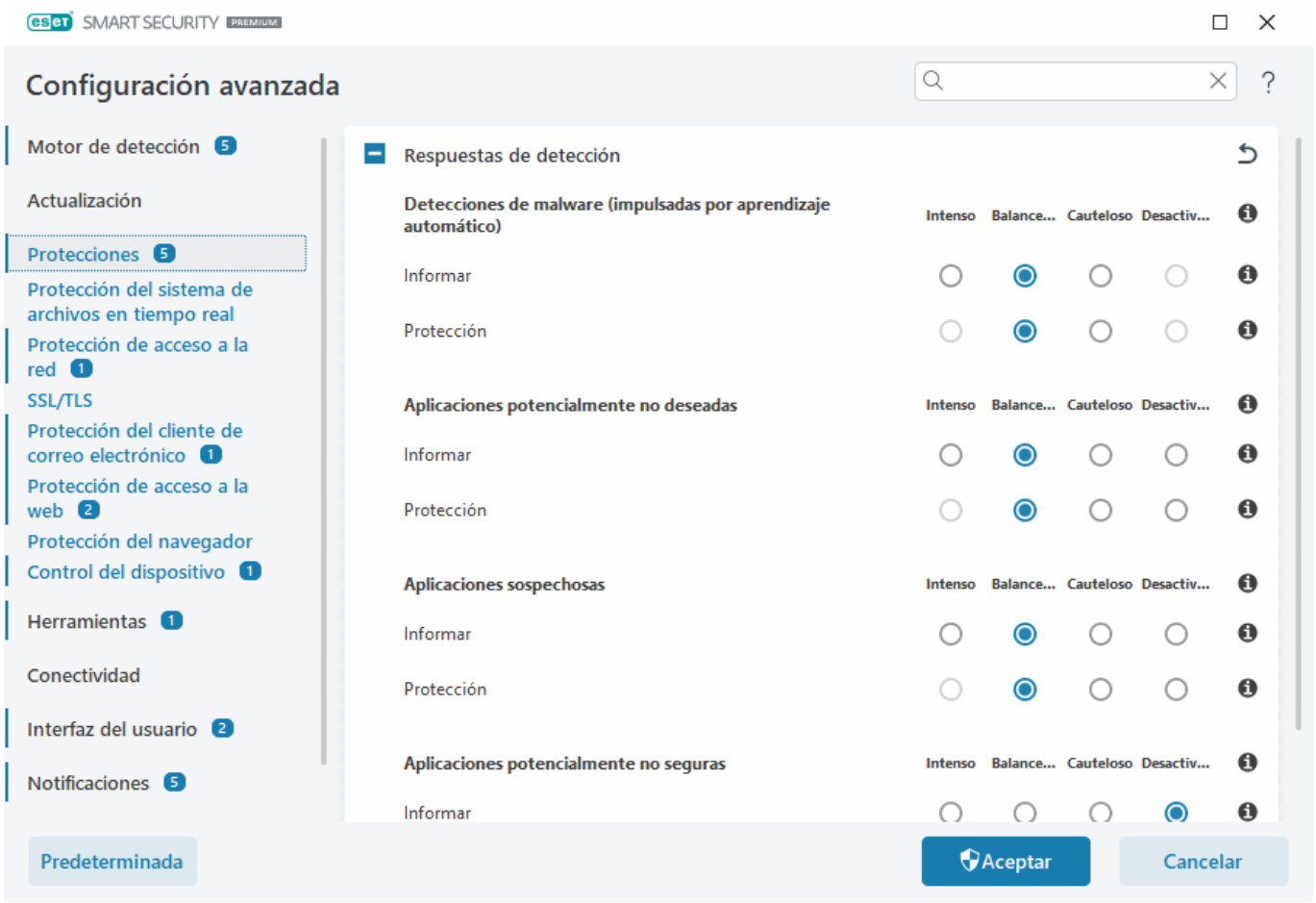
La configuración avanzada le permite configurar ESET Security Ultimate ajustes detallados según sus necesidades.

Para abrir la Configuración avanzada, abra la ventana principal del programa y presione la tecla **F5** del teclado o haga clic en **Configuración** > **Configuración avanzada**.

> Según su Configuración de acceso, es posible que se le solicite que escriba una contraseña para abrir la Configuración avanzada.

En la configuración avanzada, puede realizar los siguientes ajustes:

- Motor de detección
- Actualización
- Protecciones
- Herramientas
- Conectividad
- Interfaz del usuario
- Notificaciones
- Configuración de privacidad



Motor de detección

Configuración avanzada > **Motor de detección** le permite configurar las siguientes opciones:

- Exclusiones
- Opciones avanzadas
- Explorador del tráfico de red

Exclusiones

Las **Exclusiones** permiten excluir objetos del motor de detección. Para asegurarse de que todos los objetos se exploren, recomendamos crear únicamente exclusiones cuando sea absolutamente necesario. Las situaciones donde es posible que necesite excluir un objeto pueden incluir la exploración de las entradas de una base de datos grande que podría reducir la velocidad de su equipo durante una exploración o software que entra en conflicto con la exploración.

Exclusiones de rendimiento – permiten excluir archivos y carpetas de la exploración. También son útiles para excluir la exploración a nivel de archivos de aplicaciones de juegos o cuando provoca un comportamiento anormal del sistema o para obtener un mejor rendimiento.

Las Exclusiones de la detección permiten excluir objetos de la detección por el nombre, ruta o hash de la detección. Las exclusiones de la detección no excluyen archivos y carpetas de la exploración como las exclusiones

de rendimiento. Las exclusiones de la detección excluyen objetos solo cuando el motor de detección los detecta y existe una regla pertinente en la lista de exclusiones.

No debe confundirse con otros tipos de exclusiones:

- Exclusiones de procesos – Todas las operaciones de archivos atribuidas a procesos de aplicaciones excluidas se excluyen de la exploración (podría ser necesario para mejorar la velocidad de la copia de seguridad y la disponibilidad del servicio),
- Extensiones de archivo excluidas,
- Exclusiones de HIPS,
- Filtro de exclusión para la protección basada en la nube.

Exclusiones de rendimiento

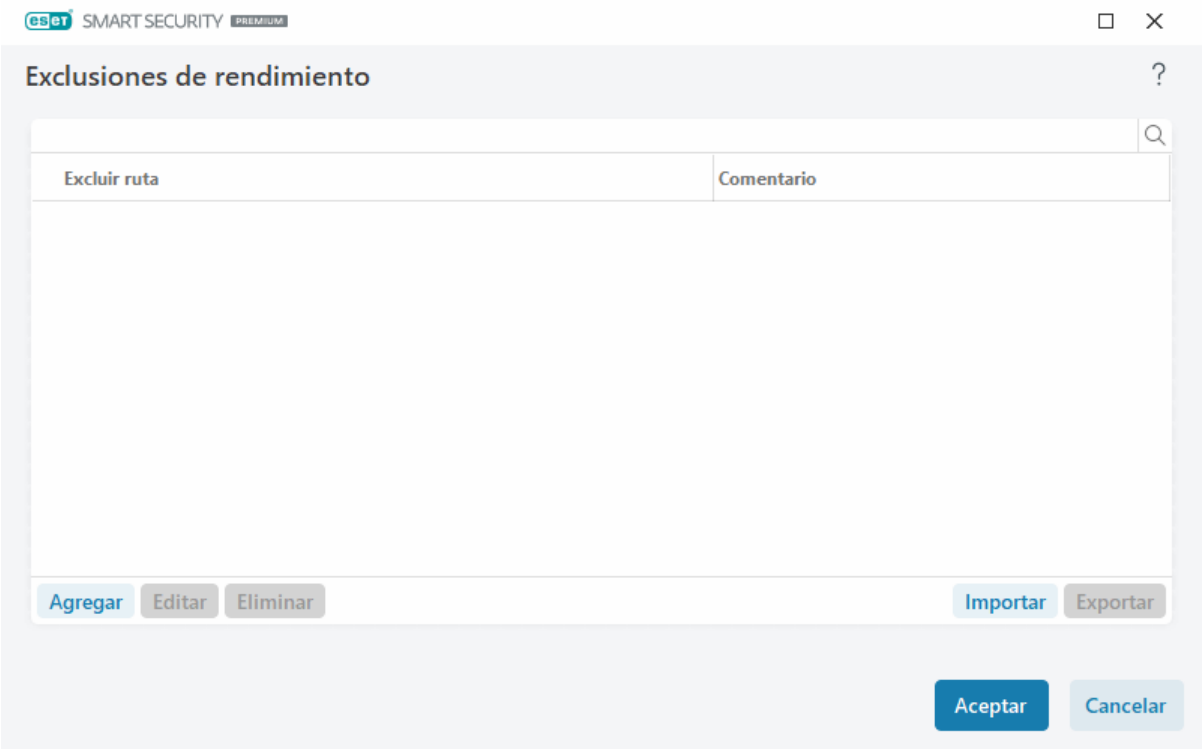
Las exclusiones de rendimiento permiten excluir archivos y carpetas de la exploración.

Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos crear exclusiones únicamente cuando sea absolutamente necesario. Sin embargo, existen situaciones en las que deba excluir un objeto; por ejemplo, las entradas de una base de datos grande que podría reducir la velocidad de su equipo durante una exploración o software que entra en conflicto con la exploración.

Puede añadir archivos y carpetas en la lista de exclusiones para que se excluyan de la exploración en Configuración avanzada > **Motor de detección** > **Exclusiones** > **Exclusiones de rendimiento** > **Editar**.

> No debe confundirse con Exclusiones de detección, Extensiones de archivo excluidas, Exclusiones de HIPS o Exclusiones de procesos.

Para excluir un objeto (ruta: archivo o carpeta) de la exploración, haga clic en **Agregar** e ingrese la ruta aplicable o selecciónelo en la estructura de árbol.



Una amenaza dentro de un archivo no se detectará por el módulo de **protección del sistema de archivos en tiempo real** o módulo de **exploración del equipo** si un archivo cumple con los criterios para la exclusión de la exploración.

Elementos de control

- **Agregar** – excluye objetos de la detección.
- **Editar** – le permite editar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (CTRL + clic para seleccionar múltiples entradas).

Agregar o editar exclusión de rendimiento

Esta ventana de diálogo excluye una ruta específica (archivo o directorio) para este equipo.

Seleccione la ruta o introdúzcala manualmente

Para elegir una ruta que corresponda, haga clic en **...** en el campo **Ruta**.
Al escribir manualmente, vea más ejemplos de formatos de exclusiones a continuación.

Puede usar comodines para excluir un grupo de archivos. Un signo de interrogación (*?*) representa un carácter único, mientras que un asterisco (***) representa una cadena de cero o más caracteres.

Formato de las exclusiones

• Si desea excluir todos los archivos y subcarpetas en una carpeta, escriba la ruta a la carpeta y use la máscara ***
• Si solo desea excluir archivos doc, use la máscara **.doc*
• Si el nombre del archivo ejecutable tiene un número determinado de caracteres (que varían) y solo conoce el primero (por ejemplo, "D"), use el siguiente formato:
D????.exe (los símbolos de interrogación reemplazan a los caracteres faltantes/desconocidos)
Ejemplos:
• *C:\Tools**: la ruta debe terminar con la barra diagonal inversa (\) y el asterisco (*) para indicar que es una carpeta y que se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
• *C:\Tools*.**: el mismo comportamiento que *C:\Tools**
• *C:\Tools* – La carpeta *Tools* no se excluirá.. Desde el punto de vista del módulo de exploración, *Tools* también puede ser un nombre de archivo.
• *C:\Tools*.dat* – Excluirá archivos .dat en la carpeta *Tools*.
• *C:\Tools\sg.dat* – Excluirá este archivo en particular ubicado en la ruta exacta.

Variables del sistema en las exclusiones

Puede usar variables del sistema como %PROGRAMFILES% para definir las exclusiones de exploración.
• Para excluir la carpeta Archivos de programa con esta variable del sistema, use la ruta *%PROGRAMFILES%** (recuerde que debe agregar barra diagonal inversa al final de la ruta) cuando agregue exclusiones.
• Si desea excluir todos los archivos y carpetas en un subdirectorio de *%PROGRAMFILES%*, use la ruta *%PROGRAMFILES%\Directorio_excluido**

Expandir la lista de variables del sistema compatibles

Las siguientes variables pueden usarse en el formato de exclusión de ruta:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
No se admiten las variables del sistema específicas del usuario (p. ej., *%TEMP%* o *%USERPROFILE%*) ni las variables de entorno (p. ej., *%PATH%*).

No se admiten comodines en el medio de una ruta

Es posible que el uso de comodines en el medio de la ruta (p. ej., *C:\Tools*\Data\file.dat*) funcione, pero no se admite oficialmente para las exclusiones de rendimiento.
Cuando usa Exclusiones de la detección, no hay restricciones para el uso de comodines en el medio de la ruta.

Orden de exclusiones

- No hay opciones para ajustar el nivel de prioridad de las exclusiones con los botones arriba/abajo (en cuanto a las reglas de firewall donde las reglas se ejecutan de arriba a abajo).
- Cuando la primera regla aplicable es encontrada por el explorador, la segunda regla aplicable no será evaluada.
- Mientras menos reglas haya, mejor es el desempeño del explorador.
- Evite la creación de reglas concurrentes.

Formato de las exclusiones de ruta

Puede usar comodines para excluir un grupo de archivos. Un signo de interrogación (*?*) representa un carácter único, mientras que un asterisco (***) representa una cadena de cero o más caracteres.

Formato de las exclusiones

- Si desea excluir todos los archivos y subcarpetas en una carpeta, escriba la ruta a la carpeta y use la máscara ***
- Si solo desea excluir archivos doc, use la máscara **.doc*
- Si el nombre del archivo ejecutable tiene un número determinado de caracteres (que varían) y solo conoce el primero (por ejemplo, "D"), use el siguiente formato:
D????.exe (los símbolos de interrogación reemplazan a los caracteres faltantes/desconocidos)

Ejemplos:

- *C:\Tools**: la ruta debe terminar con la barra diagonal inversa (\) y el asterisco (*) para indicar que es una carpeta y que se excluirá todo el contenido de la carpeta (archivos y subcarpetas).
- *C:\Tools*.**: el mismo comportamiento que *C:\Tools**
- *C:\Tools* – La carpeta *Tools* no se excluirá.. Desde el punto de vista del módulo de exploración, *Tools* también puede ser un nombre de archivo.
- *C:\Tools*.dat* – Excluirá archivos .dat en la carpeta *Tools*.
- *C:\Tools\sg.dat* – Excluirá este archivo en particular ubicado en la ruta exacta.

Variables del sistema en las exclusiones

Puede usar variables del sistema como %PROGRAMFILES% para definir las exclusiones de exploración.

- Para excluir la carpeta Archivos de programa con esta variable del sistema, use la ruta *%PROGRAMFILES%** (recuerde que debe agregar barra diagonal inversa al final de la ruta) cuando agregue exclusiones.
- Si desea excluir todos los archivos y carpetas en un subdirectorio de *%PROGRAMFILES%*, use la ruta *%PROGRAMFILES%\Directorio_excluido**

Expandir la lista de variables del sistema compatibles

Las siguientes variables pueden usarse en el formato de exclusión de ruta:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

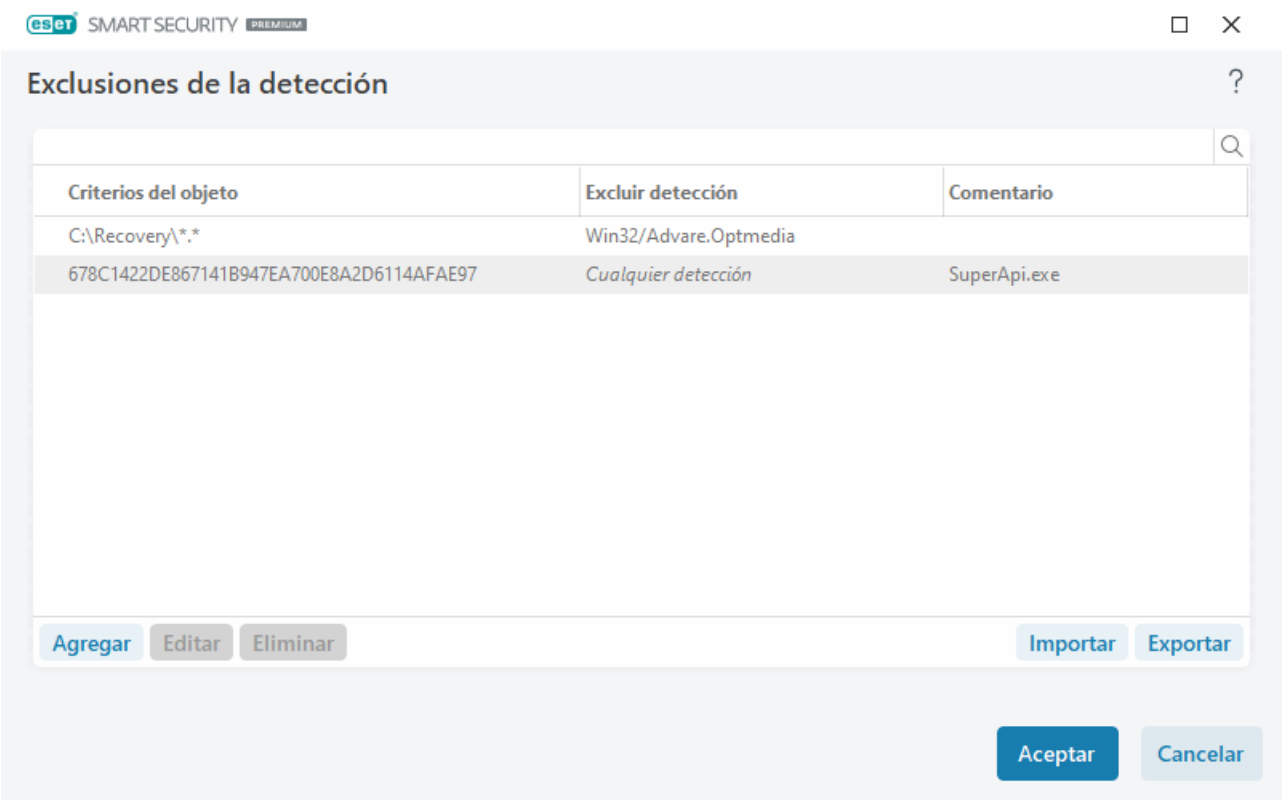
No se admiten las variables del sistema específicas del usuario (p. ej., *%TEMP%* o *%USERPROFILE%*) ni las variables de entorno (p. ej., *%PATH%*).

Exclusiones de la detección

Las exclusiones de la detección permiten excluir objetos de la detección mediante el filtro del nombre de la detección, la ruta del objeto o su hash.

Cómo funcionan las exclusiones de la detección

Las exclusiones de la detección no excluyen archivos y carpetas de la exploración como las Exclusiones de rendimiento. Las exclusiones de la detección excluyen objetos solo cuando el motor de detección los detecta y existe una regla pertinente en la lista de exclusiones.
Por ejemplo (consulte la primera fila de la imagen a continuación), cuando se detecta un objeto como Win32/Adware.Optmedia y el archivo detectado es *C:\Recovery\file.exe*. En la segunda fila, cada archivo que tenga el hash SHA-1 pertinente siempre será excluido independientemente del nombre de la detección.



Para garantizar que se detecten todas las amenazas, recomendamos crear exclusiones solo cuando sea absolutamente necesario.

Para añadir archivos y carpetas a la lista de exclusiones, abra Configuración avanzada > **Motor de detección** >**Exclusiones** > **Exclusiones de la detección** > **Editar**.

No debe confundirse con Exclusiones de rendimiento, Extensiones de archivo excluidas, Exclusiones de HIPS o Exclusiones de procesos.

Para excluir un objeto (por su nombre de detección o hash) del motor de detección, haga clic en **Agregar**.

Para Aplicaciones potencialmente no deseadas y Aplicaciones potencialmente no seguras, también se puede crear la exclusión por su nombre de detección:

- En la ventana de alerta que informa sobre la detección (haga clic en **Mostrar opciones avanzadas** y luego

seleccione **Excluir de la detección**).

• En el menú contextual Archivos de registro, con el asistente para Crear exclusiones de la detección.

• Al hacer clic en **Herramientas** > **Cuarentena** y luego clic derecho en el archivo en cuarentena y seleccionar **Restaurar y excluir de la exploración** del menú contextual.

Criterios de objeto de exclusiones de la detección

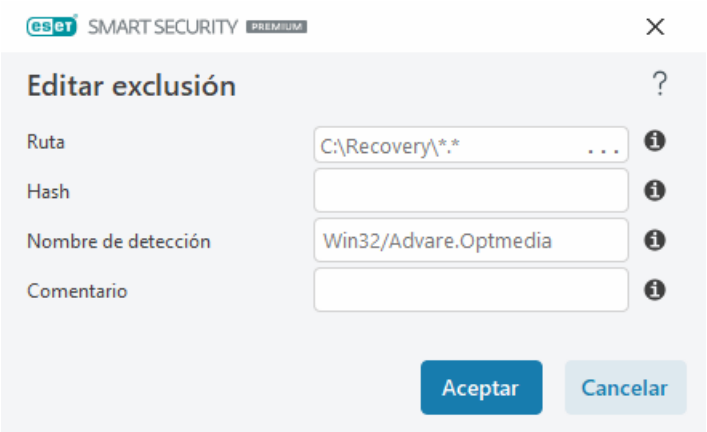
- **Ruta** – Limite una exclusión de la detección para una ruta específica (o cualquiera).
- **Nombre de detección**: si se muestra el nombre de una detección junto a un archivo excluido, significa que el archivo solo se excluirá en lo que respecta a la dicha detección, pero no se excluirá completamente. Si dicho archivo más tarde se infecta con otro malware, el módulo antivirus lo detectará.
- **Hash**: excluye un archivo en base a hash específico SHA-1, independientemente del tipo de archivo, su ubicación, nombre o extensión.

Agregar o editar exclusiones de la detección

Excluir detección

Se debe proporcionar un nombre válido de detección de ESET. Para un nombre de detección válido, vaya a Archivos de registro y seleccione **Detecciones** en el menú desplegable de archivos de registro. Esto resulta útil cuando se detecta una muestra con falso positivo en ESET Security Ultimate. Las exclusiones de infiltraciones reales son muy peligrosas, considere excluir solo archivos/directorios afectados haciendo clic en **...** en el campo **Ruta** o solo temporalmente. Las exclusiones también se aplican para aplicaciones potencialmente no deseadas, aplicaciones potencialmente peligrosas o aplicaciones sospechosas.

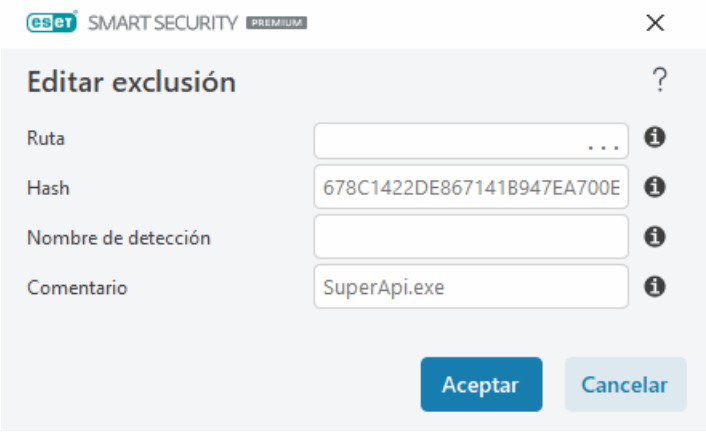
Consulte también Formato de las exclusiones de ruta.



Consulte el ejemplo de Ejemplo de exclusiones de la detección a continuación.

Excluir hash

Excluye un archivo en base a hash específico SHA-1, independientemente del tipo de archivo, su ubicación, nombre o extensión.



Exclusiones por nombre de detección

Para excluir una detección específica por su nombre, ingrese el nombre de detección válido: Win32/Adware.Optmedia

También puede usar el siguiente formato cuando excluya una detección en la ventana de alerta de ESET Security Ultimate:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Elementos de control

- **Agregar** – excluye objetos de la detección.
- **Editar** – le permite editar las entradas seleccionadas.
- **Eliminar**: quita las entradas seleccionadas (CTRL + clic para seleccionar múltiples entradas).

Asistente para crear exclusiones de la detección

También puede crear una exclusión de la detección desde el menú contextual de Archivos de registro (no disponible para las detecciones de malware):

1. En la ventana principal del programa, haga clic en **Herramientas** > **Archivos de registro**.
2. Haga clic derecho en una detección del **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 **Modificar criterios**:

- **Archivos exactos** – Excluir cada archivo por hash SHA-1.
- **Detección** – Excluir cada archivo por nombre de detección.
- **Ruta + Detección** – Excluir cada archivo por ruta y nombre de detección, incluido el nombre del archivo (p. ej., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

La opción recomendada se selecciona de forma predeterminada en función del tipo de detección.

De manera opcional, puede agregar un **Comentario** antes de hacer clic en **Crear exclusión**.

Opciones avanzadas del motor de detección

Activar análisis avanzado mediante AMSI es la herramienta Microsoft Antimalware Scan Interface que permite analizar scripts PowerShell, scripts ejecutados por Windows Script Host y datos analizados con AMSI SDK.

Explorador del tráfico de red

El explorador de tráfico de red proporciona protección contra malware para protocolos de aplicación, que integra múltiples técnicas avanzadas de exploración de malware. El explorador de tráfico de red explora los protocolos HTTP(S), POP3(S) e IMAP(S) automáticamente, independientemente del navegador de Internet o del cliente de correo electrónico. Puede habilitar/deshabilitar el explorador de tráfico de red en Configuración avanzada > **Motor de detección** > **Explorador de tráfico de red**.

Habilitar explorador de tráfico de red: si desactiva esta opción, no se explorarán los protocolos HTTP(S), POP3(S) e IMAP(S). Tenga en cuenta que las siguientes funciones ESET Security Ultimate requieren que el explorador de tráfico de red esté habilitado:

- Protección de acceso a la web
- Control parental
- Seguridad y privacidad del navegador
- Banca y navegación seguras
- SSL/TLS
- Protección antiphishing
- Protección del cliente de correo electrónico

Protección basada en la nube

ESET LiveGrid® (creada en el sistema avanzado de alerta temprana ESET ThreatSense.Net) utiliza los datos que los usuarios de ESET enviaron de todo el mundo y los envía al laboratorio de investigación de ESET. Al proporcionar muestras sospechosas y metadatos, ESET LiveGrid® nos permite reaccionar inmediatamente ante las necesidades de nuestros clientes y mantener a ESET receptivo a las últimas amenazas.

ESET LiveGuard es una característica que añade una capa de protección específicamente diseñada para mitigar amenazas nunca vistas. Cuando esta opción 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.

Se encuentran disponibles las siguientes opciones:

Habilitar el sistema de reputación de ESET LiveGrid®, el sistema de comentarios de ESET LiveGrid® y ESET LiveGuard

El sistema de reputación de ESET LiveGrid® ofrece listas blancas y negras basadas en la nube. El sistema de comentarios de ESET LiveGrid® recopilará información acerca de su equipo relacionada con las amenazas recién detectadas. La función ESET LiveGuard detecta nuevas amenazas nunca vistas mediante el análisis de su comportamiento en un entorno aislado.

Puede verificar la reputación de los Procesos en ejecución y de los archivos directamente desde la interfaz del programa o desde el menú contextual, con información adicional disponible en ESET LiveGrid®. Con la protección proactiva de ESET LiveGuard, se bloquea la ejecución de nuevos archivos hasta recibir el resultado del análisis.

Habilitar el sistema de reputación de ESET LiveGrid®

El sistema de reputación de ESET LiveGrid® ofrece listas blancas y negras basadas en la nube.

Puede verificar la reputación de los Procesos activos y de los archivos directamente desde la interfaz del programa o desde el menú contextual, con información adicional disponible en ESET LiveGrid®.

Habilitar el sistema de comentarios de ESET LiveGrid®

Además del sistema de reputación de ESET LiveGrid®, el sistema de comentarios de ESET LiveGrid® recopilará información sobre su equipo relacionada con las amenazas recientemente detectadas. Esta información puede incluir:

- Muestra o copia del archivo en el que apareció la amenaza
- Ruta al archivo
- Nombre del archivo
- Fecha y hora
- El proceso por el que apareció la amenaza en el ordenador
- Información sobre el sistema operativo del equipo

En forma predeterminada, ESET Security Ultimate está configurado para enviar archivos sospechosos al laboratorio de virus de ESET para su análisis detallado. Los archivos con extensiones específicas, como *.doc* o *.xls*, siempre se excluyen. También puede agregar otras extensiones si hay archivos específicos que usted o su organización prefieren no enviar.

Obtenga más información sobre el envío de datos relevantes en la Política de privacidad.

Puede elegir no habilitar ESET LiveGrid®

No perderá funcionalidad alguna en el software, pero, en algunos casos, ESET Security Ultimate puede responder más rápido a las nuevas amenazas cuando se habilita ESET LiveGrid®. Si ya usó ESET LiveGrid® y lo deshabilitó, es posible que hayan quedado paquetes de datos para enviar. Aun después de su desactivación, dichos paquetes se enviarán a ESET. Una vez que se envíe toda la información actual, no se crearán más paquetes.

Lea más sobre ESET LiveGrid® en el glosario.
Consulte nuestras instrucciones ilustradas disponibles en inglés y en otros idiomas para activar o desactivar ESET LiveGrid® en ESET Security Ultimate.

Configuración de la protección basada en la nube, en la Configuración avanzada

Para acceder a la configuración avanzada de ESET LiveGrid® y ESET LiveGuard, abra la Configuración avanzada > **Motor de detección** > **Protección basada en la nube**.

- **Habilitar el sistema de reputación ESET LiveGrid® (recomendado)** – el sistema de reputación ESET LiveGrid® mejora la eficacia de las soluciones anti-malware de ESET al comparar los archivos analizados con una base de datos de elementos de listas blancas y listas negras en la nube.

- **Habilitar el sistema de comentarios de ESET LiveGrid®** – Envía los datos de envío relevantes (descritos en la **sección de envío de muestra** a continuación) junto con informes de falla y estadísticas al laboratorio de investigación de ESET para un mayor análisis.

- **Habilitar ESET LiveGuard**: la función ESET LiveGuard detecta nuevas amenazas nunca vistas mediante el análisis de su comportamiento en un entorno aislado. ESET LiveGuard solo puede activarse si está habilitado ESET LiveGrid®.

- **Enviar informes de error y datos de diagnóstico**: envíe datos de diagnóstico relacionados con ESET LiveGrid®, como informes de falla y módulos de volcado de memoria. Recomendamos mantener esta función habilitada para ayudar a ESET a diagnosticar problemas, mejorar los productos y garantizar una mejor protección del usuario final.

- **Enviar estadísticas anónimas** – permita a ESET recopilar información acerca de amenazas detectadas recientemente como el nombre de la amenaza, la fecha y la hora de detección, el método de detección y los metadatos asociados, la versión del producto, y la configuración, incluida la información sobre su sistema.

- **Correo electrónico de contacto (opcional)** – puede incluir su correo electrónico junto con los archivos sospechosos, así podrá utilizarse para contactarlo en caso de que se requiera información adicional para el análisis. No recibirá respuesta alguna de ESET a menos que se necesite información adicional.

Envío de muestras

Envío manual de muestras: le permite enviar muestras a ESET manualmente desde el menú contextual, Cuarentena o Herramientas.

Envío automático de muestras detectadas

Seleccione qué tipo de muestras se enviarán a ESET para su análisis y para mejorar la detección futura (el tamaño máximo predeterminado de la muestra es de 64 MB). Se encuentran disponibles las siguientes opciones:

- **Todas las muestras detectadas**: todos los objetos detectados por el motor de detección (incluso las aplicaciones potencialmente no deseadas cuando se habilitan en la configuración del explorador).

- **Todas las muestras, excepto los documentos**: todos los objetos detectados, excepto los **documentos**

(consulte a continuación).

- **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, muestras que casi no se detectan o alguno de los módulos de protección de ESET Security Ultimate consideran estas muestras sospechosas o con un comportamiento poco claro (el tamaño máximo predeterminado de la muestra es de 64 MB).

- **Ejecutables**: incluye archivos ejecutables, como .exe, .dll, .sys.
- **Archivos**: incluye tipos de archivos, como .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripts**: incluye tipos de archivos de script, como .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Otros** – Incluye tipos de archivos como .jar, .reg, .msi, .sfw, .lnk.
- **Posibles correos electrónicos spam** – permite enviar partes de correos electrónicos con spam o correos electrónicos con spam completos adjuntos a ESET para que realice un análisis más profundo. Activar esta opción mejora la detección global de spam, que incluye mejoras en la detección futura de spam para usted.
- **Quitar ejecutables, archivos, scripts, otras muestras y posibles correos electrónicos spam desde servidores de ESET**: define cuándo quitar las muestras que ESET LiveGuard envía para analizar.
- **Documentos**: incluye documentos Microsoft Office o PDF con contenido activo o sin este.
- **Quitar documentos de los servidores de ESET**: define cuándo se deben quitar los documentos que ESET LiveGuard envía para analizar.

Expandir para ver una lista de todos los tipos de archivos de documento 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

El filtro de exclusión le permite excluir archivos o ciertas carpetas del envío (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. Los tipos de archivos más comunes se excluyen en forma predeterminada (.doc, etc.). Si lo desea, puede agregar archivos a la lista de archivos excluidos.

Para excluir archivos descargados de `download.domain.com`, abra la Configuración avanzada > **Motor de detección** > **Protección basada en la nube** > **Envío de muestras** y haga clic en **Editar** junto a **Exclusiones**. Agregue la exclusión `.download.domain.com`.

Tamaño máximo de muestras (MB): define el tamaño máximo de las muestras que se envían automáticamente (1-64 MB).

Filtro de exclusión para la protección basada en la nube

El filtro de exclusión permite excluir ciertos archivos o carpetas del envío de muestras. Los archivos incluidos en la lista nunca se enviarán a los laboratorios de ESET para su análisis, aunque contengan un código sospechoso. Los tipos de archivo comunes (tales como .doc, etc.) se excluyen de forma predeterminada.

Esta función resulta útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo.

Para excluir archivos descargados de download.domain.com, abra la Configuración avanzada > **Motor de detección** > **Protección en la nube** > **Envío de muestras** > **Exclusiones** y agregue la exclusión *download.domain.com*.

ESET LiveGuard

ESET LiveGuard es una característica que añade una capa de protección basada en la nube específicamente diseñada para mitigar amenazas nunca vistas.

Cuando esta opción 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 aislado y nuestros motores avanzados de detección de malware las evalúan. Se envían muestras maliciosas o correos electrónicos spam sospechosos 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 equipo**
- Configuración avanzada > **Motor de detección** > **Protección basada en la nube**

Para acceder a la configuración avanzada de ESET LiveGuard, abra la Configuración avanzada > **Motor de detección** > **Protección basada en la nube** > **ESET LiveGuard**.

Acción tras la detección: define la medida que se debe tomar si la muestra analizada se evalúa como una amenaza.

Protección proactiva: permite o bloquea la ejecución de los archivos que ESET LiveGuard está analizando. Si un archivo es sospechoso, la protección proactiva bloquea su ejecución hasta que finaliza el análisis. La protección proactiva detecta archivos de las siguientes fuentes:

- Archivos descargados con un navegador web compatible
- Descargado de un cliente de correo
- Archivos extraídos de un archivo no cifrado o cifrado con una de las utilidades de archivo compatibles

- Archivos ejecutados y abiertos ubicados en un dispositivo extraíble

Consulte las aplicaciones compatibles en la siguiente tabla:

Navegadores web	Clientes de correo	Utilidades de archivo	Dispositivos extraíbles
Internet Explorer	Microsoft Outlook	WinRAR	Unidad flash USB
Microsoft Edge	Mozilla Thunderbird	WinZIP	Disco duro USB
Chrome	Microsoft Mail	Unpacker integrado de Microsoft Explorer	CD/DVD
Firefox		7zip	Disquete
Opera			Lector de tarjetas integrado
Brave Navegador			

Nota
La protección proactiva bloquea los archivos copiados con Windows Explorer de una ubicación excluida a una protegida porque ESET Security Ultimate reconoce a `explorer.exe` como una utilidad de archivo.

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 en el archivo y en **Desbloquear archivo analizado por ESET LiveGuard**.

Tiempo de espera máximo 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 el estado del análisis mediante notificaciones. Consulte las notificaciones disponibles a continuación:

Título de notificación	Descripción
Archivo bloqueado debido al análisis	El archivo está bloqueado por ESET LiveGuard. ESET LiveGuard analiza el archivo para garantizar que es seguro usarlo. Puede esperar o elegir una de las siguientes opciones: • **Desbloquear el archivo**: desbloquea el archivo, pero el análisis continúa. Recibirá una notificación sobre el resultado. No se recomienda si no está seguro de la integridad del archivo. • **Cambiar configuración**: abre la ventana de configuración de protección del equipo, donde puede desactivar ESET LiveGuard y su protección proactiva.
Archivo bloqueado	El archivo ya no está bloqueado. El análisis continúa y se mostrará una notificación sobre el resultado. Puede abrir el archivo.
Archivo todavía 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. El archivo se ha limpiado.
Uso seguro del archivo	ESET LiveGuard ha finalizado el análisis y es seguro usar el archivo.

Si ESET LiveGuard no funciona correctamente, recibirá una notificación en la ventana principal del programa > **Vista general**. Siga las instrucciones de la notificación para resolver el problema. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Exploración de malware

Se puede acceder a la sección **Exploración de malware** desde Configuración avanzada > **Motor de detección** > **Exploración de malware** y le permite configurar los parámetros de exploración para los perfiles de exploración.

Exploración a pedido

Perfil seleccionado – Un conjunto específico de parámetros que usa en la exploración bajo demanda. Para crear uno nuevo, haga clic en **Editar** junto a la **Lista de perfiles**. Consulte Perfiles de exploración para obtener información detallada.

Después de seleccionar el perfil de exploración, puede configurar las siguientes opciones:

Destinos de exploración: si desea explorar un objeto específico o un grupo de objetos, haga clic en **Editar** junto a **Destinos de exploración** y elija una opción desde la estructura (de árbol) de la carpeta. Consulte Destinos de exploración para obtener información detallada.

Protección de acuerdo a las necesidades y con aprendizaje automático: puede configurar niveles de informes y protección para cada perfil de exploración. De forma predeterminada, los perfiles de exploración 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 exploración

Hay cuatro perfiles de exploración predefinidos en ESET Security Ultimate:

- **Análisis inteligente** – Es el perfil de exploración avanzada predeterminado. El perfil de análisis inteligente utiliza la tecnología de optimización inteligente, que excluye los archivos que se encontraron limpios en una exploración anterior y que no se han modificado desde esa exploración. Esto permite tener tiempos de exploración más bajos con un impacto mínimo en la seguridad del sistema.

- **Exploración del menú contextual** – Puede iniciar la exploración del menú contextual de cualquier archivo desde el menú contextual. El perfil de exploración del menú contextual le permite definir una configuración de exploración que se utilizará cuando se ejecuta la exploración de esta manera.

- **Exploración exhaustiva** – El perfil de exploración exhaustiva no utiliza la optimización inteligente de forma predeterminada, por lo que no se excluye ningún archivo de la exploración mediante este perfil.

- **Exploración del equipo** – Es el perfil predeterminado utilizado en la exploración estándar del equipo.

Es posible guardar los parámetros preferidos de exploración para usarlos en el futuro. Se recomienda crear un perfil distinto (con varios objetos para explorar, métodos de exploración y otros parámetros) para cada exploración utilizada regularmente.

Para crear un nuevo perfil, abra Configuración avanzada > **Motor de detección** > **Exploración de malware** >

Exploración a demanda > **Lista de perfiles** > **Editar**. La ventana **Administrador de perfiles** incluye el menú desplegable **Perfil seleccionado** que enumera los perfiles de exploración existentes así como la opción de crear uno nuevo. Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte ThreatSense, donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

Suponga que desea crear su propio perfil de exploración y la configuración de **Explore su equipo** es parcialmente adecuada, pero no desea explorar empaquetadores en tiempo real o aplicaciones potencialmente no seguras y, además, quiere aplicar una **Reparar siempre la detección**. Ingrese el nombre de su nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione su nuevo perfil desde el menú desplegable **Perfil seleccionado** y ajuste los parámetros restantes para cumplir con sus requisitos, y haga clic en **Aceptar** para guardar su nuevo perfil.

Objetos para explorar

En el menú desplegable **Objetivos de exploración**, puede seleccionar objetivos de exploración predefinidos.

- **Por configuración de perfil**: selecciona los objetos especificados en el perfil de exploración seleccionado.
- **Medios extraíbles** – selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
- **Unidades locales** – selecciona todos los discos rígidos del sistema.
- **Unidades de red** – selecciona todas las unidades de red asignadas.
- **Selección personalizada** – cancela todas las selecciones anteriores.

La estructura de la carpeta (árbol) también contiene objetos específicos para explorar.

- **Memoria operativa** – explora todos los procesos y datos que la memoria operativa utiliza actualmente.
- **Sectores de inicio/UEFI** – explora los sectores de inicio y UEFI para detectar la presencia de virus. Lea más sobre el análisis UEFI en el glosario.
- **Base de datos WMI**: explora la base de datos Windows Management Instrumentation (WMI) en su totalidad, todos los espacios de nombre, las instancias y propiedades. Busca referencias para archivos infectados o malware insertados como datos.
- **Registro del sistema**: explora el registro del sistema en su totalidad, como claves y subclaves. Busca referencias para archivos infectados o malware insertados como datos. Al desinfectar las detecciones, la referencia permanece en el registro para garantizar que no se pierdan datos importantes.

Para ir rápidamente a un objeto de exploración (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 la exploración, marque la casilla de verificación en la estructura de árbol.

Exploración en estado inactivo

Puede habilitar la exploración en estado inactivo en Configuración avanzada > **Motor de detección** > **Exploración de malware** > **Exploración en estado inactivo**.

Exploración en estado inactivo

Habilite el interruptor junto a **Habilitar exploración en estado inactivo** para habilitar esta función. Cuando el equipo está en estado inactivo, se realiza una exploración silenciosa en todas las unidades locales.

De forma predeterminada, la exploración en estado inactivo no se ejecutará cuando el equipo (portátil) está funcionando con la energía de la batería. Puede anular esta configuración al activar el interruptor junto a **Ejecutar incluso si el equipo recibe alimentación de la batería** en la Configuración avanzada.

Encienda el interruptor junto a **Habilitar registro** en la Configuración avanzada para registrar el resultado de la exploración del equipo en la sección Archivos de registro (desde la ventana principal del programa haga clic en **Herramientas** > **Archivos de registro** y seleccione **Exploración del equipo** en el menú desplegable **Registro**).

Detección en estado inactivo

Consulte Desencadenadores de detección en estado inactivo para obtener una lista completa de condiciones que deben cumplirse para activar la exploración del 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 en estado inactivo

La configuración de la detección en estado inactivo puede establecerse desde Configuración avanzada > **Motor de detección** > **Exploración de malware** > **Exploración en estado inactivo** > **Detección en estado inactivo**. Esta configuración especifica un desencadenante para la exploración en estado inactivo:

- **Pantalla apagada o protector de pantalla**
- **Bloqueo de equipo**
- **Cierre de sesión de usuario**

Use el interruptor de cada estado correspondiente para habilitar o deshabilitar los desencadenantes de la detección en estado inactivo.

Exploración en el inicio

En forma predeterminada, la exploración automática de archivos durante el inicio del sistema se realizará durante el inicio del sistema y durante la actualización del motor de detección. Esta exploración depende de la Configuración y de las tareas en Tareas programadas.

Las opciones de exploración en el inicio son parte de una tarea programada de **Verificación de archivos de inicio del sistema**. Para cambiar la configuración, vaya a **Herramientas** > **Tareas programadas**, haga clic en **Exploración automática de archivos durante el inicio del sistema** y en **Editar**. En el último paso, aparecerá la ventana Exploración automática de archivos durante el inicio del sistema. Para obtener instrucciones detalladas sobre la creación y administración de tareas programadas, consulte la 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.

Verificación de archivos de inicio automático

Al crear una tarea programada de verificación de archivos de inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Escanear objetivo** especifica la profundidad de la exploración para los archivos que se ejecutan al inicio del sistema en base a un algoritmo sofisticado. Los archivos se organizan en orden descendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrado** (la mayoría de los archivos escaneados)
- **Archivos poco usados**
- **Archivos usados habitualmente**
- **Archivos de uso frecuente**
- **Solo los archivos más frecuentemente utilizados** (los archivos menos explorados)

También se incluyen dos grupos específicos:

- **Archivos que se ejecutan antes del registro del usuario**: contiene archivos de las ubicaciones a las que puede accederse sin que el usuario se registre (incluye casi todas las ubicaciones de inicio tales como servicios, objetos del ayudante de exploración, winlogon notify, entradas de las tareas programadas de ventanas, dll conocidos, etc.).
- **Archivos que se ejecutan después del registro del usuario** - Contiene archivos de las ubicaciones a las que puede accederse solo después de que un usuario se registre (incluye archivos que solo se ejecutan para un usuario específico, por lo general archivos en *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se exploran son fijas para cada grupo anterior. Si elige una profundidad inferior de exploración de los archivos ejecutados al iniciar el sistema, los archivos no explorados se explorarán cuando se abren o ejecutan.

Prioridad de exploración: el nivel de prioridad usado para determinar cuándo se iniciará una exploración:

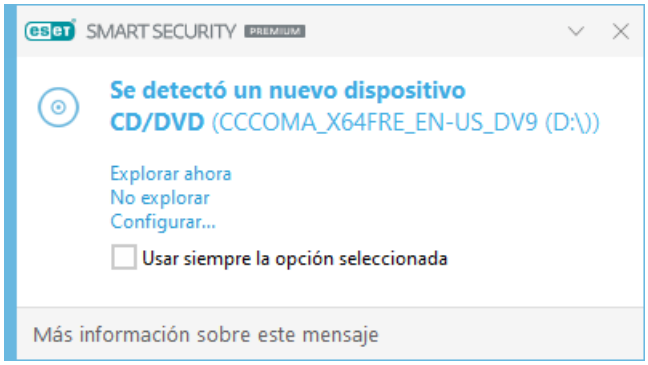
- **Cuando está inactivo** - La tarea se realizará solo cuando el sistema esté inactivo,
- **Más baja**: cuando la carga del sistema es lo más baja posible,
- **Inferior**: en una carga baja del sistema,
- **Normal** – En una carga del sistema promedio.

Medios extraíbles

ESET Security Ultimate proporciona la exploración automática de los medios extraíbles (CD/DVD/USB/...) al insertarlos en un equipo. Resulta útil si el administrador del equipo desea prevenir que los usuarios utilicen

medios extraíbles con contenido no solicitado.

Cuando se inserten medios extraíbles y se configure **Mostrar las opciones de exploración** en Configuración avanzada > **Motor de detección** > **Exploración de malware** > **medios extraíbles**, se mostrará el siguiente cuadro de diálogo:



Opciones para este diálogo:

- **Explorar ahora** – desencadenará la exploración de los medios extraíbles.
- **No explorar:** no se explorarán los medios extraíbles.
- **Configuración** – abre la Configuración avanzada.
- **Usar siempre la opción seleccionada** – de seleccionarse, se llevará a cabo la misma acción cuando se inserte un medio extraíble en el futuro.

Además, ESET Security Ultimate presenta la funcionalidad de Control del dispositivo, que le permite definir las reglas para el uso de dispositivos externos en un equipo determinado. Se pueden encontrar más detalles sobre el Control del dispositivo en la sección Control del dispositivo.

Para acceder a la configuración de la exploración de medios extraíbles, abra la Configuración avanzada > **Motor de detección** > **Exploraciones de malware** > **Medios extraíbles**.

Acción para realizar tras insertar un medio: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el equipo (CD/DVD/USB). Seleccione la acción deseada luego de insertar un medio extraíble en un equipo:

- **No explorar**: no se realizará ninguna acción y no se abrirá la ventana **Se detectó un nuevo dispositivo**.
- **Exploración automática del dispositivo**: se llevará a cabo una exploración del equipo en los dispositivos de medios extraíbles insertados.
- **Mostrar las opciones de exploración** – abre la sección de configuración de **medios extraíbles**.

Protección de documentos

La característica de protección de documentos explora los documentos de Microsoft Office antes de que se abran, así como los archivos descargados automáticamente por Internet Explorer, por ej., los elementos Microsoft

ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección del sistema de archivos en tiempo real. Puede deshabilitarse para mejorar el rendimiento en los sistemas que no manejan un alto volumen de documentos de Microsoft Office.

Para activar la protección de documentos, abra la Configuración avanzada > **Motor de detección** > **Exploración de malware** > **Protección de documentos** y haga clic en el interruptor junto a **Habilitar 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.

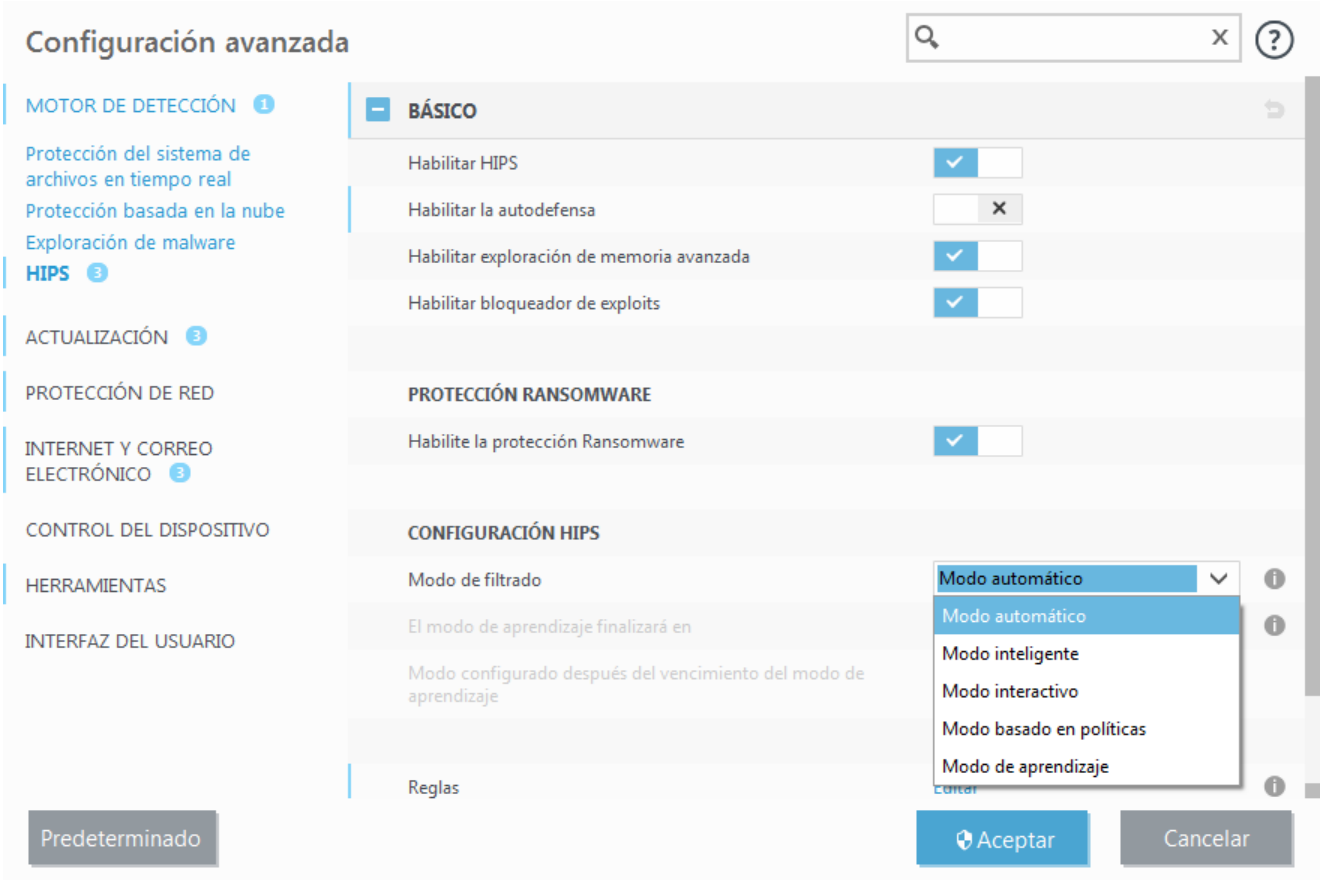
Esta característica se activa por medio de las aplicaciones que usan Microsoft Antivirus API (por ejemplo, Microsoft Office 2000 y posteriores, o Microsoft Internet Explorer 5.0 y posteriores).

HIPS – Sistema de prevención de intrusiones basado en el host

Las modificaciones de la configuración del HIPS deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de HIPS puede llevar a la inestabilidad del sistema.

El **Sistema de prevención de intrusiones basado en el host (HIPS)** protege su sistema contra malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS utiliza el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro. El HIPS es independiente de la protección del sistema de archivos en tiempo real y no es un firewall; solo monitorea los procesos activos en el sistema operativo.

Puede configurar los ajustes de HIPS en Configuración avanzada > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones basado en el host**. El estado de HIPS (habilitado/deshabilitado) se muestra en la ventana principal del programa de ESET Security Ultimate > **Configuración** > **Protección del equipo**.



Sistema de prevención de intrusiones basado en el host

Habilitar HIPS: HIPS se habilita de manera predeterminada en ESET Security Ultimate. Al desactivar HIPS, se desactivan el resto de las características de HIPS, como Bloqueador de exploits.

Habilitar la autodefensa: ESET Security Ultimateutiliza la tecnología incorporada de **autodefensa** como parte de HIPS para evitar que el software malicioso corrompa o deshabilite su protección antivirus y antispyware. La autodefensa protege al sistema crucial y los procesos de ESET, las claves de registro y los archivos de ser manipulados.

Habilitar el servicio protegido: habilita la protección para ESET Service (ekrn.exe). Cuando está habilitado, el servicio se inicia como un proceso de Windows protegido para defender contra ataques de malware.

Habilitar explorador de memoria avanzado: trabaja en conjunto con el Bloqueador de exploits para fortalecer la protección contra el malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. La exploración de memoria avanzada está habilitada en forma predeterminada. Lea más información sobre este tipo de protección en el glosario.

Habilitar bloqueador de exploits: está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office. El bloqueador de exploits está habilitado en forma predeterminada. Lea más información sobre este tipo de protección en el glosario.

Inspección profunda del comportamiento

Habilitar inspección profunda del comportamiento: otra capa de protección que es parte de la función de HIPS. Esta extensión de HIPS analiza el comportamiento de todos los programas que se ejecutan en su equipo y le

advierte si el comportamiento de los procesos es malicioso.

Las exclusiones de HIPS para la inspección profunda del comportamiento permiten excluir procesos de la exploración. Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos únicamente crear exclusiones cuando sea absolutamente necesario.

Escudo contra ransomware

Habilitar protección contra ransomware: es otra capa de protección que funciona como parte de la función HIPS. Debe tener habilitado el sistema de reputación de ESET LiveGrid® para que funcione la protección de ransomware. Lea más información sobre este tipo de protección.

Habilitar Intel® Threat Detection Technology – ayuda a detectar ataques de ransomware mediante el uso de la única telemetría de CPU Intel para aumentar la eficacia de detección, reducir las alertas de falso positivo y ampliar la visibilidad para capturar técnicas de evasión avanzadas. Consulte los procesadores compatibles.

Configuración HIPS

El **modo de filtrado** se puede realizar en uno de los siguientes cuatro modos:

Modo de filtrado	Descripción
Modo automático	Las operaciones están habilitadas, excepto las que se encuentran bloqueadas por las reglas predefinidas que protegen su sistema.
Modo inteligente	Se notificará al usuario solo en caso de eventos muy sospechosos.
Modo interactivo	El programa le solicitará al usuario que confirme las operaciones.
Modo basado en políticas	Bloquea todas las operaciones que no están definidas por una regla específica que las permite.
Modo de aprendizaje	Las operaciones están habilitadas y se crea una regla luego de cada operación. Las reglas creadas en este modo se pueden ver en el editor de **reglas HIPS**, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Cuando selecciona el **Modo de aprendizaje** en el menú desplegable **Modo de filtrado**, la **configuración del modo de aprendizaje finalizará** cuando esté disponible. Seleccione el intervalo de tiempo durante el que desea activar el modo de aprendizaje; el tiempo máximo es de 14 días. Cuando el tiempo especificado haya pasado, se le solicitará que edite las reglas creadas por HIPS mientras estuvo en el modo de aprendizaje. También puede elegir un modo de filtrado diferente, o posponer la decisión y continuar utilizando el modo de aprendizaje.

Modo configurado después del vencimiento del modo de aprendizaje: seleccione el modo de filtrado que se usará después del vencimiento del modo de aprendizaje. Después del vencimiento, la opción **Preguntar al usuario** requerirá privilegios administrativos para realizar un cambio en el modo de filtrado de HIPS.

El sistema HIPS monitorea los sucesos dentro del sistema operativo y reacciona consecuentemente en función de reglas similares a las que usa el firewall. Haga clic en **Editar** junto a **Reglas** para abrir el editor de **reglas HIPS**. En la ventana de reglas HIPS, puede seleccionar, agregar, editar o quitar reglas. Para más información sobre la creación de reglas y las operaciones de HIPS, consulte Cómo editar una regla de HIPS.

Exclusiones de HIPS

Las exclusiones le permiten excluir procesos de la inspección profunda del comportamiento de HIPS.

Para editar exclusiones de HIPS, abra Configuración avanzada > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones basado en el host** > **Exclusiones** > **Editar**.

> No debe confundirse con Extensiones de archivo excluidas, Exclusiones de detección, Exclusiones de rendimiento o Exclusiones de procesos.

Para excluir un objeto, haga clic en **Agregar** e ingrese la ruta a un objeto o selecciónelo en la estructura de árbol. También puede Editar o Eliminar las entradas seleccionadas.

Configuración avanzada de HIPS

Las opciones que se muestran a continuación resultan útiles para la depuración y el análisis de la conducta de una aplicación.

Controladores siempre permitidos para cargar – los controladores seleccionados siempre tienen permitido cargar independientemente del modo de filtrado configurado, a menos que se bloquee explícitamente por una regla de usuario.

Registrar todas las operaciones bloqueadas: todas las operaciones bloqueadas se escribirán en el registro de HIPS. Utilice esta característica solo cuando se resuelvan problemas o lo solicite el soporte técnico de ESET, ya que puede generar un archivo de registro muy grande y ralentizar su equipo.

Notificar cuando ocurran cambios en las aplicaciones de inicio – muestra una notificación del escritorio cada vez que se agrega o quita una aplicación del inicio del sistema.

Controladores siempre permitidos para cargar

Los controladores que se muestran en esta lista siempre tendrán permitido cargar independientemente del modo de filtrado de HIPS, a menos que se bloquee explícitamente por una regla de usuario.

Agregar – agrega un controlador nuevo.

Editar – edita un controlador seleccionado.

Quitar – elimina un controlador de la lista.

Restablecer – vuelve a cargar un conjunto de controladores del sistema.

> Haga clic en **Restablecer** si no desea que se incluyan los controladores que ha agregado en forma manual. Esto puede ser útil si ha agregado varios controladores y no puede eliminarlos de la lista en forma manual.

> Tras la instalación, la lista de controladores está vacía. ESET Security Ultimate rellena la lista automáticamente con el correr del tiempo.

Ventana interactiva de HIPS

La ventana de notificación de HIPS le permite crear una regla en función de cualquier acción nueva que el HIPS detecte para, posteriormente, definir las condiciones mediante las cuales se permitirá o denegará dicha acción.

Las reglas creadas a partir de la ventana de notificación se consideran equivalentes a las creadas manualmente. En consecuencia, la regla creada desde una ventana de diálogo puede ser menos específica que la que activa la ventana de diálogo. Esto significa que, después de crear una regla en el cuadro de diálogo, la misma operación puede activar la misma ventana. Para más información, consulte Prioridad para reglas de HIPS.

Si la acción predeterminada para una regla está configurada en **Preguntar siempre**, una ventana de diálogo aparecerá cada vez que se active la regla. Puede elegir **Denegar** o **Permitir** la operación. Si no elige una acción en el tiempo dado, se seleccionará una nueva acción en función de las reglas.

Recordar hasta salir de la aplicación hace que la acción (**Permitir/Denegar**) se utilice hasta que haya un cambio de reglas o del modo de filtrado, una actualización de módulo del HIPS o un reinicio del sistema. Las reglas temporales se eliminarán después de cualquiera de estas tres acciones.

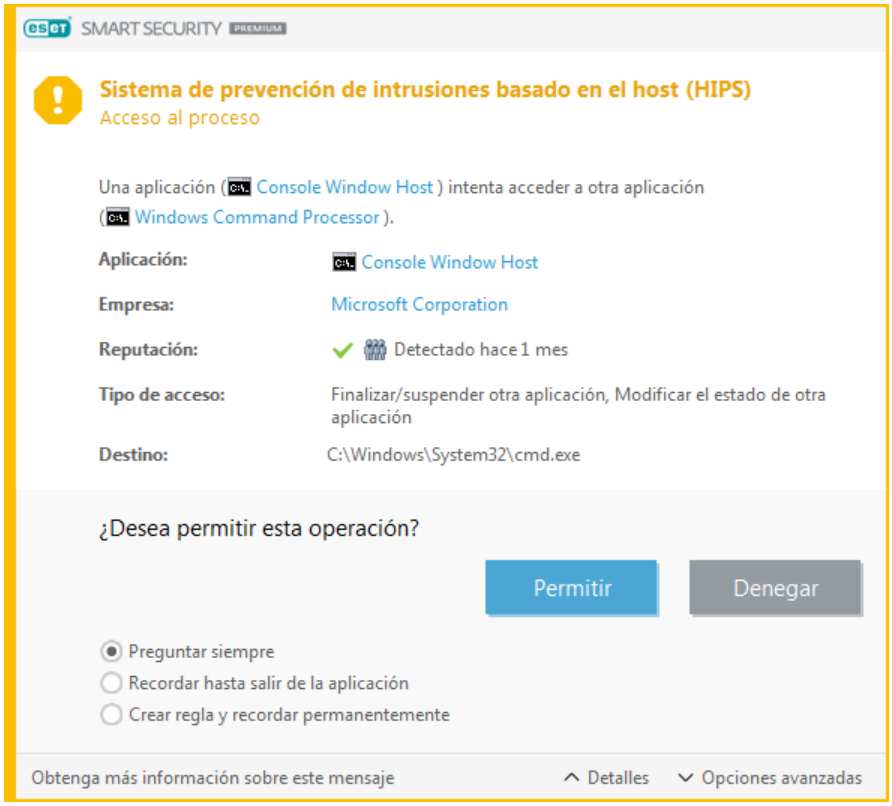
La opción **Crear regla y recordar permanentemente** creará una nueva regla HIPS que puede modificarse más adelante en la sección Administración de reglas del HIPS (requiere de privilegios de administración).

Haga clic en **Detalles** al pie para ver qué aplicación activa la operación, cuál es la reputación del archivo o qué tipo de operación se le pide autorizar o rechazar.

Para acceder a las configuraciones de parámetros de reglas más detallados, haga clic en **Opciones avanzadas**. Las opciones de abajo se encuentran disponibles si elige **Crear regla y recordar permanentemente**:

- **Crear una regla válida solo para esta aplicación**: si quita la marca de verificación de esta casilla, se creará la regla para todas las aplicaciones de origen.
- **Solo para la operación**: elija el archivo de la regla/la aplicación/la operación de registro. Consulte las descripciones de todas las operaciones del HIPS.
- **Solo para el destino**: elija el archivo de la regla/la aplicación/el destino del registro.

> ¿Notificaciones del HIPS interminables?
> Para evitar que aparezcan las notificaciones, cambie el modo de filtrado a **automático** en Configuración avanzada > **Motor de detección** > **HIPS** > **Sistema de prevención de intrusiones basado en el host**.



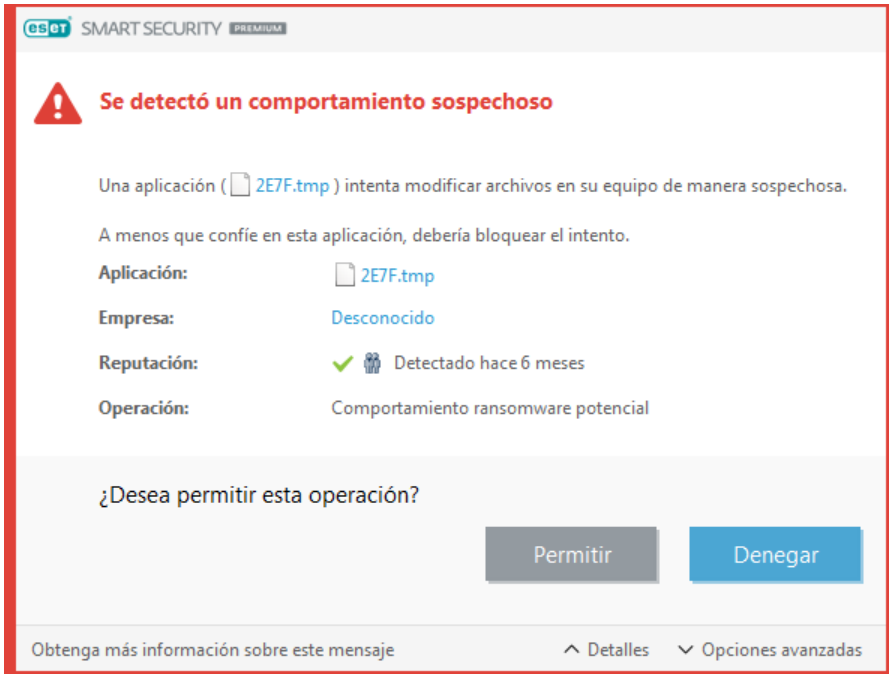
Finalizó el modo de aprendizaje

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 usa mejor para la configuración inicial de HIPS, pero solo debe mantenerse activado durante un breve período de tiempo. No se requiere la interacción del usuario porque ESET Security Ultimate guarda las reglas según los parámetros predefinidos. Cambie al modo **interactivo** o **basado en políticas** después de que se hayan creado todas las reglas para los procesos necesarios que se ejecutan en el sistema operativo a fin de evitar riesgos de seguridad.

Puede posponer esta decisión si no desea cambiar la configuración.

Se detectó un comportamiento ransomware potencial

Esta ventana interactiva aparecerá cuando se detecta un comportamiento ransomware potencial. Puede elegir **Denegar** o **Permitir** la operación.



Haga clic en **Detalles** para ver los parámetros específicos de detección. La ventana de diálogo le permite **Enviar el archivo para su análisis** o **Excluirlo de la detección**.

Para que la protección contra Ransomware funcione correctamente, ESET LiveGrid® debe estar habilitado.

Administración de reglas del HIPS

Una lista de reglas definidas por el usuario y agregadas automáticamente desde el sistema HIPS. Encontrará más detalles sobre la creación de reglas y las operaciones del sistema HIPS en el capítulo Configuración de reglas HIPS. También consulte Principio general de HIPS.

Columnas

Regla – nombre de la regla definido por el usuario o elegido automáticamente.

Habilitada: desactive el interruptor si desea conservar la regla en la lista, pero no quiere usarla.

Acción – la regla especifica una acción; **Permitir**, **Bloquear** o **Preguntar**; que se deberá llevar a cabo bajo las condiciones adecuadas.

Orígenes – la regla solo se utilizará si una aplicación o las aplicaciones accionan el evento.

Destinos – la regla solo se utilizará si la operación se relaciona con un archivo, una aplicación o una entrada de registro específicos.

Severidad de registro – si activa esta opción, la información sobre esta regla se incluirá en el registro de HIPS.

Notificar – si se acciona un evento, aparece una ventana de notificación emergente pequeña en la esquina inferior derecha.

Elementos de control

Agregar – crea una regla nueva.

Editar – le permite editar las entradas seleccionadas.

Quitar – quita las entradas seleccionadas.

Prioridad para reglas del HIPS

No hay opciones para ajustar el nivel de prioridad de las reglas del HIPS utilizando los botones arriba/abajo (en cuanto a las reglas de firewall donde las reglas se ejecutan de arriba a abajo).

- Todas las reglas que usted cree tienen la misma prioridad
- Cuanto más específica la regla, mayor la prioridad (por ejemplo, la regla para una aplicación específica tiene mayor prioridad que la regla para todas las aplicaciones).
- A nivel interno, HIPS contiene reglas de prioridad elevada a las que usted no puede acceder (por ejemplo, no puede sobrescribir las reglas definidas de autodefensa)
- No se aplicará una regla que usted cree y que podría inmovilizar el sistema operativo (tendrá la prioridad más baja)

Editar una regla HIPS

Consulte primero la administración de reglas HIPS.

Nombre de la regla – nombre de la regla definido por el usuario o elegido automáticamente.

Acción – especifica una acción; **Permitir**, **Bloquear** o **Preguntar**; que se deberá llevar a cabo si se cumple con las condiciones.

Operaciones que afectan – 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.

Habilitada: deshabilite el interruptor si desea conservar la regla en la lista pero no quiere aplicarla.

Severidad de registro – si activa esta opción, la información sobre esta regla se incluirá en el registro de HIPS.

Notificar al usuario – si se acciona un evento, aparece una ventana de notificación emergente pequeña en la esquina inferior derecha.

La regla está compuesta por partes que describen las condiciones que la accionan:

Aplicaciones de origen–la regla solo se utilizará si esta aplicación o estas aplicaciones accionan el evento. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar archivos nuevos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Archivos de destino: la regla solo se usará si la operación está relacionada con este destino. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos nuevos, o puede

seleccionar **Todos los archivos** en el menú desplegable para agregar todos 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 carpetas o archivos nuevos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Entradas de registro– la regla solo se utilizará si la operación está relacionada con este destino. Seleccione **Entradas específicas** en el menú desplegable y haga clic en **Agregar** para ingresarlas en forma manual o haga clic en **Abrir el editor de registros** 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 el sistema HIPS no se pueden bloquear y están permitidas en forma predeterminada. Además, el sistema HIPS no monitorea todas las operaciones del sistema. HIPS monitorea las operaciones que se pueden considerar no seguras.

Descripciones de las operaciones más importantes:

Operaciones de archivos

- **Eliminar el archivo** – la aplicación pide permiso para eliminar el archivo de destino.
- **Escribir en el archivo** – la aplicación pide permiso para escribir en el archivo de destino.
- **Acceso directo al disco** – la aplicación está intentando leer el disco o escribir en él de una forma que no es la estándar, lo que evade los procedimientos comunes de Windows. Esto puede provocar que se modifiquen los archivos sin haber aplicado las reglas correspondientes. Esta operación puede haberse generado por malware que intenta evadir la detección, un software de creación de copias de seguridad que intenta hacer una copia exacta del disco, o un administrador de particiones que intenta reorganizar los volúmenes de disco.
- **Instalar enlace global** – se refiere al llamado de la función SetWindowsHookEx de la biblioteca MSDN.
- **Cargar controlador** – instalación y carga de controladores en el sistema.

Operaciones de la aplicación

- **Depurar otra aplicación** – adjuntar un depurador al proceso. Cuando se depura una aplicación, es posible ver y modificar muchos detalles de su conducta, así como acceder a sus datos.
- **Interceptar eventos desde otra aplicación** – la aplicación de origen está intentando capturar eventos dirigidos a una aplicación específica (por ejemplo, un keylogger que intenta capturar eventos del navegador).
- **Finalizar/suspender otra aplicación** – suspende, reanuda o termina un proceso (se puede acceder directamente desde el Explorador de procesos o el Panel de procesos).
- **Iniciar una aplicación nueva** – inicio de aplicaciones o procesos nuevos.
- **Modificar el estado de otra aplicación** – la aplicación de origen está intentando escribir en la memoria de las aplicaciones de destino o ejecutar un código en su nombre. Esta funcionalidad puede resultar útil para proteger una aplicación esencial mediante su configuración como aplicación de destino en una regla que

bloquee el uso de dicha operación.

Operaciones de registros

• **Modificar la configuración del inicio** – cualquier cambio en la configuración que defina qué aplicaciones se ejecutarán durante el inicio de Windows. Pueden encontrarse, por ejemplo, al buscar la clave Run en el registro de Windows.

• **Eliminar del registro** – eliminar una clave de registro o su valor.

• **Volver a nombrar la clave de registro** – volver a nombrar claves de registros.

• **Modificar el registro** – crear nuevos valores de claves de registro, modificar los valores existentes, cambiar datos de lugar en el árbol de la base de datos o configurar derechos de usuarios o de grupos para las claves de registro.

Puede usar caracteres globales con ciertas restricciones al ingresar un destino. En lugar de usar una clave específica, se puede usar el símbolo * (asterisco) en las rutas del registro. 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 a una clave de registro. Una ruta a una clave de registro que contenga * define “esta ruta o cualquier ruta de cualquier nivel que se encuentre después de ese símbolo”. Esta es la única manera de usar caracteres globales para archivos de destino. Primero se evaluará la parte específica de la ruta y luego la ruta que sigue al carácter global (*).

Si crea una regla muy genérica, se mostrará la advertencia sobre este tipo de regla.

En el siguiente ejemplo, mostraremos cómo restringir las conductas no deseadas de una aplicación específica:

1. Póngale un nombre a la regla y seleccione **Bloquear** (o **Preguntar** si prefiere elegir más adelante) desde el menú desplegable **Acción**.

2. Habilite el interruptor junto a **Notificar al usuario** para mostrar una notificación cada vez que se aplique una regla.

3. Seleccione al menos una operación en la sección **Operaciones que afectan** para la cual se aplicará la regla.

4. Haga clic en **Siguiente**.

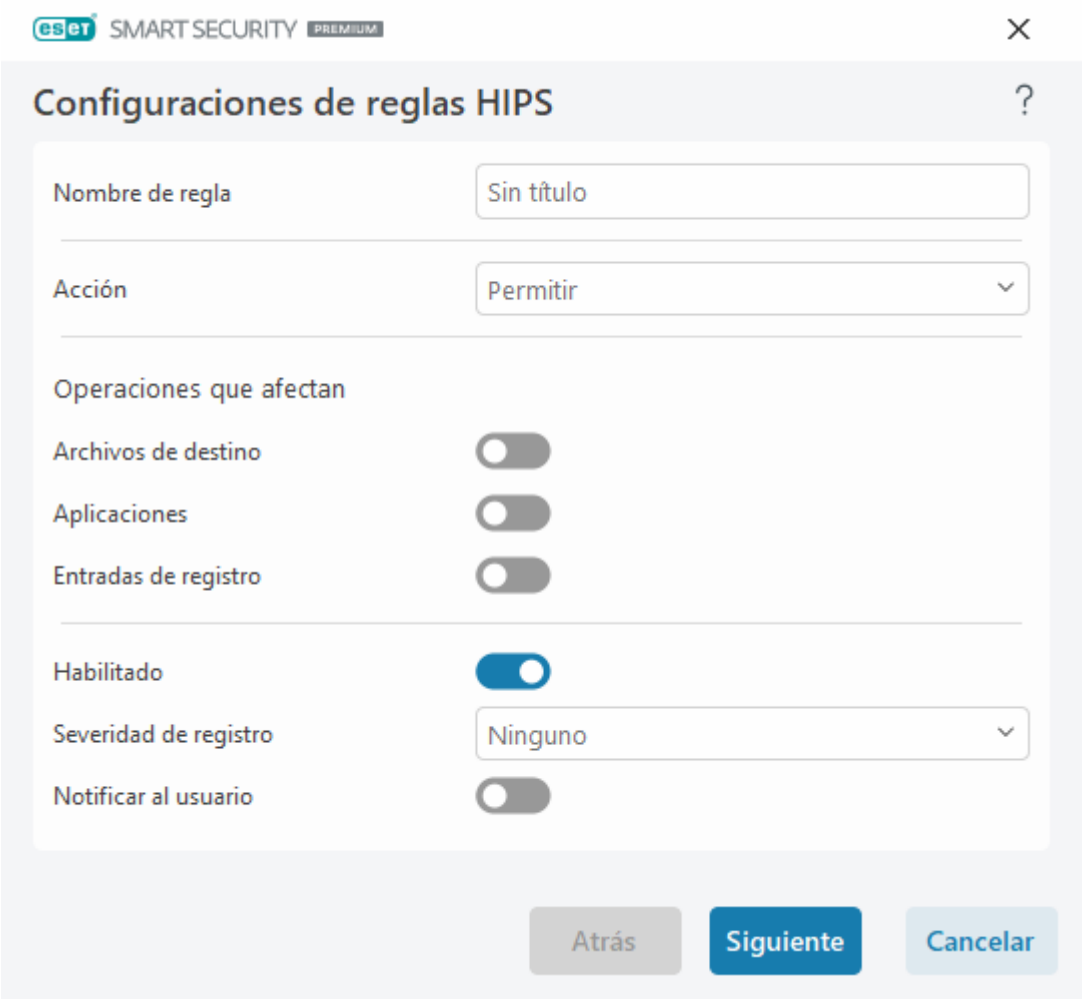
5. En la ventana **Aplicaciones de origen**, seleccione **Aplicaciones específicas** en el menú desplegable para aplicar la nueva regla a todas las aplicaciones que intenten llevar a cabo alguna de las operaciones de aplicaciones seleccionadas en las aplicaciones que especificó.

6. Haga clic en **Agregar** y, luego, en **...** para elegir una ruta para una aplicación específica y, luego, presione **Aceptar**. Añada más aplicaciones si lo prefiere.
Por ejemplo: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Seleccione la operación **Escribir en el archivo**.

8. Seleccione **Todos los archivos** del menú desplegable. De esta manera, se bloquearán los intentos por escribir archivos por parte de la(s) aplicación(es) seleccionada(s) en el paso anterior.

9. Haga clic en **Finalizar** para guardar la regla nueva.



Agregado de una aplicación/ruta de registro para HIPS

Para seleccionar la ruta al archivo de una aplicación, haga clic en la opción **...**. Cuando seleccione una carpeta, se incluirán todas las aplicaciones que se encuentren en esta ubicación.

La opción **Abrir el editor de registros** iniciará el editor del registro de Windows (regedit). Al agregar una ruta de registro, ingrese la ubicación correcta en el campo **Valor**.

Ejemplos de la ruta al archivo o registro:

- *C:\Archivos de programa\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Actualización

Las opciones de configuración de la actualización están disponibles en Configuración avanzada > **Actualizar**. Esta sección especifica la información del origen de la actualización, como los servidores de actualización que se utilizan y los datos de autenticación para estos servidores.

Actualización

El perfil de actualización que está actualmente en uso se muestra en el menú desplegable **Seleccionar perfil de actualización predeterminado**.

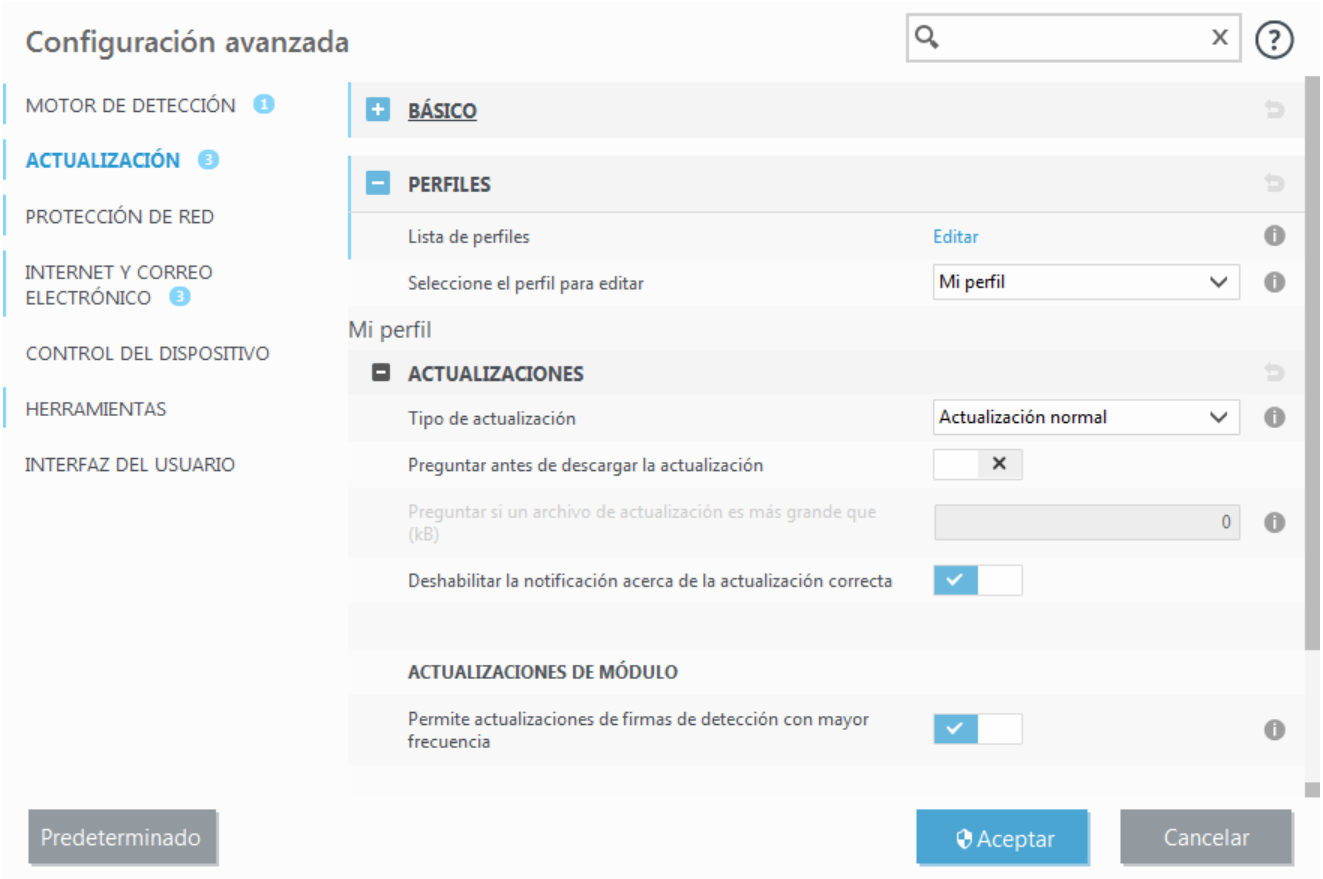
Para crear un nuevo perfil, consulte la sección Actualizar perfiles.

Cambio automático de perfil: permite asignar un perfil de actualización a un perfil de conexión de red específico.

Si experimenta alguna dificultad cuando intenta descargar las actualizaciones de los módulos o el motor de detección, haga clic en **Borrar** junto a **Borrar el caché de actualización** para borrar la caché o los archivos de actualización temporales.

Reversión de módulo

Si sospecha que la nueva actualización del motor de detección o de los módulos de programas puede ser inestable o estar corrupta, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización para un período elegido.



Para que las actualizaciones se descarguen correctamente, es esencial que complete correctamente todos los parámetros de actualización. Si usa un firewall, asegúrese de que el programa de ESET tenga permiso para comunicarse con Internet (por ejemplo, una comunicación HTTP).

Perfiles

Se pueden crear perfiles de actualización para diversas configuraciones y tareas de actualización. La creación de perfiles de actualización resulta útil en particular para usuarios móviles, que necesitan un perfil alternativo para

las propiedades de conexión a Internet que cambian con frecuencia.

El menú desplegable **Seleccionar perfil para editar** muestra el perfil seleccionado actualmente, que en forma predeterminada está configurado en **Mi perfil**. Para crear un perfil nuevo, haga clic en **Editar** junto a la **Lista de perfiles**, ingrese su propio **Nombre de perfil** y luego haga clic en **Agregar**.

Actualizaciones

De forma predeterminada, el **Tipo de actualización** está configurado en **Actualización normal** para garantizar que los archivos de actualización se descarguen automáticamente del servidor de ESET con la menor carga de tráfico de red. Las actualizaciones previas a su lanzamiento (la opción **Actualización previa a su lanzamiento**) son actualizaciones que fueron evaluadas en forma interna y que estarán disponibles al público en general en poco tiempo. Puede beneficiarse de la habilitación de las actualizaciones previas al lanzamiento mediante el acceso a las soluciones y los métodos de detección más recientes. Sin embargo es posible que las actualizaciones previas a la publicación no sean lo suficientemente estableces en todo momento y NO DEBEN utilizarse en estaciones de trabajo y servidores de producción donde se necesita de estabilidad y disponibilidad máximas.

Preguntar antes de descargar la actualización: el programa mostrará una notificación en la que puede elegir confirmar o rechazar la descarga de archivos de actualización.

Preguntar si el tamaño de un archivo de actualización es mayor que (kB): el programa mostrará un diálogo de confirmación si el tamaño del archivo de actualización es mayor que el valor especificado. Si el tamaño del archivo de actualización se encuentra configurado en 0 kB, el programa siempre mostrará un diálogo de confirmación.

Actualizaciones del módulo

Habilitar actualizaciones más frecuentes de firmas de detección – las firmas de detección se actualizarán en intervalos más cortos. Deshabilitar esta configuración puede afectar negativamente la tasa de detección.

Actualizaciones del producto

Actualizaciones de características de la aplicación: instala automáticamente nuevas versiones de ESET Security Ultimate.

Opciones de conexión

Para utilizar un servidor proxy para descargar actualizaciones, consulte la sección Opciones de conexión.

Actualizar reversión

Si sospecha que la nueva actualización del motor de detección o los módulos de programas pueden ser inestables o estar corruptos, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización de manera temporal. O bien puede habilitar las actualizaciones que se deshabilitaron anteriormente si las pospuso de manera indefinida.

ESET Security Ultimate registra instantáneas del motor de detección y de los módulos de programas para usar con la característica de revisión. Para crear instantáneas de la base de datos de virus, deje **Crear instantáneas de los módulos** habilitado. Cuando **Crear instantáneas de los módulos** está habilitado, la primera instantánea se crea durante la primera actualización. La siguiente se crea después de 48 horas. El campo **Cantidad de instantáneas**

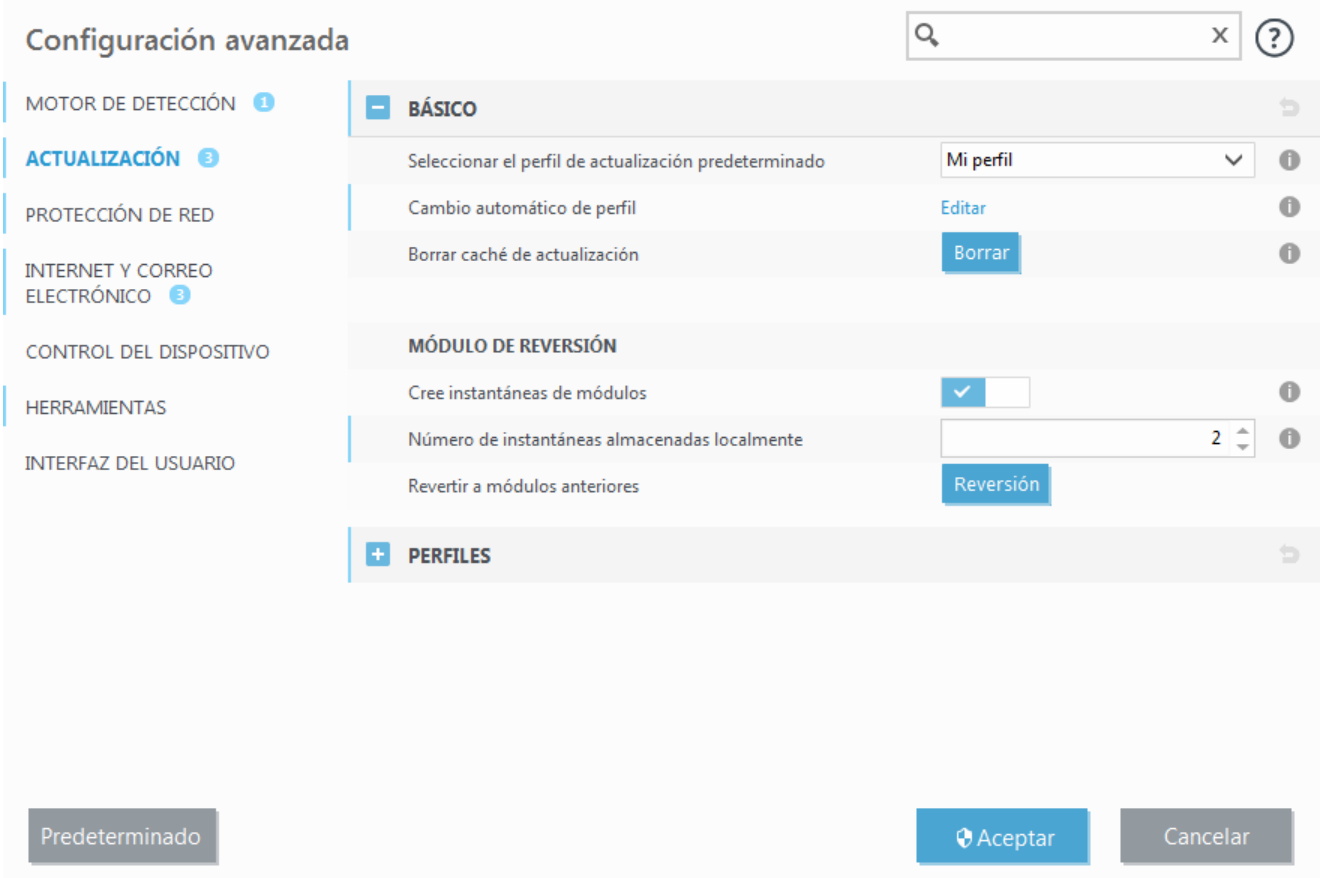
almacenadas localmente define la cantidad de instantáneas anteriores del motor de detección que se almacenaron.

> Cuando se alcanza la cantidad máxima de instantáneas (por ejemplo, tres), la instantánea más antigua se reemplaza con una nueva cada 48 horas. ESET Security Ultimate revierte las versiones de actualización del motor de detección y del módulo del programa a la instantánea más antigua.

Si hace clic en **Revertir** en Configuración avanzada > **Actualizar** > **Actualizar**, debe seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el período de tiempo en el que el motor de detección y las actualizaciones del módulo de programa estarán en pausa.

Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas de forma indefinida hasta restaurar la funcionalidad manualmente. ESET no recomienda seleccionar esta opción porque representa un riesgo de seguridad potencial.

Si se realiza una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permiten las actualizaciones durante el intervalo de tiempo seleccionado desde el menú desplegable **Suspender actualizaciones**. La versión del motor de detección regresa a la versión más antigua disponible y se guarda como una instantánea en el sistema local de archivos del equipo.



Suponga que 22700 es el número de versión más reciente del motor de detección y que 22698 y 22696 se guardan como instantáneas del motor de detección. Tenga en cuenta que 22697 no está disponible porque. En este ejemplo, el equipo se apagó durante la actualización de 22697 y se ofreció una actualización más reciente antes de descargar 22697. Si ha ingresado 2 (dos) en el campo **Cantidad de instantáneas almacenadas localmente** y hace clic en **Revertir**, el motor de detección (incluidos los módulos de programa) se restaurará a la versión número 22696. Este proceso puede tardar unos minutos. Revise si la versión del motor de detección se ha revertido en la pantalla Actualizar.

Intervalo de tiempo de reversión

Si hace clic en **Revertir** en Configuración avanzada > **Actualizar** > **Actualizar**, debe seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el período de tiempo en el que el motor de detección y las actualizaciones del módulo de programa estarán en pausa.

Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas de forma indefinida hasta restaurar la funcionalidad manualmente. ESET no recomienda seleccionar esta opción porque representa un riesgo de seguridad potencial.

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 características o cambian las que ya existen de versiones anteriores. Puede realizarse automáticamente sin la intervención del usuario, pero también puede elegir recibir una notificación. Después de instalar una actualización de características de la aplicación, es posible que sea necesario reiniciar el equipo.

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 de proxy** y seleccione una de las siguientes tres opciones:

- No usar servidor proxy
- Conexión a través de un servidor proxy
- Usar la configuración global del servidor proxy

Seleccione la opción **Usar la configuración global del servidor proxy**, para usar la configuración del servidor proxy ya especificada en Configuración avanzada > **Conectividad** > **Servidor proxy**.

Seleccione **No usar servidor proxy** para indicar que no se usará ningún servidor proxy para actualizar ESET Security Ultimate.

La opción **Conexión a través de un servidor proxy** debe estar seleccionada en los siguientes casos:

- Uso de un servidor proxy diferente al definido en Configuración avanzada > **Conectividad** para actualizar ESET Security Ultimate. En esta configuración, la información del proxy nuevo se debe especificar en dirección de **Servidor de proxy**, **Puerto** de comunicación (3128, predeterminado) y **Nombre de usuario** y **Contraseña** para el servidor proxy, si fuera necesario.
- La configuración del servidor proxy no se estableció en forma global, pero ESET Security Ultimate se conectará a un servidor proxy para descargar las actualizaciones.
- El equipo está conectado a Internet mediante un servidor proxy. Durante la instalación del programa, la configuración se copia de Internet Explorer, pero si se cambia (p. ej., cambia el ISP), verifique desde esta ventana que la configuración del proxy sea la correcta. De lo contrario, el programa no podrá conectarse con los servidores de actualización.

La configuración predeterminada para el servidor proxy es **Usar la configuración global del servidor proxy**.

Use conexión directa si el proxy no está disponible – si no puede llegar al proxy durante la actualización, se evadirá.

> Los campos **Nombre de usuario** y **Contraseña** de esta sección son específicos del servidor proxy. Complete estos campos solo si necesita el nombre de usuario y la contraseña para acceder al servidor proxy. Estos campos solo deberían completarse si tiene la certeza de que se requiere una contraseña para acceder a Internet a través de un servidor proxy.

Protecciones

Las protecciones defienden el sistema ante ataques maliciosos mediante el control de archivos, correos electrónicos y comunicaciones por Internet. Por ejemplo, la corrección comienza si se detecta un objeto clasificado como malware. Protecciones puede eliminarlo bloqueándolo y luego realizar la limpieza, eliminación o la colocación en cuarentena.

Para configurar las protecciones en detalle, abra Configuración avanzada > **Protecciones**.

> Las modificaciones de las protecciones deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de los ajustes puede reducir el nivel de protección.

En esta sección:

- Respuestas de detección
- Configuración de informes
- Configuración de protección

Respuestas de detección

Las respuestas de detección permiten configurar niveles de informes y protección para las siguientes categorías:

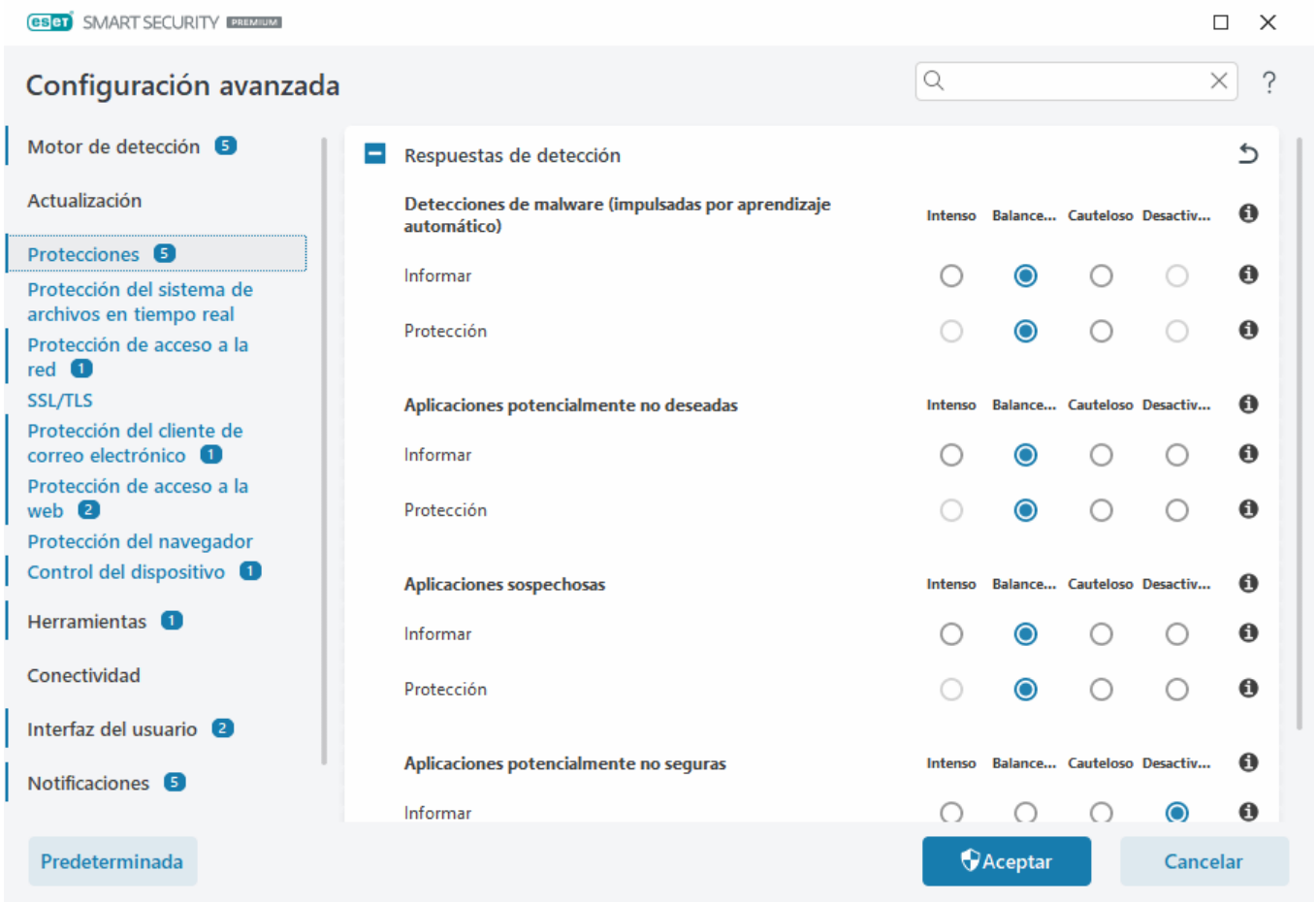
- **Detecciones de malware (impulsadas por aprendizaje automático)** – Un virus del equipo es un programa con códigos maliciosos que está adjunto o añadido a archivos existentes de su equipo. Sin embargo, el término “virus” suele utilizarse en forma errónea. “Malware” (software malicioso) es un término más preciso. La detección de malware se realiza mediante la combinación del módulo del motor de detección con el componente de aprendizaje automático. Obtenga más información sobre estos tipos de aplicaciones en el Glosario.

- **Aplicaciones potencialmente no deseadas**: Grayware o aplicación potencialmente no deseada (PUA, ‘Potentially Unwanted Application’) es una amplia categoría de software, cuya intención no es tan inequívocamente maliciosa como con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas o esperadas por el usuario. Obtenga más información sobre estos tipos de aplicaciones en el Glosario.

- Entre las **aplicaciones sospechosas**, se incluyen programas comprimidos con empaquetadores o protectores.

Generalmente, los autores de malware explotan estos tipos de protectores para evadir la detección.

- **Aplicación potencialmente no segura** : hace referencia al software comercial y legítimo que puede utilizarse inadecuadamente para fines maliciosos. Algunos ejemplos de aplicaciones potencialmente inseguras son las herramientas de acceso remoto, aplicaciones para adivinar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por el usuario). Obtenga más información sobre estos tipos de aplicaciones en el Glosario.



Protección mejorada

El aprendizaje automático avanzado ahora es parte de las protecciones y funciona como una capa avanzada de protección que mejora la detección según el aprendizaje automático. Obtenga más información sobre este tipo de protección en el Glosario.

Configuración de informes

Cuando se produce una detección (p. ej., se encuentra una amenaza y se la clasifica como malware), la información se registra en el Registro de detecciones, y se producen Notificaciones en el escritorio si están configuradas en ESET Security Ultimate.

El umbral de informe está configurado para cada categoría (denominadas “CATEGORÍA”):

1. Detecciones de malware

2. Aplicaciones potencialmente no deseadas

3.Potencialmente no seguro

4.Aplicaciones sospechosas

Los informes se realizan 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. Esta configuración de informes no influye en el bloqueo, la desinfección o la eliminación de objetos.

Lea la información a continuación antes de modificar un umbral (o nivel) para los informes de CATEGORÍA:

Umbral	Explicación
Intenso	Configuración de máxima sensibilidad para informes de CATEGORÍA. Se informan más amenazas. La configuración como **"Intenso"** puede identificar erróneamente objetos como CATEGORÍA.
Balanceado	Configuración balanceada para informes de CATEGORÍA. Esta configuración se optimiza para equilibrar el rendimiento y la precisión de las tasas de detección y el número de objetos que se reportan falsamente.
Cauteloso	Configuración para informes de CATEGORÍA para minimizar la cantidad de objetos identificados en forma errónea al mismo tiempo que se mantiene un nivel suficiente de protección. Los objetos se reportan únicamente cuando la probabilidad es evidente y concuerda con el comportamiento de CATEGORÍA.
Desactivado	Los informes para CATEGORÍA no se encuentran activados, y las amenazas de este tipo no se detectan, reportan o desinfectan. Por lo tanto, esta configuración deshabilita la protección contra este tipo de amenazas. La opción "Desactivado" no está disponible para los informes de malware y es el valor predeterminado para las aplicaciones potencialmente no seguras.

Disponibilidad de módulos de protección de ESET Security Ultimate

La disponibilidad (habilitada o deshabilitada) de un módulo de protección para el umbral de una CATEGORÍA seleccionada es la siguiente:

	Intenso	Balanceado	Cauteloso	Desactivado*
Módulo de aprendizaje automático avanzado	✔ (modo intenso)	✔ (modo conservador)	X	X
Módulo del motor de detección	✔	✔	✔	X
Otros módulos de protección	✔	✔	✔	X

* No recomendado

Determina la versión del producto, las versiones del módulo del programa y la fecha de la versión

1. Haga clic en **Ayuda y soporte** > **Acerca de ESET Security Ultimate**.
2. En la pantalla **Acerca de**, la primera línea muestra el número de la versión de su producto ESET.
3. Haga clic en **Componentes instalados** para acceder a información sobre módulos específicos.

Notas importantes

Hay varias notas importantes a tener en cuenta cuando se configura el umbral adecuado para su entorno:

- El umbral **Balanceado** se recomienda para la mayoría de las configuraciones.

- Mientras más alto sea el umbral de informes, más alta será la tasa de detección pero habrá más probabilidades de objetos identificados en forma errónea.

• Desde el punto de vista del mundo real, no existen garantías de una tasa de detección del 100 % ni tampoco 0 % de probabilidades de evitar la categorización incorrecta de objetos no infectados como malware.

• Mantenga actualizados ESET Security Ultimate y sus módulos para maximizar el equilibrio entre desempeño, precisión de tasas de detección y cantidad de objetos informados en forma errónea.

Configuración de protección

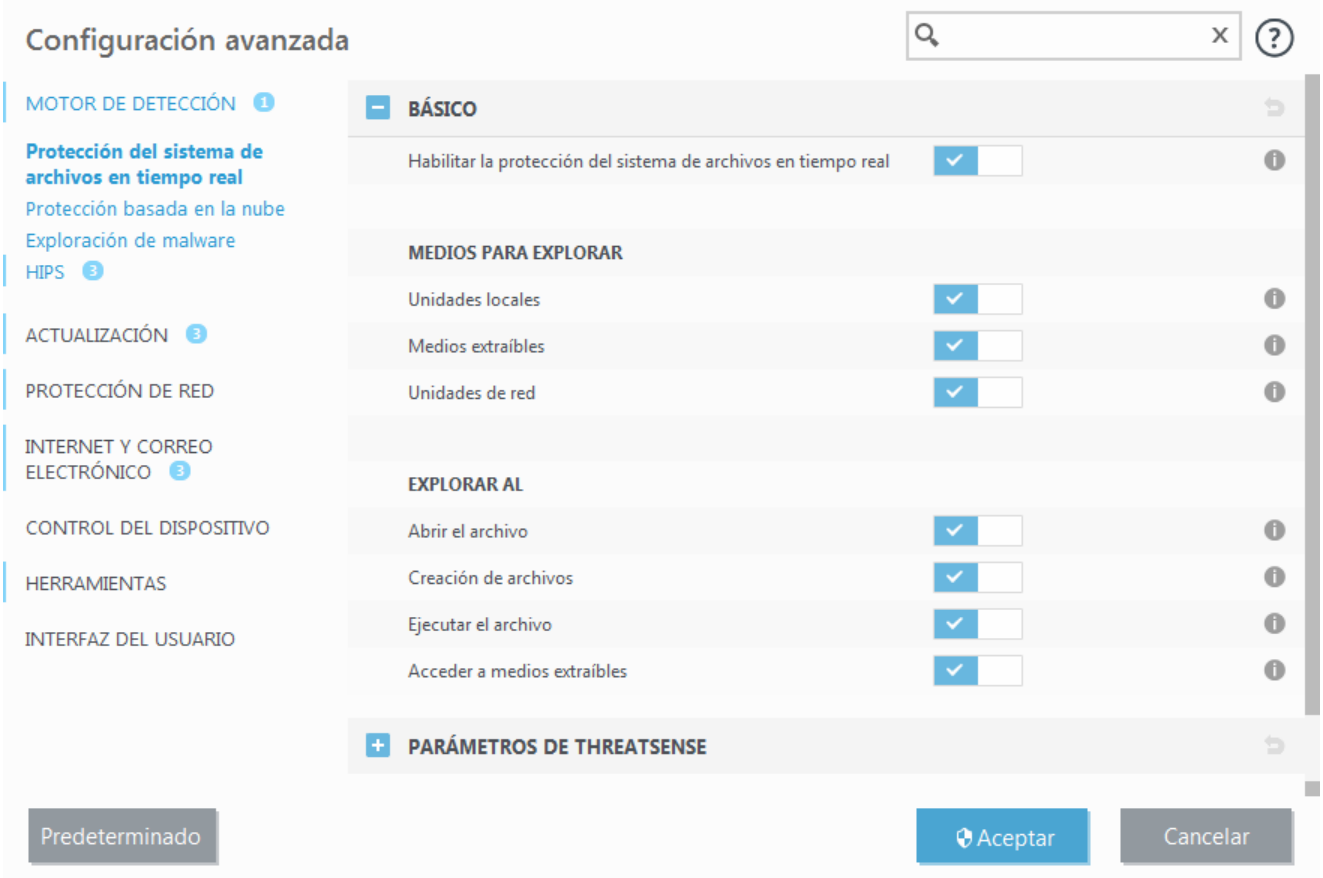
Si se reporta un objeto clasificado como CATEGORÍA, el programa bloquea el objeto, luego se lo desinfecta, elimina o coloca en Cuarentena.

Lea la información a continuación antes de modificar un umbral (o nivel) para la protección de CATEGORÍA:

Umbral	Explicación
Intenso	Las amenazas reportadas de nivel intenso (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección). Esta configuración se recomienda cuando todos los equipos han sido explorados con configuración agresiva y cuando los objetos reportados en forma errónea han sido agregados a las exclusiones de detección.
Balanceado	Las amenazas reportadas de nivel balanceado (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
Cauteloso	Las detecciones reportadas de nivel cauteloso se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
Desactivado	De utilidad para la identificación y exclusión de objetos reportados en forma errónea. La opción “Desactivado” no está disponible para la protección contra malware y es el valor predeterminado para las aplicaciones potencialmente no seguras.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los archivos del sistema para detectar código malicioso al abrirlos, crearlos o ejecutarlos.



En forma predeterminada, la protección del sistema de archivos en tiempo real se ejecuta junto al inicio del sistema y proporciona una exploración ininterrumpida. No recomendamos deshabilitar la opción **Habilitar la protección del sistema de archivos en tiempo real** en la Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Protección del sistema de archivos en tiempo real**.

Medios para explorar

En forma predeterminada, todos los tipos de medios se exploran en busca de amenazas potenciales:

- **Unidades locales** – Escanea todo el sistema y discos duros fijos (ejemplo: *C:*\, *D:*\).
- **Medios extraíbles** – Escanea CD/DVD, almacenamiento USB, tarjetas de memoria, etc.
- **Unidades de red** – Escanea todas las unidades de red asignadas (ejemplo: *H:*\ como *store04*) o unidades de red de acceso directo (ejemplo: *store08*).

Recomendamos que use la configuración predeterminada y solo modificarla en casos específicos, como por ej., si al explorar ciertos medios, se ralentizan significativamente las transferencias de archivos.

Explorar al

De forma predeterminada, todos los archivos se analizan cuando se abren, crean o ejecutan. Se recomienda mantener estas configuraciones predeterminadas, ya que proveen el máximo nivel de protección en tiempo real del equipo:

- **Abrir el archivo** – Escanea al abrir un archivo.
- **Creación del archivo** – Escanea al crear o modificar un archivo.

- **Ejecución del archivo** – Escanea al ejecutar un archivo.

- **Acceso al sector de inicio de medios extraíbles** – Cuando se inserta un medio extraíble que contiene un sector de inicio en un dispositivo, se explora de inmediato el sector de inicio. Esta opción no habilita la exploración de archivos de medios extraíbles. La exploración de archivos de medios extraíbles se encuentra en **Medios para explorar** > **Medios extraíbles**. Para que **Acceso al sector de inicio de medios extraíbles** funcione correctamente, mantenga habilitado **Sectores de inicio/UEFI** en ThreatSense.

Exclusiones de procesos

Consulte Exclusiones de procesos.

ThreatSense

La protección del sistema de archivos en tiempo real verifica todos los tipos de medios y el control se acciona por diversos sucesos, como el acceso a un archivo. Al usar los métodos de detección de la tecnología **ThreatSense** (descritos en ThreatSense), la protección del sistema de archivos en tiempo real puede configurarse para tratar nuevos archivos creados de modo diferente a los ya existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para controlar más de cerca a los nuevos archivos creados.

Para asegurar el mínimo impacto en el sistema al usar la protección en tiempo real, los archivos que ya se exploraron no se vuelven a explorar reiteradamente (a menos que se hayan modificado). Se exploran los archivos nuevamente inmediatamente después de cada actualización del motor de detección. Este comportamiento se controla mediante el uso de la **Optimización inteligente**. Si se deshabilita esta **Optimización inteligente**, se exploran todos los archivos cada vez que se accede a los mismos. 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 **Habilitar la optimización inteligente**.

La protección del sistema de archivos en tiempo real también le permite configurar Parámetros ThreatSense adicionales.

Exclusiones de procesos

La funcionalidad de Exclusiones de procesos le permite excluir procesos de la aplicación de la protección del sistema de archivos en tiempo real. Para mejorar la velocidad de la copia de seguridad, la integridad del proceso y la disponibilidad del servicio, se utilizan ciertas técnicas que se conoce que entran en conflicto con la protección contra el malware a nivel del archivo durante la copia de seguridad. La única manera de evitar con efectividad ambas situaciones consiste en desactivar el software contra el malware. Al excluir procesos específicos (por ejemplo, los que corresponden a la solución de la copia de seguridad), todas las operaciones de que se atribuyen a dichos procesos excluidos se ignoran y consideran seguras, por lo tanto, se minimiza la interferencia con el proceso de copia de seguridad. Le sugerimos que sea precavido al crear exclusiones: una herramienta de copia de seguridad que se ha excluido puede acceder a archivos infectados sin ejecutar una alerta, motivo por el cual solo se autorizan los permisos extendidos en el módulo de protección en tiempo real.

> No debe confundirse con Extensiones de archivo excluidas, Exclusiones de HIPS, Exclusiones de detección o Exclusiones de rendimiento.

Las exclusiones de los procesos contribuyen a atenuar el riesgo de que se produzcan conflictos y mejorar el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo en el rendimiento general y la estabilidad del sistema operativo. La exclusión de un proceso o 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 ha sido diseñada para excluir herramientas de copia de seguridad. El hecho de excluir procesos de la herramienta de copia de seguridad de la exploración no solo garantiza la estabilidad del sistema, sino que también afecta el rendimiento de la copia de seguridad, ya que la copia de seguridad no se ve ralentizada cuando se está ejecutando.

Haga clic en **Editar** para abrir la ventana de administración de **Exclusiones de procesos**, donde puede agregar exclusiones y buscar un archivo ejecutable (por ejemplo, *Backup-tool.exe*), que se excluirá de la exploración.
Tan pronto se agrega el archivo *.exe* a las exclusiones, la actividad de este proceso no se somete a la monitorización de ESET Security Ultimate y no se ejecutan exploraciones en ninguna operación de archivos que lleva a cabo este proceso.

Si no utiliza la función de buscar al seleccionar el proceso ejecutable, deberá ingresar manualmente la ruta completa al ejecutable. De lo contrario, la exclusión no funcionará correctamente y es posible que HIPS muestre errores.

También puede **Editar** los procesos existentes o **Eliminarlos** de las exclusiones.

En la protección de acceso a la web, no se tiene en cuenta esta exclusión. Por lo tanto, si excluye el archivo ejecutable del navegador web, seguirán explorándose los archivos descargados. De esta manera, pueden seguir detectándose las infiltraciones. Esta situación es solo un ejemplo. No recomendamos crear exclusiones para navegadores web.

Agregado o edición de exclusiones de procesos

Esta ventana de diálogo le permite **agregar** procesos excluidos del motor de detección. Las exclusiones de los procesos contribuyen a atenuar el riesgo de que se produzcan conflictos y mejorar el rendimiento de las aplicaciones excluidas, lo que, a su vez, tiene un efecto positivo en el rendimiento general y la estabilidad del sistema operativo. La exclusión de un proceso o aplicación es una exclusión de su archivo ejecutable (*.exe*).

Seleccione la ruta del archivo de una aplicación exceptuada al hacer clic en ... (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). NO ingrese el nombre de la aplicación.
Tan pronto se agrega el archivo *.exe* a las exclusiones, la actividad de este proceso no se somete a la monitorización de ESET Security Ultimate y no se ejecutan exploraciones en ninguna operación de archivos que lleva a cabo este proceso.

Si no utiliza la función de buscar al seleccionar el proceso ejecutable, deberá ingresar manualmente la ruta completa al ejecutable. De lo contrario, la exclusión no funcionará correctamente y es posible que HIPS muestre errores.

También puede **Editar** los procesos existentes o **Eliminarlos** de las exclusiones.

Cuándo modificar la configuración de la protección en tiempo real

La protección en tiempo real es el componente más imprescindible para mantener un sistema seguro. Siempre sea precavido al modificar sus parámetros. Recomendamos modificar los parámetros únicamente en casos específicos.

Después de la instalación de ESET Security Ultimate, todos los ajustes de configuración se optimizan para proporcionar el máximo nivel de seguridad del sistema para los usuarios. Para restaurar la configuración predeterminada, haga clic en ↩ junto a Configuración avanzada > **Protecciones** > **Respuestas de detección**.

Verificación de la protección en tiempo real

Para verificar que la protección en tiempo real se encuentra activa y es capaz de detectar virus, use un archivo de prueba de *www.eicar.com*. Este archivo de prueba es un archivo inofensivo, al que detectan todos los programas antivirus. El archivo fue creado por la empresa EICAR (European Institute for Computer Antivirus Research, Instituto Europeo para la Investigación de los Antivirus Informáticos, por sus siglas en inglés) para comprobar la eficacia de los programas antivirus.

El archivo está disponible para su descarga desde http://www.eicar.org/download/eicar.com.
Después de introducir esta URL en su navegador, debería visualizar un mensaje que indica que se eliminó la amenaza.

Qué hacer si la protección en tiempo real no funciona

En esta sección, se describirán problemas que se pueden presentar al utilizar la protección en tiempo real y se indicará cómo resolverlas.

La protección en tiempo real está deshabilitada

Si un usuario desactiva la protección en tiempo real sin darse cuenta, 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 equipo** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no se activa durante el inicio del sistema, es posible que se deba a que **Habilitar la protección del sistema de archivos en tiempo real** está deshabilitada. Para asegurarse de que esta opción esté habilitada, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no detecta ni desinfecta infiltraciones

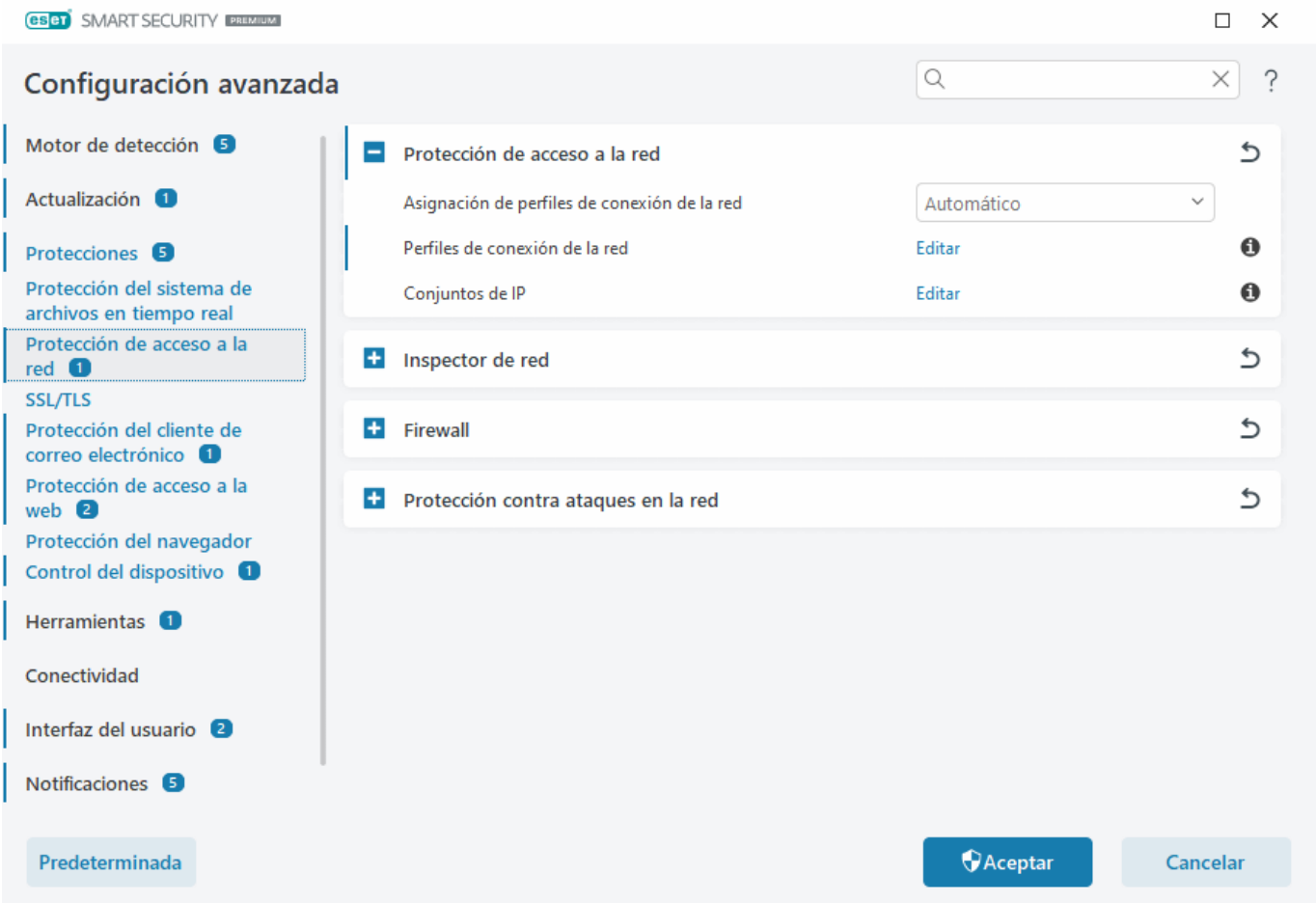
Asegúrese de que no haya otros programas antivirus instalados en el equipo. Si hay dos programas antivirus instalados a la vez, es posible que tengan conflictos entre ellos. Es recomendable desinstalar cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y está activada la opción **Activar protección del sistema de archivos en tiempo real**), es posible que se deba a conflictos con otros programas. Para resolver este problema, cree un registro de ESET SysInspector y envíelo a Soporte técnico de ESET para su análisis.

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 a su equipo en redes específicas, permitir/denegar el acceso a dispositivos de red desde su equipo y más, según la configuración. De forma predeterminada, ESET Security Ultimate tiene reglas de firewall preconfiguradas y protección de acceso a la red para una máxima seguridad. Sin embargo, es posible que determinados entornos necesiten una configuración personalizada. El cambio de la configuración predeterminada debe llevarlo a cabo únicamente un usuario experimentado.



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 firewall para conexiones de red específicas.

Conjuntos de IP: puede definir colecciones de direcciones IP que conforman un grupo lógico de direcciones IP,

que puede utilizar para las reglas de firewall.

Inspector de red

Firewall

Protección contra ataques de red

Perfiles de conexión de la red

Los perfiles se pueden utilizar para controlar el comportamiento de la protección de red ESET Security Ultimate para conexiones de red específicas. Al crear o editar una regla de firewall, una regla IDS o una regla de protección contra ataques por fuerza bruta, puede asignarla a un perfil específico o aplicarla a todos los perfiles. Cuando un perfil esté activo en una conexión de red, solo se aplicarán las reglas globales (reglas sin ningún perfil especificado) y las reglas asignadas a dicho perfil. Puede crear diversos perfiles con diferentes reglas asignadas a las conexiones de red para modificar el comportamiento del firewall fácilmente.

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 la red: 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 **Solicitar** en el menú desplegable) Configurar la protección de red y se asigne 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 > **Configuración** > **Protección de red** > **Conexiones de red**. Desplácese sobre una conexión de red específica y haga clic en el icono de menú ⋮ > **Editar** para abrir la ventana Configurar protección de red y seleccione un perfil.

Perfiles de conexión de la 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 redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de 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.

Público: para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a 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 cambie a otro perfil, aparecerá 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 ventana lista de **perfiles de conexión de red**.

Los siguientes perfiles están predefinidos y no se pueden editar/eliminar:

Privado: para redes confiables (red doméstica o de oficina). Su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto está disponible). Recomendamos el uso de 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.

Público: para redes no confiables (red pública). Los archivos y las carpetas en su equipo no se comparten con otros usuarios en la red o no están visibles para ellos, y el uso compartido de recursos del equipo está desactivado. Recomendamos el uso de esta configuración al acceder a redes inalámbricas. Este perfil se asigna automáticamente a cualquier conexión de red que no esté configurada como Dominio o Red privada en Windows.

Arriba/Superior/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 su prioridad. Siempre se aplica el primer perfil coincidente).

Agregar o editar un perfil

El perfil de conexión de red personalizado permite aplicar reglas de firewall y definir configuraciones adicionales para conexiones de red específicas. Especificará a qué conexiones de red se asignará el perfil personalizado en la sección Activadores.

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 para su perfil.

Descripción: descripción del perfil para identificarlo con mayor facilidad.

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: su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo (el acceso a archivos e impresoras compartidos está habilitado, la comunicación entrante RPC está habilitada y el uso compartido de escritorio remoto 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 es

255.255.255.0, la subred 192.168.1.0/24 se agregará a la zona de confianza de dicha conexión de red. Si el adaptador tiene más direcciones/subredes, todas serán de confianza.

Informar sobre cifrado Wi-Fi débil: ESET Security Ultimate mostrará una notificación de escritorio cuando se conecte a una red inalámbrica desprotegida o a una red con 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 definidos en activadores para un perfil de red conectado, 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 perfiles de conexión de red. Un usuario experimentado debe llevar a cabo la creación de perfiles de conexión de red personalizados.

Los siguientes activadores están disponibles (si desea conocer los detalles de su red actual, consulte Conexiones de red):

Adaptador

Tipo de adaptador: aplica el perfil si la conexión de red se establece en el tipo de adaptador seleccionado.
Nombre del adaptador: aplica el perfil si el nombre del adaptador de red coincide.
IP del adaptador: aplica el perfil si la dirección IP del adaptador de red coincide.

DNS

Sufijo DNS: aplica el perfil si el nombre de dominio coincide.
IP**DNS**: aplica el perfil si la dirección IP del servidor DNS coincide.

WINS

Aplica el perfil si la Windows Internet Name Service (WINS) dirección IP asignada coincide.

DHCP

IP DHCP: coincide con la dirección IP del servidor DHCP.

Puerta de enlace predeterminada

IP: aplica el perfil si la dirección IP de la puerta de enlace predeterminada coincide.
Dirección MAC: aplica el perfil si la dirección MAC de la puerta de enlace predeterminada coincide.

Wi-Fi

SSID:aplica el perfil si el SSID (nombre de la red Wi-Fi) coincide.
Nombre del perfil: aplica el perfil si el nombre del perfil de Wi-Fi coincide.
Tipo de seguridad: aplica el perfil si el tipo de seguridad coincide con el seleccionado en el menú desplegable. Si quiere hacer coincidir más de uno, cree otro activador.
Tipo de cifrado: aplica el perfil si el tipo de cifrado coincide con el seleccionado en el menú desplegable. Si quiere hacer coincidir más de uno, cree otro activador.
Seguridad de red: aplica el perfil si la red está **abierta/protegida**.

Perfil de Windows

Aplica el perfil si la red está configurada en Windows como **Dominio/Privado/Público**.

Autenticación

La autenticación de red busca un servidor específico en la red y usa cifrado asimétrico (RSA) para autenticar dicho 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 mediante alguno de los siguientes tipos de archivos:
• Clave pública cifrada PEM (.pem); puede generar esta clave con 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 realizó con éxito. Si la autenticación no está configurada correctamente, se mostrará uno de los siguientes mensajes de error:
Falló la autenticación del servidor. Firma no válida o que no coincide.
La firma del servidor no coincide con la clave pública ingresada.
Falló la autenticación del servidor. El nombre de la red no coincide.
El nombre de la red configurada no corresponde al nombre de la red del servidor de autenticación. Revise los dos nombres y asegúrese de que sean iguales.
Falló la autenticación del servidor. No válido o sin respuesta desde el servidor.
No se recibe respuesta alguna si el servidor no está en funcionamiento o no se puede acceder al mismo. Se puede recibir una respuesta no válida si otro servidor HTTP se ejecuta en la dirección especificada.
Se ingresó una clave pública no válida.
Verifique que el archivo de la clave pública que ha ingresado no esté dañado.

Conjuntos de IP

Un conjunto de IP es una colección de direcciones IP que conforman un grupo lógico de direcciones IP, y que es útil cuando se reutiliza el mismo conjunto de direcciones en distintas reglas de firewall o reglas de protección contra ataques por fuerza bruta. ESET Security Ultimate también contiene conjuntos de IP predefinidos para los que se aplican reglas internas. Un ejemplo de este tipo de grupo es la **zona de confianza**. La zona de confianza representa un grupo de direcciones de red donde su equipo y los archivos compartidos almacenados en su equipo están visibles para otros usuarios en la red y estos pueden acceder a los recursos del equipo.

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 equipo 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 equipos remotos.

Descripción: descripción general del grupo.

Direcciones IP: direcciones de IP remotas que pertenecen a un conjunto de IP.

Elementos de control

Cuando **agrega** o **edita** un conjunto de IP, los siguientes campos se encuentran disponibles:

Nombre – nombre de un grupo de equipos remotos.

Descripción: descripción general del grupo.

Dirección del equipo remoto (IPv4, IPv6, rango, máscara) – le permite agregar una dirección remota, un rango de direcciones o una subred.

Eliminar: elimina una zona de la lista.

Los conjuntos de IP predefinidos no se pueden eliminar.

Ejemplos de direcciones IP

Agregar dirección IPv4:
Dirección única: agrega una dirección IP de un equipo individual (por ejemplo, *192.168.0.10*).
Rango de direcciones: escriba la primera y la última dirección IP para especificar el rango de IP de varios equipos (por ejemplo, *192.168.0.1 a 192.168.0.99*).
Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red para 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 equipo individual (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subred: la subred (un grupo de equipos) está definida 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 la red confiable (red doméstica o red de oficina) (por ejemplo, puertos abiertos o una contraseña de router débil). También le brinda una lista de dispositivos

conectados, categorizados por tipo de dispositivo (por ejemplo, impresora, router, dispositivo móvil, etc.) para mostrar qué está conectado a su red (por ejemplo, consolas de videojuegos, dispositivos de IoT u otros dispositivos inteligentes del hogar). Puede configurar el Inspector de red en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Inspector de red**.

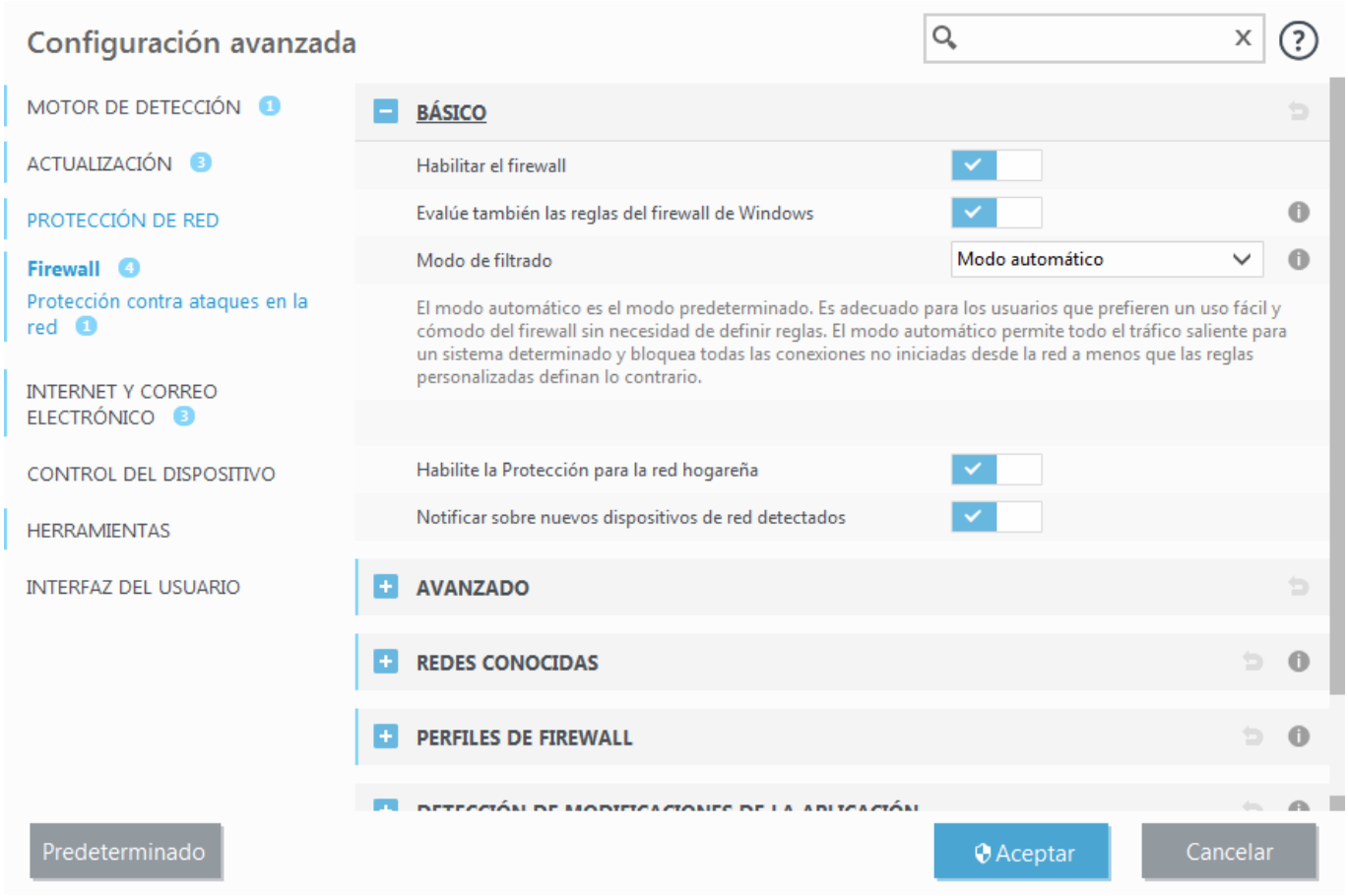
Activar el Inspector de red – Inspector de red permite identificar vulnerabilidades en redes hogareñas, como puertos abiertos o una contraseña de enrutador poco segura. Asimismo, ofrece una lista de dispositivos conectados, categorizados por tipo de dispositivo.

Notificar sobre nuevos dispositivos de red detectados: le notifica cuándo se detecta un nuevo dispositivo en su red.

Firewall

El firewall controla todo el tráfico de red entrante y saliente en su equipo en función de las reglas internas y las reglas definidas por usted. Para ello, permite o deniega las conexiones de red individuales. El firewall brinda protección frente a ataques desde dispositivos remotos y bloquea ciertos servicios potencialmente amenazantes.

Para configurar el firewall, abra **Configuración avanzada** > Protecciones > **Protección de acceso a la red** > **Firewall**.



Firewall

Habilitar el firewall

Le recomendamos dejar habilitada esta función para garantizar la seguridad de su sistema. Con el firewall

habilitado, el tráfico de red se analiza en ambas direcciones.

Reglas

La configuración de reglas le permite ver y editar todas las reglas de firewall que se aplican al tráfico generado por cada aplicación individual dentro de las zonas de confianza e Internet.

> Puede crear una regla IDS cuando un Botnet ataca su equipo. Se puede modificar una regla en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra los ataques a la red** > **Reglas IDS** con clic en **Editar**.

Evalúe también las reglas del firewall de Windows

En el modo de filtrado automático, también permita el tráfico entrante permitido por las reglas del firewall de Windows, a menos que sea explícitamente bloqueado por las reglas de ESET.

Modo de filtrado

La conducta del firewall cambia de acuerdo con el modo de filtrado. Los modos de filtrado también influyen en el nivel requerido de interacción del usuario.

Los siguientes son los modos de filtrado disponibles para el firewall de ESET Security Ultimate:

Modo de filtrado	Descripción
Modo automático	Es el modo predeterminado. Este modo resulta adecuado para los usuarios que prefieren un uso sencillo y conveniente del firewall sin la necesidad de definir reglas. Se pueden crear reglas personalizadas y definidas por el usuario, pero no se requieren en el **modo automático**. El modo automático da lugar al tráfico saliente para un sistema determinado y bloquea la mayoría del tráfico entrante, a excepción de una cantidad de tráfico de la Zona de confianza (según se especifica en sistema de detección de intrusiones y opciones avanzadas/servicios permitidos) y respuestas a las comunicaciones entrantes recientes.
Modo interactivo	Modo interactivo: permite crear una configuración personalizada para el firewall. Cuando se detecta una comunicación y no existe ninguna regla que se aplique a ella, se mostrará una ventana de diálogo para informar sobre la existencia de una conexión desconocida. La ventana de diálogo da la opción de permitir o denegar la comunicación y dicha decisión puede guardarse como una nueva regla para el Firewall. Si elige crear una nueva regla, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla.
Modo basado en políticas	Bloquea todas las conexiones que no están definidas por una regla específica que las permita. Este modo hace posible que los usuarios avanzados definan reglas para permitir solo las conexiones deseadas y seguras. El Firewall bloqueará todas las demás conexiones que no estén especificadas.
Modo de aprendizaje	Crea y guarda las reglas automáticamente; este modo se recomienda para la configuración inicial del firewall, pero no se debe dejar encendido durante períodos prolongados. No se requiere la interacción del usuario porque ESET Security Ultimate guarda las reglas según los parámetros predefinidos. El modo de aprendizaje solo debe usarse hasta que se hayan creado todas las reglas para las comunicaciones requeridas y se puedan evitar inconvenientes de seguridad.

El modo de aprendizaje finalizará en: establezca la fecha y la hora en que el modo de aprendizaje finaliza automáticamente. También puede desactivar el modo de aprendizaje manualmente cuando lo desee.

Modo configurado después del vencimiento del modo de aprendizaje: defina a qué modo de filtrado se

restablecerá el firewall una vez finalizado el período para el modo de aprendizaje. Lea más sobre los modos de filtrado en la tabla anterior. Al finalizar, la opción **Preguntar al usuario** requiere privilegios administrativos para realizar un cambio en el modo de filtrado del firewall.

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 característica de detección de modificaciones de la aplicación muestra notificaciones si alguna aplicación modificada, para la que existe una regla de Firewall, intenta establecer una conexión.

Configuración de modo de aprendizaje

El modo de aprendizaje crea y guarda automáticamente una regla por cada comunicación que se ha establecido en el sistema. No se requiere la interacción del usuario porque ESET Security Ultimate guarda las reglas según los parámetros predefinidos.

Este modo puede exponer su sistema a riesgos, y solo se recomienda para la configuración inicial del Firewall.

Seleccione **Aprendizaje** en el menú desplegable en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Firewall** > **Firewall** > **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 firewall no filtra la comunicación cuando el modo de aprendizaje está activado. Se permiten todas las comunicaciones entrantes y salientes. En este modo, el equipo no cuenta con la protección completa del firewall.

Tráfico entrante de una zona de confianza – un ejemplo de una conexión entrante dentro de la zona de confianza es un dispositivo remoto de una zona de confianza que intenta establecer una comunicación con una aplicación activa en el equipo local.

Tráfico saliente a una zona de confianza – una aplicación remota que intenta establecer una conexión con otro dispositivo dentro de la red local o dentro de una red de la zona segura.

Tráfico de Internet entrante – un dispositivo remoto que intenta comunicarse con una aplicación ejecutada en el equipo.

Tráfico de Internet saliente – una aplicación local que intenta establecer una conexión con otro dispositivo.

Cada sección le permite definir los parámetros que se agregarán a las reglas recién creadas:

Agregar puerto local – incluye el número del puerto local de la comunicación de red. Para comunicaciones salientes, normalmente se generan números aleatorios. Por este motivo, es recomendable activar esta opción solo para las comunicaciones entrantes.

Agregar aplicación – incluye el nombre de la aplicación local. Esta opción es útil para reglas futuras en el nivel de las aplicaciones (reglas que definen la comunicación para una aplicación completa). Por ejemplo, puede activar la comunicación solo para un navegador Web o para un cliente de correo electrónico.

Agregar puerto remoto – incluye el número del puerto remoto de la comunicación de red. Por ejemplo, puede

permitir o denegar un servicio específico asociado a un número de puerto estándar (HTTP – 80, POP3 – 110, etc.).

Agregar dirección IP remota/Zona de confianza – se puede utilizar una dirección IP o zona remota como parámetro para la creación de nuevas reglas que definan todas las conexiones de red entre el sistema local y dicha dirección o zona remota. Esta opción resulta útil cuando el usuario desea definir acciones para un dispositivo específico o un grupo de dispositivo en red.

Cantidad máxima de reglas diferentes por cada aplicación – si una aplicación establece una comunicación a través de diferentes puertos, con varias direcciones IP, etc., el Firewall en modo de aprendizaje crea la cantidad de reglas adecuada para dicha aplicación. Esta opción le permite limitar el número de reglas que se pueden crear para una sola aplicación.

Reglas de firewall

Las reglas de Firewall representan un grupo de condiciones usadas para evaluar en forma significativa todas las conexiones de red y todas las acciones asignadas a dichas condiciones. Con las reglas de Firewall, puede definir la acción a realizar cuando se establecen diferentes tipos de conexiones de red.

Las reglas se evalúan de arriba abajo y puede ver su prioridad en la primera columna. La acción de la primera regla que coincida se utiliza para cada conexión de red que se está evaluando.

Las conexiones pueden dividirse en entrantes y salientes. Las conexiones entrantes son iniciadas por un dispositivo remoto que intenta establecer una conexión con el sistema local. Las conexiones salientes funcionan de la forma opuesta: el sistema local Contacta a un dispositivo remoto.

Cada vez que se detecte una nueva comunicación, deberá analizar cuidadosamente si la permitirá o la rechazará. Las conexiones no solicitadas, no seguras o desconocidas constituyen un riesgo para el sistema. Si se establece una conexión de ese tipo, es recomendable prestar especial atención al dispositivo remoto y a la aplicación que trata de conectarse a su equipo. Muchas infiltraciones intentan obtener y enviar datos confidenciales, o descargar otras aplicaciones maliciosas en las estaciones de trabajo locales. El firewall permite detectar y finalizar dichas conexiones.

Puede ver y editar las reglas de firewall en Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Firewall** > **Reglas** > **Editar**.

Si tiene muchas reglas de firewall, puede usar un filtro para mostrar solo reglas específicas. Para filtrar las reglas de firewall, haga clic en **Más filtros** encima de la lista Reglas de firewall. Puede filtrar las reglas en función de los siguientes criterios:

- Origen
- Dirección
- Acción
- Disponibilidad

De forma predeterminada, las reglas de firewall predefinidas están ocultas. Para mostrar todas las reglas predefinidas, desactive el interruptor situado junto a **Ocultar reglas integradas (predefinidas)**. Puede deshabilitar estas reglas, pero no puede eliminar una regla predefinida.

Haga clic en el icono de búsqueda ubicado en la parte superior derecha para buscar la(s) regla(s).

Columnas

Prioridad: las reglas se evalúan de arriba a abajo y puede ver su prioridad en la primera columna.

Habilitada: muestra si una regla está habilitada o deshabilitada; la casilla de verificación correspondiente debe estar seleccionada para habilitar una regla.

Aplicación: la aplicación a la que se aplica la regla.

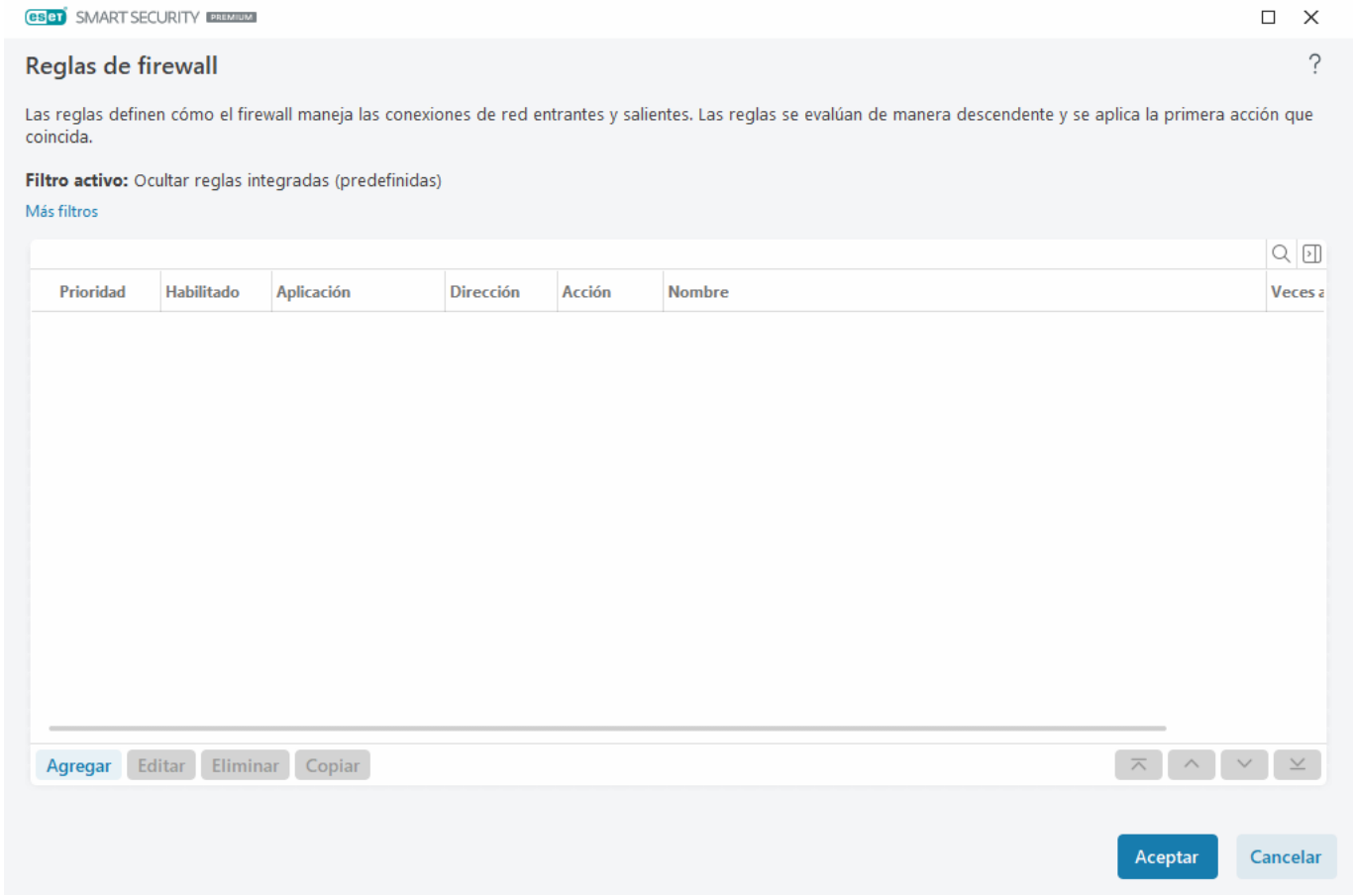
Dirección: dirección de la comunicación (entrante/saliente/ambas).

Acción: muestra el estado de la comunicación (bloquear/permitir/preguntar).

Nombre: nombre de la regla. El icono de ESET representa una regla predefinida.

Veces aplicadas: la cantidad 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 regla nueva.

Editar: Edita una regla existente.

Quitar: elimina una regla existente.

Copiar: crea una copia de la regla seleccionada.

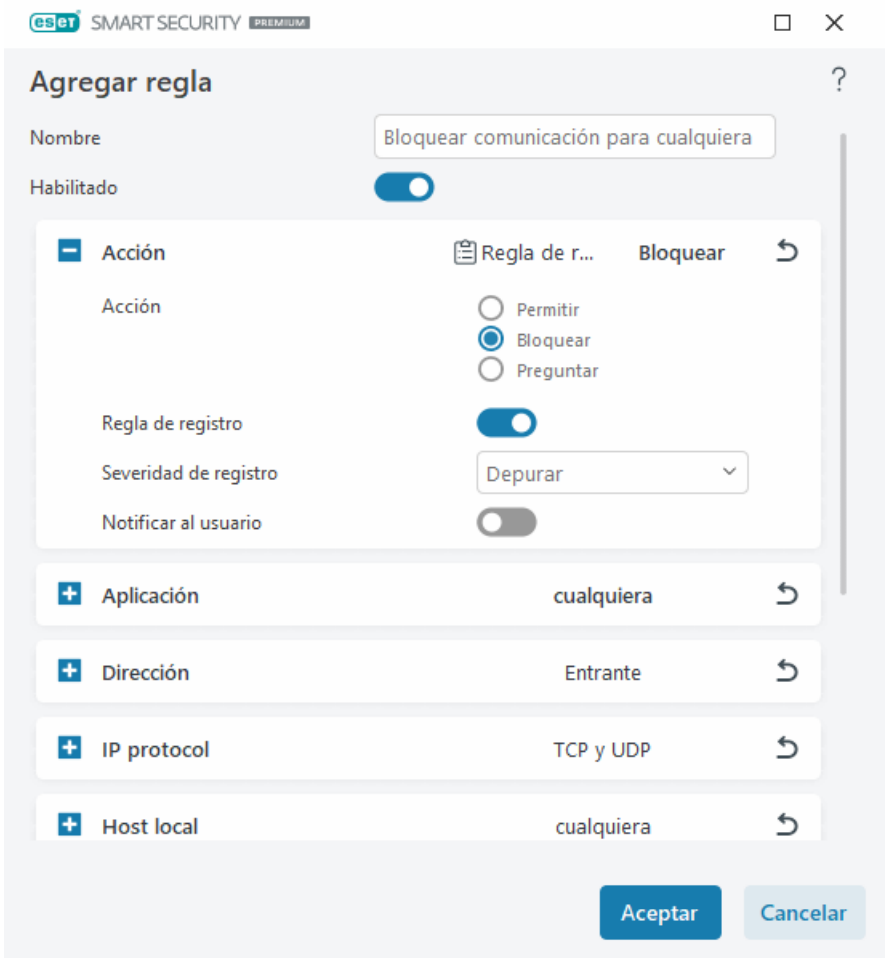
 **Superior/Arriba/Abajo/Inferior** – le permite ajustar el nivel de prioridad de las reglas (las reglas se ejecutan desde arriba hacia abajo).

Agregar o editar reglas del firewall

Las reglas de Firewall representan condiciones usadas para evaluar en forma significativa todas las conexiones de red y las acciones asignadas a dichas condiciones. La edición o incorporación de reglas del firewall puede ser necesaria cuando la configuración de red cambia (por ejemplo, se modifica la dirección de red o el número de puerto de la ubicación remota) para garantizar el correcto funcionamiento de la aplicación afectada por una regla. Un usuario experimentado debe crear reglas de firewall personalizadas.

> **Instrucciones ilustradas**
> Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:
> - Abrir o cerrar (permitir o rechazar) un puerto específico en el firewall de ESET
> - Crear una regla de firewall desde los archivos de registro en ESET Security Ultimate

Para agregar o editar una regla de firewall, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Firewall** > **Reglas** > **Editar**. En la ventana Reglas de firewall, haga clic en **Agregar** o **Editar**.



Nombre: escriba un nombre para la regla.

Habilitado: haga clic en el interruptor para activar la regla.

Agregue acciones y condiciones para la regla de firewall:

Acción

Acción: seleccione si desea **Permitir**/**Bloquear** la comunicación que coincida con las condiciones definidas en esta regla o si desea ESET Security Ultimate **Preguntar** cada vez que se establezca la comunicación.
Regla de registro: si se aplica la regla, se registrará en Archivos de registro.
Severidad de registro: seleccione la severidad del historial de registro para esta regla.
Notificar al usuario – muestra una notificación cuando se aplica la regla.

Aplicación

Especifique una aplicación en la que se aplicará esta regla.
Ruta 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 solo el nombre de la aplicación
Firma de la aplicación: puede aplicar la regla a las aplicaciones en función de sus firmas (nombre del editor). Seleccione en el menú desplegable si desea aplicar la regla a aplicaciones con **Cualquier firma válida** o a aplicaciones **firmadas por un firmante específico**. Si selecciona aplicaciones **Firmadas por un firmante específico**, debe definir el firmante en el campo **Nombre del firmante**.
Aplicación de Microsoft Store: selecciona una aplicación instalada en Microsoft Store en el menú desplegable.
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 mientras sólo se ve una ventana de aplicación. Haga clic en el interruptor para habilitar la regla para cada proceso 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.

Host 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 hosts 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 con clic en **Editar** junto a **conjuntos de IP**.

Puerto local

Números de **puertos** locales. Si no se proporcionan números, la regla se aplicará a cualquier puerto. Puede agregar 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 hosts 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 con clic en **Editar** junto a **conjuntos de IP**.

Puerto remoto

Números de **puertos** remotos. Si no se proporcionan números, la regla se aplicará a cualquier puerto. Puede agregar un solo puerto de comunicación o un rango de puertos de comunicación.

Perfil

Se puede aplicar una regla de firewall a perfiles de conexión de 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. Seleccione la casilla de verificación junto a los perfiles que quiere seleccionar.

Creamos una nueva regla para permitir que la aplicación del navegador web Firefox tenga acceso a Internet/los sitios web de la red local:
1.En la sección **Acción**, seleccione **Acción** > **Permitir**.
2.En la sección **Aplicación**, especifique la **ruta de aplicación** del explorador web (por ejemplo C:\Program Files\Firefox\Firefox.exe). NO escriba solo el nombre de la aplicación
3.En la sección **Dirección**, seleccione **Dirección** > **Saliente**.
4.En la sección **Protocolo IP**, seleccione **TCP & 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

La característica de detección de modificaciones de la aplicación muestra notificaciones si alguna aplicación modificada, para la que existe una regla de firewall, intenta establecer una conexión. La modificación de la aplicación es un mecanismo que permite reemplazar temporalmente o en forma definitiva una aplicación original por otro archivo ejecutable de la aplicación (brinda protección contra las reglas de firewall abusivas).

Tenga en cuenta que esta característica no está destinada a detectar modificaciones en cualquier aplicación en general. El objetivo es evitar el abuso de las reglas de firewall existentes, y solo se supervisan las aplicaciones para las que existen reglas de firewall específicas.

Para editar la **detección de modificaciones de la aplicación**, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Firewall** > **Detección de modificaciones de la aplicación**.

Habilitar la detección de modificaciones en las aplicaciones – si se selecciona, 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 firewall.

Permitir la modificación de aplicaciones firmadas (de confianza) – no notifica si la aplicación tiene la misma firma digital válida antes y después de la modificación.

Lista de aplicaciones excluidas de la detección: esta ventana le permite agregar o eliminar aplicaciones individuales para las cuales se permiten modificaciones sin notificación.

Lista de aplicaciones excluidas de la detección

El firewall en ESET Security Ultimate detecta los cambios en las aplicaciones para las que existen reglas (consulte Detección de modificaciones de la aplicación).

En algunos casos, quizá no le interese usar esta funcionalidad para ciertas aplicaciones si desea excluirlas de la verificación que realiza el firewall.

Agregar: abre una ventana donde puede seleccionar una aplicación para agregarla a la lista de aplicaciones excluidas de la detección de modificaciones. Puede elegir de una lista de aplicaciones en ejecución con comunicación de red abierta, para la cual existen reglas de Firewall, o agregar una aplicación específica.

Editar: abre una ventana donde puede cambiar la ubicación de una aplicación que se encuentra en la lista de aplicaciones excluidas de la detección de modificaciones. Puede elegir de una lista de aplicaciones en ejecución con comunicación de red abierta, para la cual existen reglas de firewall, o cambiar la ubicación de forma manual.

Quitar – quita entradas de la lista de aplicaciones excluidas de la detección de modificaciones.

Protección contra ataques en la red (IDS)

La protección contra ataques de red (IDS) mejora la detección de exploits para vulnerabilidades conocidas. Lea más sobre la protección contra ataques de red en el Glosario. Para configurar la protección contra ataques a la red, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques a la red**.

Habilitar la Protección contra ataques en la red (IDS) – Analiza el contenido del tráfico de la red y protege de ataques en la red. Todo tráfico que se considere perjudicial será bloqueado.

Habilitar protección contra botnets: detecta y bloquea la comunicación con los servidores maliciosos de comando y control según patrones típicos cuando el equipo está infectado y un bot está tratando de comunicarse. Lea más sobre la protección contra botnets en el glosario ***.

Reglas IDS – Esta opción le permite configurar opciones avanzadas de filtrado para detectar diversos tipos de ataques y exploits que se pueden utilizar para dañar su equipo.

> **Instrucciones ilustradas**
> Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:
> - Excluir una dirección IP de IDS en ESET Security Ultimate

Todos los eventos importantes detectados por la protección de red se guardan en un archivo de registro. Consulte registro de protección de red para obtener más información.

Reglas 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 posible ataque. Por ejemplo, puede agregar la dirección segura conocida a las direcciones excluidas de la zona del IDS para que evada el IDS.

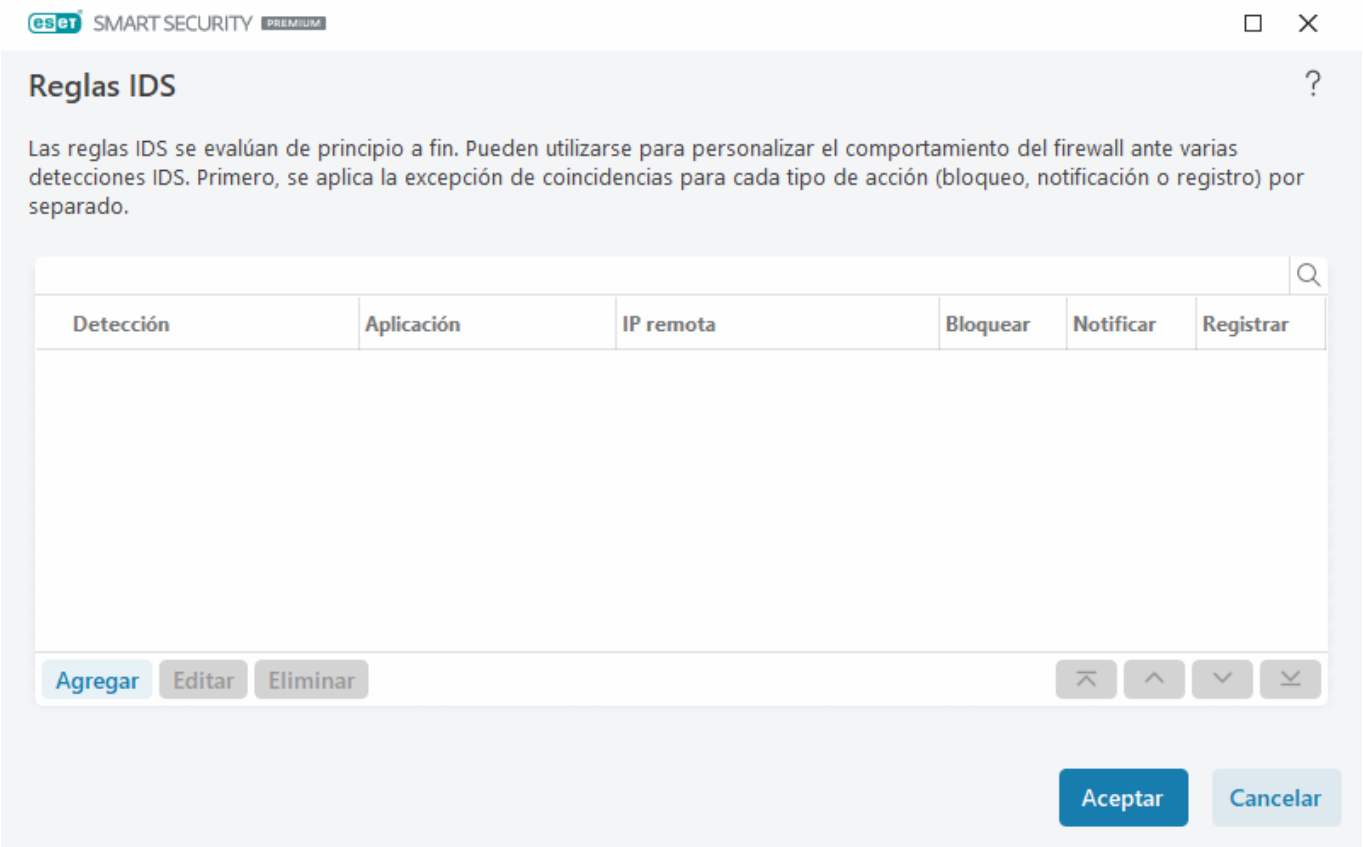
Instrucciones ilustradas

Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- Excluir una dirección IP de IDS en ESET Security Ultimate

Administrar reglas IDS

- **Agregar**: haga clic para crear una nueva regla IDS.
- **Editar**: haga clic para editar una regla IDS existente.
- **Quitar**: seleccione y haga clic si desea quitar una regla existente de la lista de reglas IDS.
- **Superior/Arriba/Abajo/Inferior**: le permite ajustar el nivel de prioridad de las reglas (las excepciones se evalúan desde arriba hacia abajo).



Editor de reglas

Detección: tipo de detección

Nombre de amenaza: puede especificar un nombre de amenaza para algunas de las detecciones disponibles.

Aplicación : seleccione la ruta del archivo de una aplicación exceptuada al hacer clic en ... (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). NO ingrese el nombre de la aplicación.

Dirección IP remota: una lista de direcciones/rangos/subredes IPv4 o IPv6 remotas. Si incluye varias direcciones, deben estar separadas por una coma.

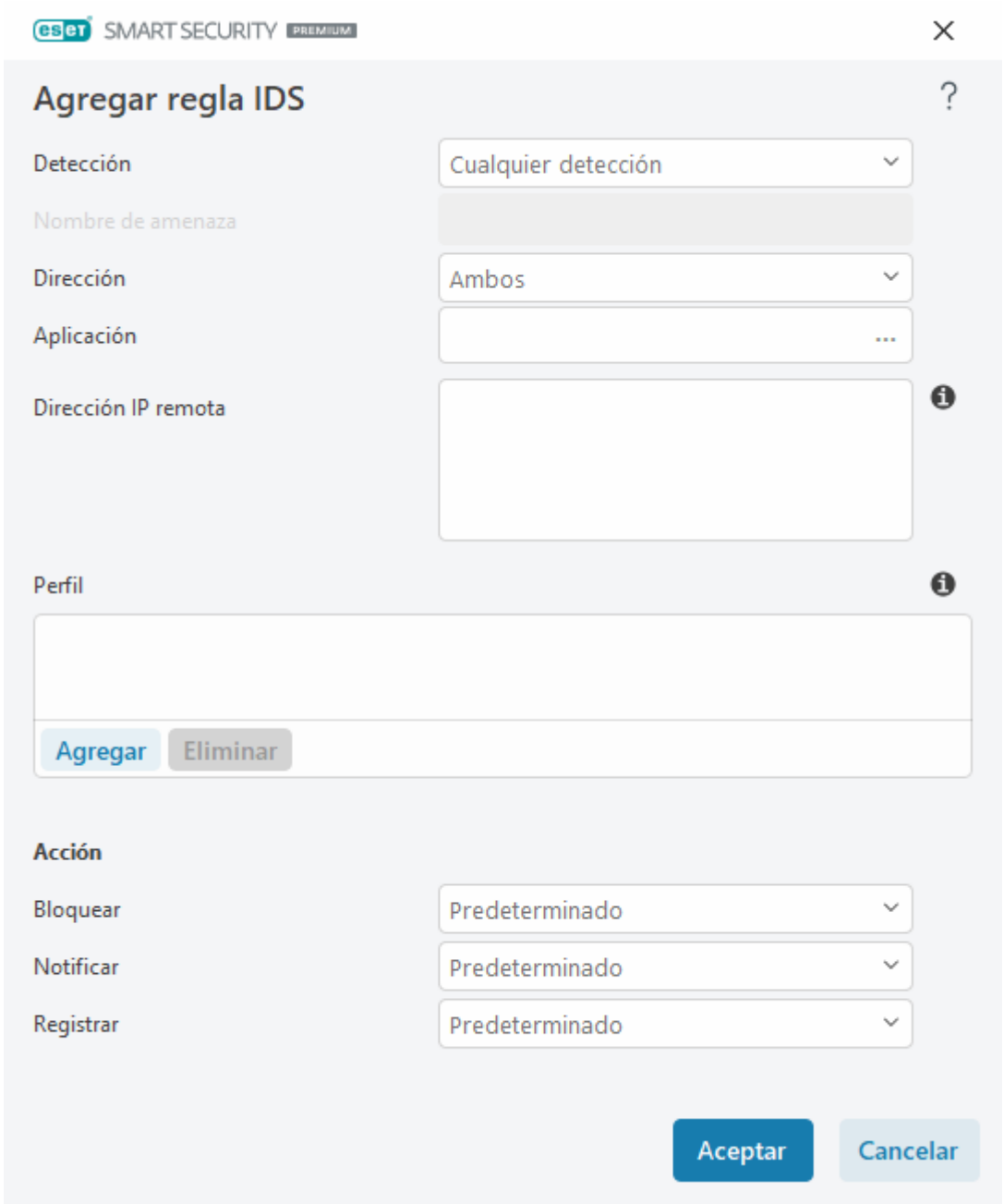
Perfil: puede elegir un perfil de conexión de red al que se aplicará esta regla.

Acción

Bloquear : cada proceso de sistema tiene su propia conducta predeterminada y acción asignada (bloquear o permitir). Para anular la conducta predeterminada de ESET Security Ultimate, puede seleccionar si bloquearla o permitirla mediante el uso del menú desplegable.

Notificar : seleccione Sí para mostrar las notificaciones de escritorio en su equipo. Seleccione No si no quiere recibir notificaciones de escritorio. Los valores disponibles son Predeterminado/Sí/No.

Registro: Seleccione **Sí** para registrar eventos en archivos de registro. Seleccione **No** si no quiere recibir eventos de registro. Los valores disponibles son **Predeterminado/Sí/No**.



Si quiere mostrar una notificación y recopilar un registro cada vez que ocurre el evento:
1.Haga clic en **Agregar** para agregar una nueva regla IDS.
2.Seleccione la detección específica del menú desplegable **Detección**.
3.Seleccione una ruta de aplicación haciendo clic en **...** para el que desea aplicar esta notificación.
4.Deje la opción **Predeterminado** en el menú desplegable **Boquear**. De esta manera, se heredará la acción predeterminada aplicada por ESET Security Ultimate.
5.Seleccione ambos menús desplegables **Notificar** y **Registrar** en la opción **Sí**.
6.Haga clic en **Aceptar** para guardar esta notificación.

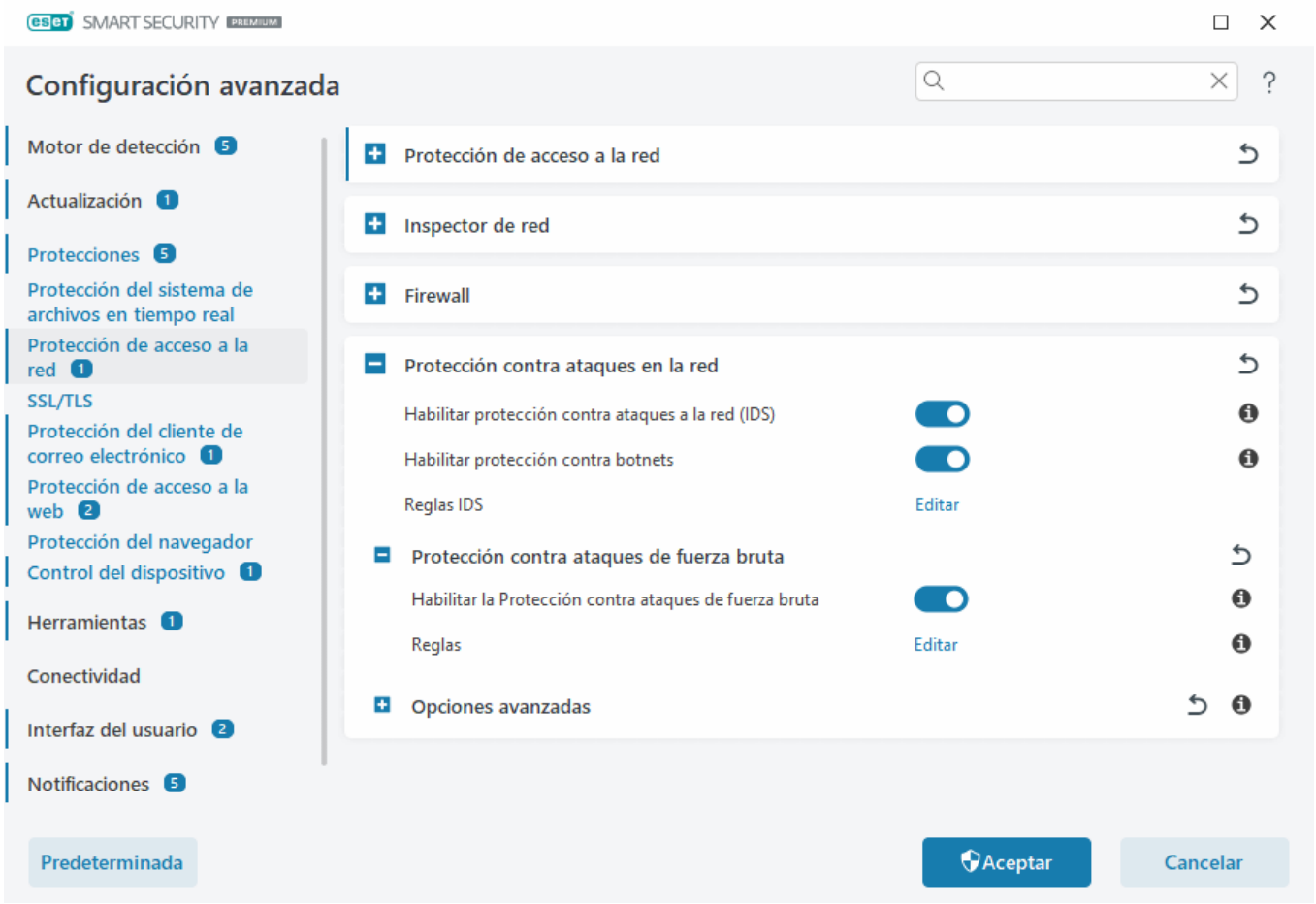
Si no quiere mostrar una notificación recurrente que no considera una amenaza de un tipo particular de **detección**:
1.Haga clic en **Agregar** para agregar una nueva regla IDS.
2.Seleccione la detección específica del menú desplegable **Detección**, por ejemplo, **Sesión de SMB sin extensiones de seguridad** o **Ataque de exploración de puertos TCP**.
3.Seleccione **En** del menú desplegable de dirección en caso de que se trate de una comunicación entrante.
4.Configure el menú desplegable de la opción **Notificar** en **No**.
5.Configure el menú desplegable de la opción **Registrar** en **Sí**.
6.Deje la opción **Aplicación** en blanco.
7.Si la comunicación no procede de una dirección IP específica, deje la opción **Direcciones IP remotas** en blanco.
8.Haga clic en **Aceptar** para guardar esta notificación.

Protección contra ataques de fuerza bruta

La protección contra ataques por fuerza bruta bloquea los ataques de adivinar contraseñas para los servicios RDP y SMB. Un ataque por fuerza bruta es un método para descubrir una contraseña de destino intentando de forma sistemática todas las letras, números y símbolos que se pueden intentar de forma sistemática. Para configurar la protección contra ataques por fuerza bruta, abra Configuración avanzada > **Protecciones** > **Protección de acceso a la red** > **Protección contra ataques a la red** > **Protección contra ataques por fuerza bruta**.

Activar la protección contra ataques por fuerza bruta: ESET Security Ultimate inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas.

Reglas: le 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 por fuerza bruta le permiten crear, modificar y ver reglas para las conexiones de red entrantes y salientes. Las reglas predefinidas no se pueden editar ni eliminar.

Administrar las reglas de protección contra ataques de fuerza bruta

Agregar – crea una regla nueva.

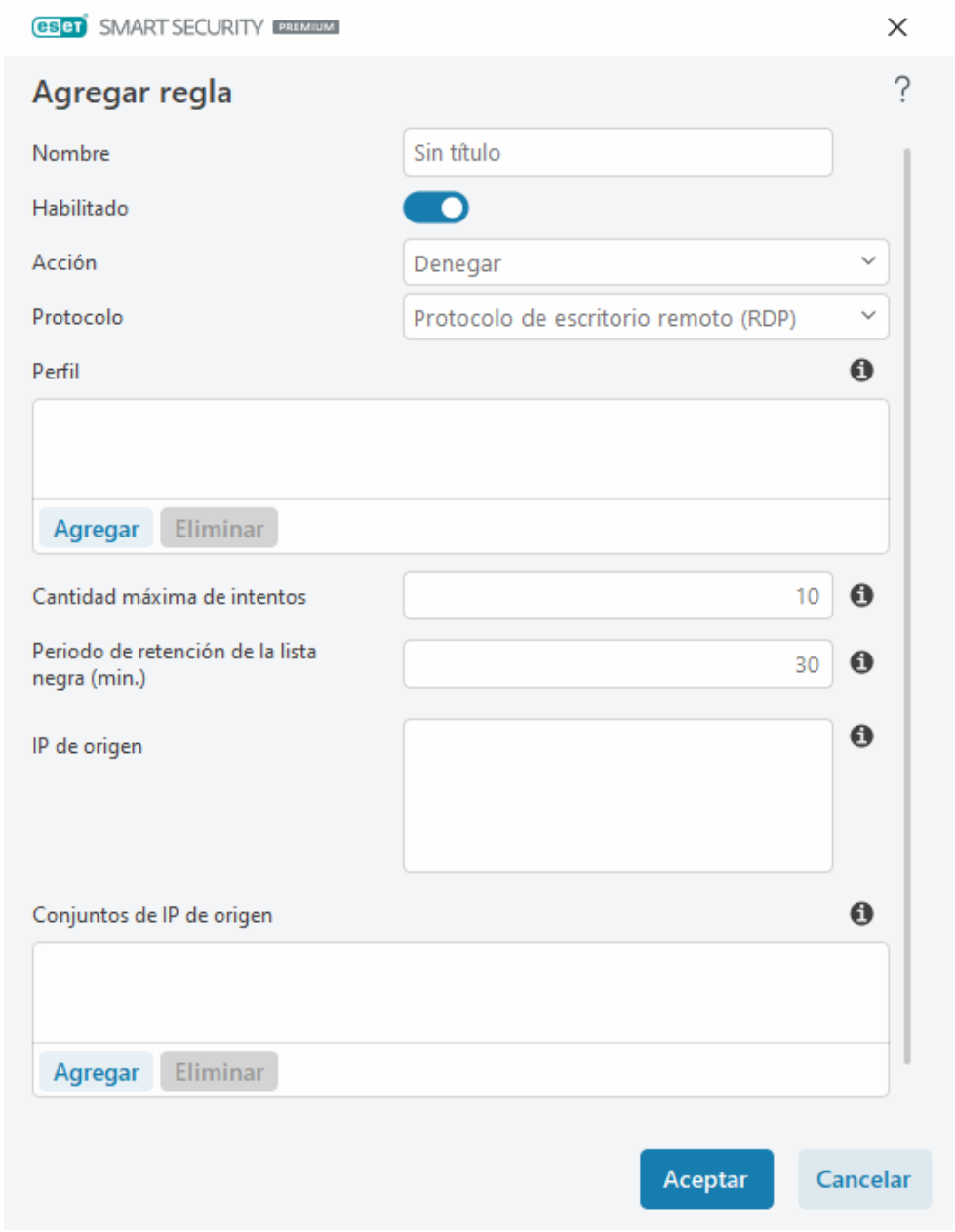
Editar – Edita una regla existente.

Eliminar: elimina una regla existente de la lista de reglas.

Superior/Arriba/Abajo/Inferior: permite ajustar el nivel de prioridad de las reglas.

> Para garantizar la máxima protección posible, se aplica la regla de bloqueo con el valor de **Cantidad máxima de intentos** más bajo, aun si la regla se encuentra en una posición más baja en la lista de Reglas cuando varias reglas de bloqueo cumplen las condiciones de detección.

Editor de reglas



Nombre: nombre de la regla.

Habilitada: deshabilite el interruptor si desea conservar la regla en la lista pero no quiere aplicarla.

Acción: elija si desea **denegar** o **permitir** la conexión si se cumple la configuración de la regla.

Protocolo: el protocolo de comunicación que inspeccionará esta regla.

Perfil: se pueden definir y aplicar reglas personalizadas para perfiles específicos.

Cantidad máxima de intentos - La cantidad máxima de intentos permitidos de repetición de ataques 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 en el cual la dirección caduca de la lista negra.

IP de origen: una lista de subredes, rangos o direcciones IP. Si incluye varias direcciones, deben estar separadas por una coma.

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 ataques a la red** > **Opciones avanzadas**, puede habilitar o deshabilitar la detección de varios tipos de ataques y vulnerabilidades que pueden dañar su equipo.

En algunos casos no recibirá una notificación de amenaza sobre las comunicaciones bloqueadas. Consulte la sección Registrar y crear reglas o excepciones desde el registro para obtener instrucciones para ver todas las comunicaciones bloqueadas en el registro del Firewall.

La disponibilidad de las opciones determinadas en esta ventana pueden variar dependiendo del tipo o versión de su producto de ESET y el módulo de firewall, como así también de la versión de su sistema operativo.

Detección de intrusiones

Detección de intrusiones supervisa la comunicación de los dispositivos en la red para detectar actividad maliciosa.

- **Protocolo SMB** – detecta y bloquea distintos problemas de seguridad en el protocolo SMB.
- **Protocolo RPC** – detecta y bloquea distintos CVE en el sistema remoto de llamadas de procedimientos desarrollado para el Entorno de Computación Distribuida (DCE).
- **Protocolo RDP** – detecta y bloquea varios CVE en el protocolo RDP (consulte arriba).
- **ARP Detección de ataques por envenenamiento:** detección de ARP los ataques por envenenamiento iniciados por ataques de intermediario o detección de un examen del conmutador de red. La aplicación o el dispositivo de red utilizan 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 exploración de puerto; una aplicación diseñada para sondear puertos abiertos de un host enviando solicitudes de cliente a un rango de direcciones de puerto, con el objetivo de encontrar puertos activos y explotar la vulnerabilidad del servicio. Lea más información sobre este tipo de ataque en el glosario.
- **Bloquear la dirección no segura una vez detectado el ataque** – las direcciones IP detectadas como fuentes de ataques se agregan a la Lista negra para prevenir la conexión durante un cierto periodo. Puede definir el **período de retención de la lista negra**, que establece el tiempo durante el cual se bloqueará la dirección después de la detección del ataque.
- **Notificar sobre la detección de ataques** – activa el área de notificación de Windows en la esquina inferior derecha de la pantalla.
- **Mostrar notificaciones también para ataques entrantes frente a agujeros de seguridad** – le proporciona alertas si se detectan ataques frente a agujeros de seguridad, o si una amenaza intenta ingresar al sistema de esta forma.

Inspección de paquetes

Tipo de análisis de paquete que filtra los datos que se transfieren a través de la red.

- **Permitir una conexión entrante para intercambios admin. en el protocolo de SMB**: los intercambios

administrativos (intercambios admin.) son los intercambios de red predeterminados que intercambian particiones del disco rígido (*C$*, *D$*, ...) en el sistema junto con la carpeta del sistema (*ADMIN$*). Deshabilitar la conexión a intercambios de admin. debería mitigar cualquier riesgo de seguridad. Por ejemplo, el gusano Conficker realiza ataques por diccionario para conectarse a intercambios de admin.

- **Denegar dialectos SMB anteriores (no compatibles)** – Denegar sesiones SMB que usan un dialecto SMB anterior que no es compatible con IDS. Los sistemas operativos modernos de Windows son compatibles con los dialectos SMB anteriores debido a la compatibilidad con versiones anteriores con los sistemas operativos anteriores, como Windows 95. El atacante puede usar un dialecto anterior en una sesión SMB para evadir la inspección de tráfico. Denegar dialectos SMB anteriores si su equipo no necesita intercambiar archivos (o usar la comunicación SMB en general) con un equipo que posee una versión anterior de Windows.

- **Denegar sesiones SMB sin extensiones de seguridad** – se puede utilizar la seguridad extendida durante la negociación de la sesión SMB para proporcionar un mecanismo de autenticación más seguro que la autenticación Desafío/respuesta del administrador LAN (LM). El esquema LM es considerado débil y no se recomienda su uso.

- **Denegar la abertura de archivos ejecutables en un servidor fuera de la Zona de confianza en el protocolo de SMB** – anula la conexión cuando intenta ejecutar un archivo ejecutable (.exe,.dll,...) desde una carpeta compartida en el servidor que no pertenece a la zona de confianza en el firewall. Tenga en cuenta que puede ser legítimo copiar archivos ejecutables desde orígenes de confianza. Tenga en cuenta que la copia de archivos ejecutables desde fuentes de confianza puede ser legítima. Sin embargo, esta detección debería mitigar los riesgos de la abertura no deseada de un archivo en un servidor malicioso (por ejemplo, un archivo abierto mediante un clic en un hipervínculo a un archivo ejecutable malicioso compartido).

- **Denegar** la autenticación de **NTLM en el protocolo SMB para conectarse a un servidor dentro o fuera de la Zona de confianza** – Los protocolos que usan esquemas de autenticación de NTLM (ambas versiones) están sujetos a un ataque por reenvío de credenciales (conocido como ataque de Retransmisiones SMB en el caso de un protocolo SMB). Denegar la autenticación de NTLM con un servidor fuera de la Zona de confianza debería mitigar los riesgos del reenvío de credenciales por parte de un servidor malicioso fuera de la Zona de confianza. De modo similar, puede denegar la autenticación de NTLM con servidores en la Zona de confianza.

- **Permitir la comunicación con el servicio Security Account Manager** – para obtener más información acerca de este servicio, consulte [MS-SAMR].

- **Permitir la comunicación con el servicio Local Security Authority** – para obtener más información acerca de este servicio, consulte [MS-LSAD] y [MS-LSAT].

- **Permitir la comunicación con el servicio Remote Registry** – para obtener más información acerca de este servicio, consulte [MS-RRP].

- **Permitir la comunicación con el servicio Service Control Manager** – para obtener más información acerca de este servicio, consulte [MS-SCMR].

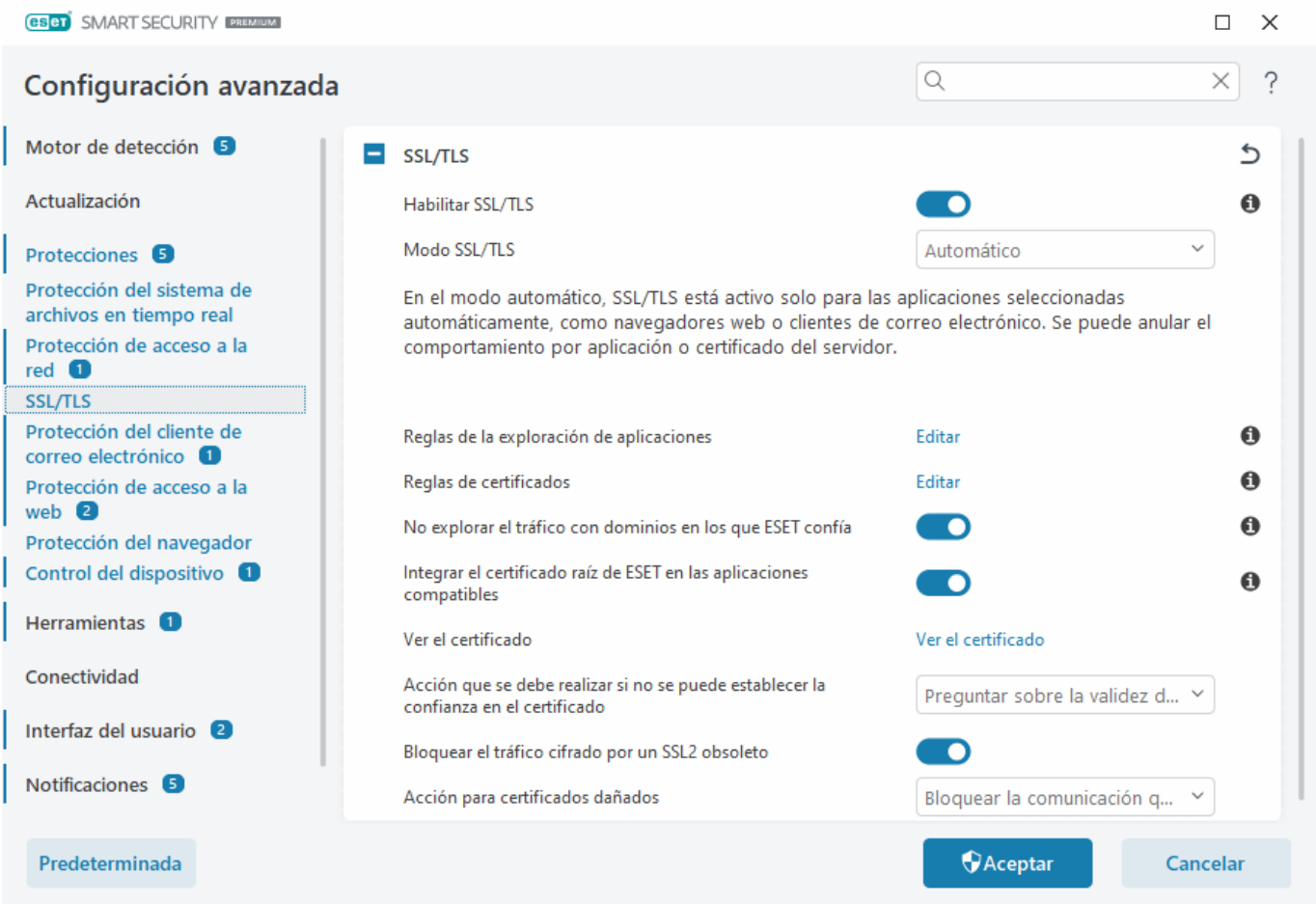
- **Permitir la comunicación con el servicio Server** – para obtener más información acerca de este servicio, consulte [MS-SRVS].

- **Permitir la comunicación con los otros servicios** – otros servicios MSRPC. MSRPC es la implementación de Microsoft del mecanismo DCE RPC. Además, MSRPC puede usar tuberías denominadas dentro del protocolo SMB (compartir archivo de red) para su transporte (transporte ncacn-np). Los servicios MSRPC proporcionan interfaces para el acceso y administración de los sistemas de Windows de modo remoto. Se han descubierto y explotado varias vulnerabilidades de seguridad bajo condiciones normales de operación en el sistema MSRPC

de Windows (gusano Conficker, gusano Sasser...). Deshabilite la comunicación con los servicios MSRPC que no necesite proporcionar para mitigar muchos riesgos de seguridad (como la ejecución remota de códigos o ataques por fallas del servicio).

SSL/TLS

ESET Security Ultimate puede comprobar si hay amenazas de comunicación que utilizan el protocolo SSL. Puede usar varios modos de filtrado para examinar las comunicaciones protegidas por SSL mediante certificados de confianza, certificados desconocidos o certificados excluidos de la verificación de las comunicaciones protegidas por SSL. Para editar la configuración de SSL/TLS, abra **Configuración avanzada** > **Protecciones** > SSL/TLS.



Habilitar SSL/TLS: si está desactivado, ESET Security Ultimate no explorará la comunicación a través de SSL/TLS.

el modo SSL/TLS está disponible en las siguientes opciones:

Modo de filtrado	Descripción
Automático	El modo predeterminado solo explorará las aplicaciones correspondientes, como los navegadores web y los clientes de correo electrónico. Seleccione las aplicaciones donde se explora la comunicación para anularlo.
Interactivo	Si ingresa un nuevo sitio protegido por SSL (con un certificado desconocido), se mostrará un cuadro de diálogo para la selección de acción. Este modo le permite crear una lista de certificados/aplicaciones SSL que se excluirán de la exploración.

Modo de filtrado	Descripción
Basado en políticas	Seleccione esta opción para explorar todas las comunicaciones protegidas por SSL excepto las protegidas por certificados excluidos de la verificación. Si se establece una nueva comunicación que use un certificado firmado desconocido, no se notificará al usuario y se filtrará la comunicación en forma automática. Al acceder a un servidor con un certificado no confiable que está 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 exploración de aplicaciones: le permite personalizar el comportamiento de ESET Security Ultimate de aplicaciones específicas.

Reglas de certificados: le permite personalizar el comportamiento de ESET Security Ultimate de certificados SSL específicos.

No explorar el tráfico con dominios en los que ESET confía: cuando esté habilitada esta opción, la comunicación con dominios de confianza se excluirá de la exploración. Una lista blanca integrada administrada por ESET determina la confiabilidad de un dominio.

Integrar el certificado raíz de ESET en las aplicaciones compatibles – para que la comunicación SSL funcione correctamente en los navegadores o clientes de correo electrónico, es imprescindible agregar el certificado raíz para ESET a la lista de certificados raíz conocidos (desarrolladores). Cuando está habilitado, ESET Security Ultimate agrega automáticamente el certificado ESET SSL Filter CA a los navegadores conocidos (por ejemplo, Opera). Para los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática. Por ejemplo, Firefox se configura de manera automática para confiar en las autoridades raíz en la tienda de certificados del sistema.

Para aplicar el certificado en navegadores no compatibles, haga clic en **Ver el certificado** > **Detalles** > **Copiar en el archivo** y luego impórtelo manualmente al navegador.

Acción que se debe realizar 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 Autoridades de Certificación de Raíz de Confianza (TRCA), (por ejemplo, certificado caducado, certificado que no es de confianza, certificado no válido para el dominio específico o la firma que se puede analizar pero no firma el certificado correctamente). Los sitios web legítimos siempre utilizarán certificados de confianza. Si no lo proporcionan, podría significar que un atacante está descifrando su comunicación o que el sitio web está experimentando dificultades técnicas.

Si se selecciona **Preguntar sobre la validez del certificado** (predeterminado), se le solicitará que seleccione la acción a realizar cuando se establezca una comunicación cifrada. Se mostrará un cuadro de diálogo para la selección de la acción donde puede marcarlo como certificado de confianza o certificado excluido. En caso de que el certificado no esté presente en la lista de TRCA, la ventana es de color rojo. Si el certificado figura en la lista de TRCA, la ventana será de color verde.

Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para que siempre se finalicen las conexiones cifradas a un sitio que use el certificado no confiable.

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 significa que el certificado utiliza un formato no reconocido por ESET Security Ultimate o que se ha recibido dañado (por ejemplo, sobrescrito por datos

aleatorios). En este caso, se recomienda dejar seleccionada la opción **Bloquear comunicaciones que usan el certificado**. Si se selecciona **Preguntar sobre la validez del certificado**, se solicita al usuario que elija una acción cuando se establezca la comunicación cifrada.

> **Ejemplos ilustrados**
> Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:
> - Notificaciones de certificados en productos hogareños de ESET Windows
> - Se muestra el mensaje "Tráfico de red cifrado: Certificado no confiable" al visitar las páginas web

Reglas de la exploración de aplicaciones

Las **reglas de exploración de aplicaciones** se puede usar para personalizar la conducta de ESET Security Ultimate para aplicaciones específicas y 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 la exploración de aplicaciones** > **Editar**.

La ventana **Reglas de exploración de aplicaciones** consta de:

Columnas

Aplicación – elija un archivo ejecutable desde el árbol del directorio, haga clic en la opción **...** e ingrese la ruta en forma manual.

Acción de exploración – seleccione **Explorar** o **Ignorar** para explorar o ignorar la comunicación. Seleccione **Auto** para explorar en el modo automático y preguntar en el modo interactivo. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Elementos de control

Agregar– agregar la aplicación filtrada.

Editar: seleccione la aplicación que desea configurar y haga clic en **Editar**.

Quitar: seleccione la aplicación que desea quitar y haga clic en **Quitar**.

Importar/**Exportar**: importe aplicaciones desde un archivo o guarde la lista actual de aplicaciones en un archivo.

Aceptar/**Cancelar** – haga clic en **Aceptar** si desea guardar los cambios o en **Cancelar** si desea salir sin guardar.

Reglas de certificados

Las reglas del certificado se pueden usar para personalizar el comportamiento de ESET Security Ultimate de 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 certificado** consta de:

Columnas

Nombre– nombre del certificado.

Emisor del certificado– nombre del creador del certificado.

Sujeto del certificado– el campo del sujeto identifica la entidad asociada con la clave pública almacenada en el campo de la clave pública del sujeto.

Acceso– seleccione **Permitir** o **Bloquear** como la **Acción de acceso** para permitir o bloquear la comunicación asegurada por este certificado, independientemente de su confianza. Seleccione **Auto** para permitir certificados de confianza y solicitar los que no son de confianza. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Explorar– seleccione **Explorar** o **Ignorar** como la **Acción de exploración** para explorar o ignorar la comunicación asegurada por este certificado. Seleccione **Auto** para explorar en el modo automático y preguntar en el modo interactivo. Seleccione **Preguntar** para preguntarle siempre al usuario qué hacer.

Elementos de control

Agregar – agregar un nuevo certificado y ajustar su configuración con respecto al acceso y a las opciones de exploración.

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** si desea guardar los cambios o en **Cancelar** si desea salir sin guardar.

Tráfico de red cifrada

Si su sistema está configurado para usar una exploración SSL/TLS, se mostrará una ventana de diálogo para elegir una acción en dos situaciones distintas:

Primero, si un sitio web usa un certificado no válido o que no se puede verificar, y ESET Security Ultimate está configurado para preguntarle al usuario en dichos casos (de forma predeterminada, "sí" para los certificados que no se pueden verificar; "no" para los que no son válidos), un cuadro de diálogo le preguntará si desea **Permitir** o **Bloquear** la conexión. Si el certificado no está ubicado en Trusted Root Certification Authorities store (TRCA), se considera no confiable.

Segundo, si el modo **SSL/TLS** está configurado en **Modo interactivo**, un cuadro de diálogo para cada sitio web le preguntará si desea **Explorar** o **Ignorar** el tráfico. Algunas aplicaciones verifican que su tráfico SSL no esté modificado ni inspeccionado por nadie; en dichos casos, ESET Security Ultimate debe **Ignorar** dicho tráfico para que la aplicación siga funcionando.

> **Ejemplos ilustrados**
> Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:
> - Notificaciones de certificados en productos hogareños de ESET Windows
> - Se muestra el mensaje "Tráfico de red cifrado: Certificado no confiable" al visitar las páginas web

En los dos casos, el usuario puede elegir recordar la acción seleccionada. Las acciones guardadas se almacenan en las reglas de certificado.

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 entre las siguientes opciones de configuración:

- Protección del transporte de correo electrónico
- Protección de la casilla de correo
- Administración de listas de direcciones
- ThreatSense

Protección del transporte de correo electrónico

IMAP(S) y POP3(S) son los protocolos de uso más generales para recibir comunicaciones de correo electrónico en una aplicación de cliente de correo electrónico. El protocolo de acceso a mensajes de Internet (IMAP, 'Internet Message Access Protocol') es otro protocolo de Internet para la recuperación del correo electrónico. El protocolo IMAP tiene algunas ventajas sobre POP3, por ejemplo, se pueden conectar simultáneamente varios clientes al mismo buzón de correo y mantener información del estado de los mensajes: si se leyó, respondió o eliminó el mensaje, etc. El módulo de protección que proporciona este control se ejecuta automáticamente cuando se inicia el sistema y queda activo en la memoria.

ESET Security Ultimate proporciona protección para estos protocolos, independientemente del cliente de correo electrónico usado, y sin requerir una nueva configuración del cliente de correo electrónico. De manera predeterminada, toda la comunicación mediante los protocolos POP3 y IMAP se explora, sin tener en cuenta los números de puerto POP3/IMAP predeterminados.
El protocolo MAPI no se explora. Sin embargo, la comunicación con el servidor Microsoft Exchange puede explorarse mediante el módulo de integración en clientes de correo electrónico, como Microsoft Outlook.

ESET Security Ultimate también admite la exploración de los protocolos IMAPS (585, 993) y POP3S (995), que usan un canal cifrado para transferir información entre el servidor y el cliente. ESET Security Ultimate verifica la comunicación mediante el SSL (protocolo de capa de conexión segura) y la TLS (seguridad de la capa de transporte).
La comunicación cifrada se explorará de forma predeterminada. Para ver la configuración del explorador, abra Configuración avanzada > **Protecciones** > SSL/TLS.

Para configurar la Protección del transporte de correo electrónico, abra Configuración avanzada > **Protecciones** > **protección del cliente de correo electrónico** > **protección del transporte de correo electrónico**.

Habilitar Protección del transporte de correo electrónico: cuando está activada, la comunicación del transporte de correo electrónico se explorará mediante ESET Security Ultimate.

Puede elegir qué protocolos de transporte de correo se explorarán con un clic en el interruptor situado junto a las siguientes opciones (de forma predeterminada, está habilitada la exploración de todos los protocolos):

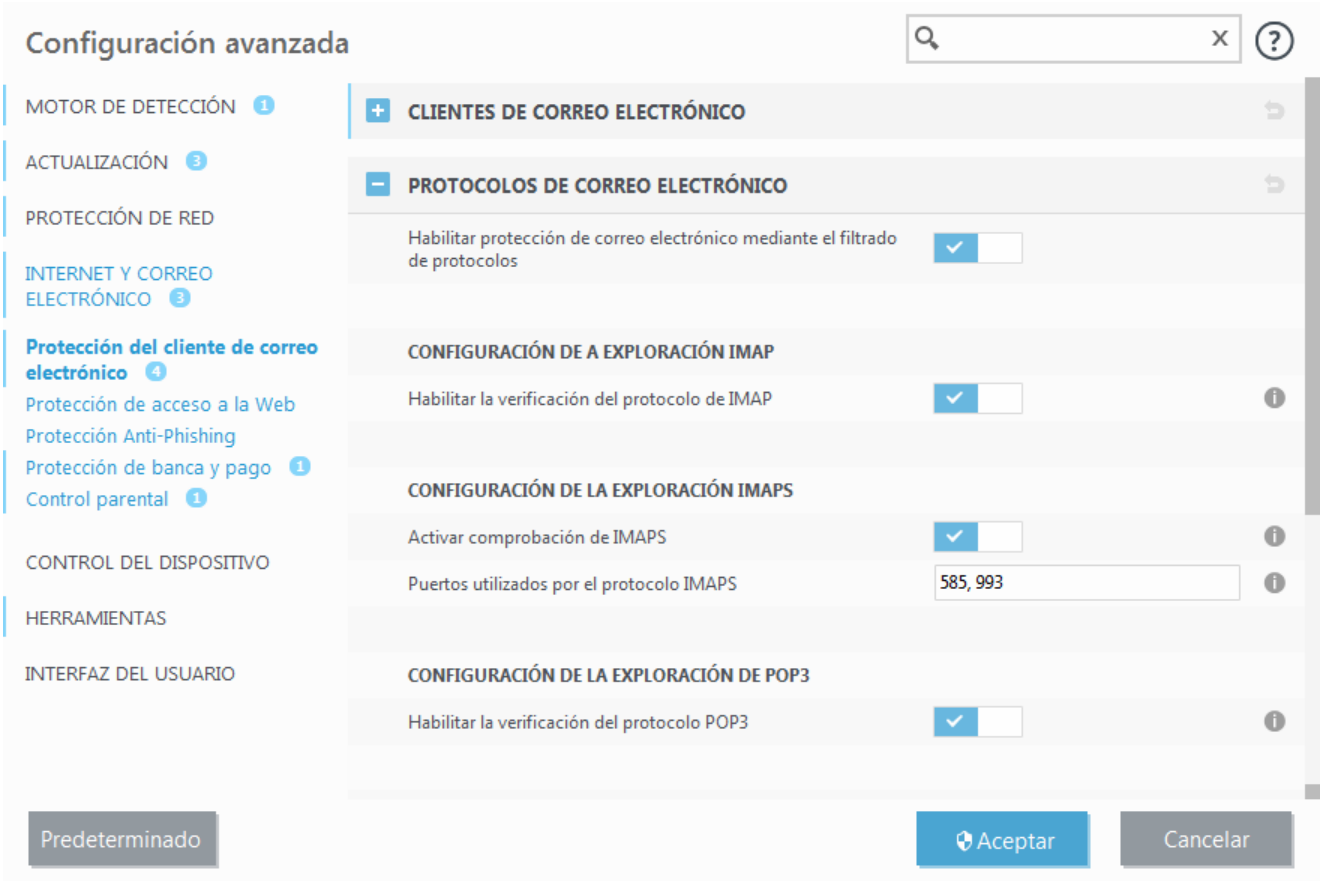
- **Explorar transporte de correo IMAP**

- **Explorar transporte de correo IMAPS**
- **Explorar transporte de correo POP3**
- **Explorar transporte de correo POP3S**

De forma predeterminada, ESET Security Ultimate explorará 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 los **Puertos utilizados por el protocolo IMAPS** o **Puertos utilizados por el protocolo POP3S**. Los números de puerto múltiples deben delimitarse con una coma.

Aplicaciones excluidas: permite excluir aplicaciones específicas de la protección del transporte de correo electrónico. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.

IP excluidas: permite excluir direcciones remotas específicas de la exploración de la protección del transporte de correo electrónico. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.



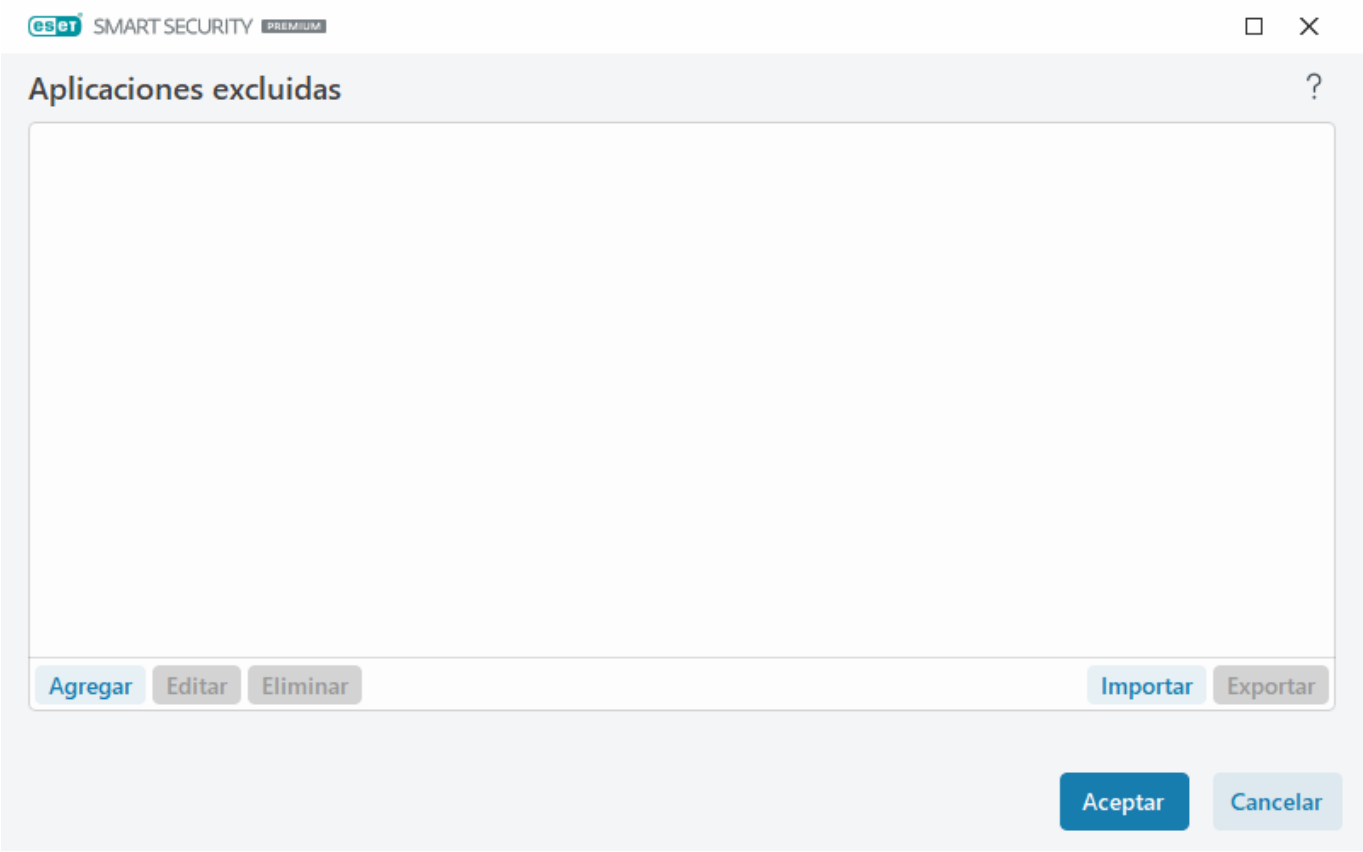
Aplicaciones excluidas

Para excluir la exploración de la comunicación para aplicaciones específicas, agréguelas a la lista. La comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable usar esta opción solamente para las aplicaciones que no funcionen correctamente cuando se explora su comunicación.

Las aplicaciones y los servicios activos se mostrarán automáticamente en esta ventana al hacer clic en **Agregar**. Haga clic en **...** y navegue hasta una aplicación para agregar la exclusión manualmente.

Editar – edite las entradas seleccionadas de la lista.

Quitar – elimine las entradas seleccionadas de la lista.



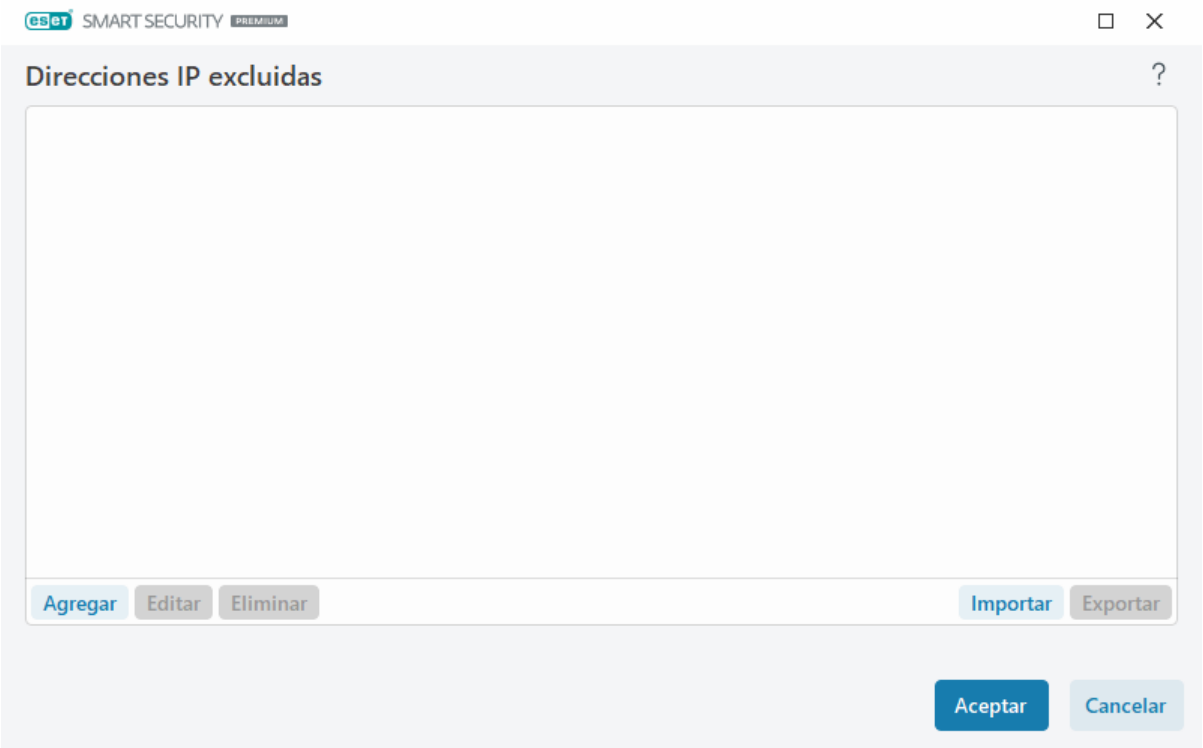
IP excluidas

Las entradas de la lista quedarán excluidas de la exploración. La comunicación HTTP(S)/POP3(S)/IMAP(S) desde o hacia las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable que únicamente use esta opción para direcciones confiables conocidas.

Haga clic en **Agregar** para agregar 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 **Quitar** para eliminar las entradas seleccionadas de la lista.



Ejemplos de direcciones IP

Agregar dirección IPv4:
Dirección única: agrega una dirección IP de un equipo individual (por ejemplo, *192.168.0.10*).
Rango de direcciones: escriba la primera y la última dirección IP para especificar el rango de IP de varios equipos (por ejemplo, *192.168.0.1 a 192.168.0.99*).
Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red para 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 equipo individual (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

Protección de la casilla de correo

La integración de ESET Security Ultimate con su buzón de correo aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico.

Para configurar la protección del buzón de correo, abra **Configuración avanzada** > Protecciones > **Protección del cliente de correo electrónico** > **Protección del buzón**.

Habilitar protección de correo electrónico mediante complementos de clientes: cuando esté deshabilitada, la protección mediante complementos de cliente de correo electrónico estará apagada.

Seleccione los correos electrónicos que desea analizar:

- **Correo electrónico recibido**
- **Correo electrónico enviado**

- **Correo electrónico leído**
- **Correo electrónico modificado**

Recomendamos mantener **Habilitar protección de correo electrónico mediante complementos de clientes** habilitado. Incluso si la integración no está habilitada o no es funcional, la comunicación por correo electrónico todavía está protegida por la Protección del transporte de correo electrónico (IMAP/IMAPS y POP3/POP3S).

Explorar en busca de spam

El correo electrónico no solicitado, denominado spam, es uno de los problemas más importantes de la comunicación electrónica. El spam representa hasta 30% de todas las comunicaciones por correo electrónico. El antispam del cliente de correo electrónico sirve para proteger contra este problema. Mediante la combinación de varios principios de seguridad del correo electrónico, el antispam del cliente de correo electrónico proporciona un filtrado superior para mantener limpio su buzón de entrada. En el caso de la detección de spam, un principio importante es reconocer correos electrónicos no solicitados a partir de direcciones de confianza predefinidas (permitidas) y direcciones de correo no deseado (bloqueadas).

El método principal utilizado para detectar spam es la exploración de las propiedades de los mensajes de correo electrónico. Los mensajes recibidos se exploran en búsqueda de los criterios antispam básicos (definiciones de mensajes, heurísticas estadísticas, reconocimiento de algoritmos y otros métodos exclusivos) y el valor de índice resultante determina si el mensaje es spam o no.

Habilitar Antispam del cliente de correo electrónico: cuando está habilitado, los mensajes recibidos se analizarán en busca de spam.

Usar explorador avanzado de spam: periódicamente se descargarán datos antispam adicionales, lo que aumentará las capacidades antispam y producirá mejores resultados.

Registro del puntaje de spam – El motor antispam de ESET Security Ultimate le asigna un puntaje de spam a cada mensaje explorado. El mensaje se guardará en el registro de protección antispam (ventana principal del programa > **Herramientas** > **Archivos de registro** > **Antispam del cliente de correo electrónico**).

- **Ninguno** – el puntaje de la exploración antispam no se registrará.
- **Reclasificado y marcado como spam** – seleccione esta opción si desea registrar un puntaje de spam para los mensajes marcados como SPAM.
- **Todos** – se guardarán en el registro todos los mensajes con su puntaje de spam.

Cuando hace clic en un mensaje de la carpeta de correo electrónico no deseado, puede elegir **Reclasificar los mensajes seleccionados como NO ES spam**, y el mensaje se enviará al buzón de entrada. Cuando hace clic en un mensaje del buzón de entrada que considera como spam, seleccione **Reclasificar los mensajes como spam**, y el mensaje se enviará a la carpeta de correo electrónico no deseado. Puede seleccionar varios mensajes y actuar en todos ellos simultáneamente.

Optimización de la gestión de adjuntos: si la optimización está deshabilitada, todos los archivos adjuntos se

exploran inmediatamente. Es posible que experimente una ralentización del rendimiento del cliente de correo electrónico.

Integraciones: le permite integrar la protección del buzón de correo en su 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 Security Ultimate con su cliente de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, puede habilitar la integración en ESET Security Ultimate. Cuando se integra a su cliente de correo electrónico, la barra de herramientas de ESET Security Ultimate se inserta directamente en el cliente de correo electrónico, lo que permite una protección de correo electrónico más eficaz. 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 – Microsoft Outlook es actualmente el único cliente de correo electrónico compatible. La protección de correo electrónico funciona como un complemento. La ventaja principal de este complemento es su independencia respecto al protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, se descifra y se envía al módulo de exploración de virus. Consulte este artículo de la base de conocimiento de ESET para ver una lista completa de las versiones compatibles de Microsoft Outlook.

Procesamiento avanzado del cliente de correo electrónico: procesa eventos extra Outlook Messaging API (MAPI)***: Objeto modificado (`fnevObjectModified`) y objeto creado (`fnevObjectCreated`). Si experimenta lentitud en el sistema al trabajar con su cliente de correo electrónico, habilite esta opción.

Barra de herramientas de Microsoft Outlook

La protección de Microsoft Outlook funciona como un módulo de complemento. Después de instalar ESET Security Ultimate, esta barra de herramientas que contiene las opciones de protección antivirus y antispam del cliente de correo electrónico se agrega a Microsoft Outlook:

Spam – marca los mensajes seleccionados como spam. Después de marcarlos, se envía una “huella digital” del mensaje a un servidor central que almacena las firmas de spam. Si el servidor recibe más “huellas digitales” similares de varios usuarios, el mensaje se clasificará como spam en el futuro.

No es spam – marca los mensajes seleccionados como correo deseado.

Direcciones de spam (bloqueadas, una 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 clasificarán automáticamente como spam.

> ⚠ Tenga cuidado con la suplantación o falsificación de la dirección del remitente en mensajes de correo electrónico, utilizada para engañar a los destinatarios con el objetivo de que lean los correos y los respondan.

Dirección de confianza (permitida, una lista de direcciones de confianza) – agrega una nueva dirección de

remitente a la lista de direcciones como permitida. Todos los mensajes recibidos de direcciones permitidas no se clasificarán nunca como spam de forma automática.

ESET Security Ultimate: haga doble clic en el ícono para abrir la ventana principal de ESET Security Ultimate.

Volver a explorar los mensajes – permite iniciar la verificación del correo electrónico en forma manual. Puede especificar los mensajes que se van a verificar así como activar la exploración repetida de los correos electrónicos recibidos. Para obtener más información, consulte Protección del buzón de correo.

Configuración del explorador: muestra las opciones de configuración de la Protección del buzón de correo.

Configuración del Antispam: muestra las opciones de configuración de la Protección del buzón de correo.

Libretas de direcciones: abra la ventana Administración de listas de direcciones, desde donde puede acceder a las listas de direcciones excluidas, de confianza y de spam.

Cuadro de diálogo de confirmación

Esta notificación sirve para corroborar que el usuario realmente desee realizar la acción seleccionada, para eliminar posibles errores.

Por otro lado, el cuadro de diálogo también ofrece la opción de deshabilitar las confirmaciones.

Volver a explorar los mensajes

La barra de herramientas de ESET Security Ultimate, integrada en los clientes de correo electrónico, les permite a los usuarios especificar varias opciones de verificación del correo electrónico. La opción **Volver a explorar los mensajes** ofrece dos modos de exploración:

Todos los mensajes de la carpeta actual – explora los mensajes en la carpeta actualmente abierta.

Solo los mensajes seleccionados – explora únicamente los mensajes marcados por el usuario.

La casilla de verificación **Volver a explorar los mensajes ya explorados** le proporciona al usuario la opción de realizar otra exploración en los mensajes que ya se habían explorado antes.

Respuesta

Según los resultados de la exploración de mensajes, ESET Security Ultimate puede mover los mensajes explorados o agregar texto personalizado al asunto. Puede configurar estas opciones en Configuración avanzada > **Protecciones** > del **cliente de correo electrónico** > **Protección del buzón de correo electrónico** > **Respuesta**.

El antispam del cliente de correo electrónico en ESET Security Ultimate le permite configurar los siguientes parámetros para los mensajes:

Agregar texto al tema del correo electrónico – permite agregar una cadena de texto personalizada como prefijo a la línea del asunto de los mensajes clasificados como spam. El **texto** predeterminado es "[SPAM]".

Mover la carpeta de spam – cuando esta opción está habilitada, los mensajes de spam se enviarán a la carpeta

predeterminada de correo electrónico no deseado, y los mensajes reclasificados como “no es” spam se enviarán al buzón de entrada. Cuando hace clic derecho en un mensaje de correo electrónico y selecciona ESET Security Ultimate en el menú contextual, puede elegir las opciones que se aplicarán.

Mover a una carpeta personalizada: cuando esta opción esté habilitada, los mensajes de spam se moverán a una carpeta especificada a continuación.

Carpeta – especificar la carpeta personalizada donde desea mover los correos electrónicos infectados al detectarlos.

Si hay un mensaje que contiene detección, de forma predeterminada, ESET Security Ultimate intenta aclarar el mensaje. Si el mensaje no se puede aclarar, puede elegir una **Acción a realizar si la limpieza no es posible**:

- **Sin acción** – si se habilita esta opción, el programa identificará los archivos adjuntos infectados, pero dejará intactos los correos electrónicos, sin realizar acción alguna.

- **Eliminar correo electrónico** – el programa notificará al usuario sobre las infiltraciones y eliminará el mensaje.

- **Mover el correo electrónico a la carpeta de elementos eliminados** – los correos electrónicos infectados se enviarán automáticamente a la carpeta de elementos eliminados.

- **Mover el correo electrónico a la carpeta** (acción predeterminada): los correos electrónicos infectados se enviarán automáticamente a la carpeta especificada.

Carpeta – especificar la carpeta personalizada donde desea mover los correos electrónicos infectados al detectarlos.

Marcar los mensajes de spam como leídos – habilítela para marcar automáticamente los mensajes de spam como leídos. Resulta útil para centrar su atención en los mensajes “no infectados”.

Marcar los mensajes reclasificados como no leídos – los mensajes originalmente clasificados como spam que luego se cambiaron a “no infectados” se mostrarán como no leídos.

Luego de verificar el correo electrónico, se puede añadir al mensaje una notificación con el resultado de la exploración. Puede elegir **Añadir mensajes de etiqueta a los correos electrónicos recibidos y leídos** o **Añadir mensajes de etiqueta a los correos electrónicos enviados**. Tenga en cuenta que, en ocasiones raras, los mensajes de etiqueta pueden omitirse en mensajes HTML problemáticos o si los mensajes están adulterados por malware. Los mensajes de etiqueta se pueden añadir a los correos electrónicos recibidos y leídos, enviados o a ambas categorías. Se encuentran disponibles las siguientes opciones:

- **Nunca**: no se agregan mensajes de etiqueta.

- **Cuando ocurre una detección**: únicamente se marcarán como verificados los mensajes que contengan software malicioso (predeterminado).

- **A todos los correos electrónicos explorados**: el programa añadirá mensajes a todos los correos electrónicos explorados.

Actualizar el asunto de los correos electrónicos recibidos leídos / **Actualizar asunto del correo electrónico**: habilite esta opción para agregar al mensaje texto personalizado especificado a continuación.

Texto para agregar en el asunto del correo electrónico detectado: si desea modificar el formato del prefijo en el

asunto de un correo electrónico infectado, edite esta plantilla. Esta función reemplazará el asunto del mensaje «Hola» por el siguiente formato: «[detección %NOMBRE DE DETECCIÓN%] Hola». La variable %DETECTIONNAME% representa la amenaza detectada.

Administración de listas de direcciones

La característica Antispam del cliente de correo electrónico de ESET Security Ultimate permite configurar varios parámetros para las listas de direcciones. Para configurar listas de direcciones, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Administración de listas de direcciones**.

Activar la lista de direcciones del usuario: active esta opción para activar la lista de direcciones del usuario.

Lista de direcciones del usuario: lista de direcciones de correo electrónico donde puede agregar, editar o eliminar direcciones para definir las reglas antispam. Las reglas de esta lista se aplicarán al usuario actual.

Permitir las listas globales de direcciones: habilite esta opción para activar la lista global de direcciones compartida por todos los usuarios en este dispositivo.

Lista global de direcciones: lista de direcciones de correo electrónico donde puede agregar, editar o eliminar direcciones para definir las reglas antispam. Las reglas de esta lista se aplicarán a todos los usuarios.

Permitir y agregar automáticamente a la lista de direcciones del usuario

Tratar direcciones de la libreta de direcciones como de confianza – Las direcciones de su lista de contactos se tratarán como de confianza sin agregarse a la lista de direcciones del usuario.

Agregar las direcciones de destinatarios desde los mensajes salientes: agregue direcciones de destinatarios desde los mensajes enviados a la lista de direcciones de usuarios como permitidas.

Agregar las direcciones de los mensajes reclasificados como NO ES spam: agregue a la lista de direcciones de usuarios direcciones de remitentes desde mensajes reclasificados como NO ES spam como permitidas.

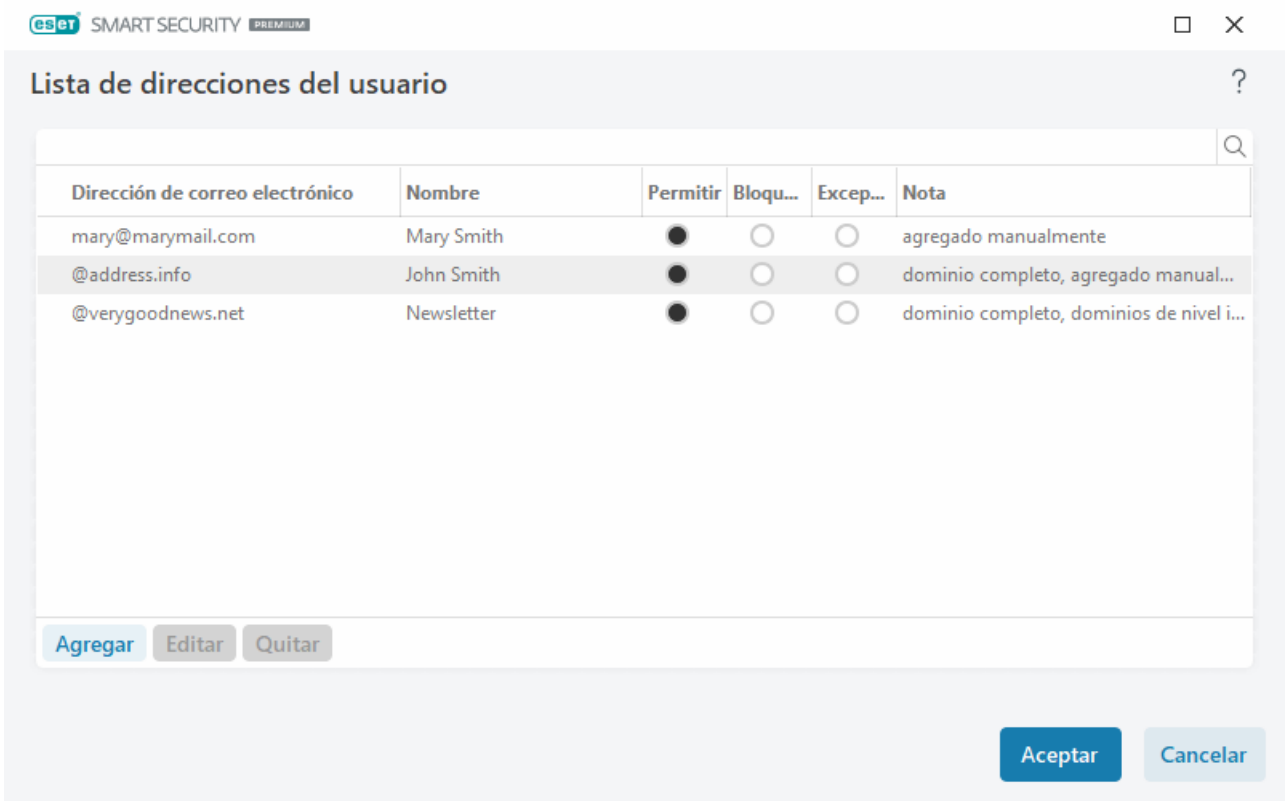
Agregar automáticamente como una excepción a la lista de direcciones del usuario

Agregar direcciones de cuentas propias: agregue sus direcciones desde cuentas existentes del cliente de correo electrónico a la lista de direcciones de usuarios como excepción.

Listas de direcciones

Para protegerse de correos electrónicos no solicitados, ESET Security Ultimate le permite clasificar las direcciones de correo electrónico en listas de direcciones.

Para editar las listas de direcciones, abra Configuración avanzada > **Protecciones** > **Protección del cliente de correo electrónico** > **Administración de listas de direcciones**, y haga clic en **Editar** junto a **Lista de direcciones del usuario** o **Lista global de direcciones**.



Columnas

Dirección de correo electrónico: dirección a la que se aplicará la regla. No se admiten comodines.

Nombre: nombre de la regla personalizada.

Permitir/bloquear/excepción: botones de opción utilizados para determinar la acción que desea realizar para la dirección de correo electrónico (haga clic en el botón de opción de la columna preferida para cambiar rápidamente la acción):

- **Permitir**: direcciones que se consideran seguras y de las que desea recibir mensajes.
- **Bloquear**: direcciones que se consideran no seguras o spam y de las que no desea recibir mensajes.
- **Excepción**: direcciones que siempre se comprueban en busca de spam y que pueden haberse alterado y utilizado para el envío de correo no deseado.

Nota: información sobre cómo se creó la regla y si se aplica a todo el dominio o a los dominios de nivel inferior.

Administración de las direcciones

- **Agregar**: haga clic para agregar una regla para una dirección nueva.
- **Editar**: seleccione y haga clic para editar una regla existente.
- **Quitar**: seleccione y haga clic si desea quitar una regla de la lista de direcciones.

Agregar/editar dirección

Esta ventana le permite agregar o editar una dirección en la administración de la lista de direcciones antispam y configurar la acción realizada:

Dirección de correo electrónico: dirección a la que se aplicará la regla.

Nombre: nombre de la regla personalizada.

Acción: acción que debe realizarse si la dirección de correo electrónico del contacto coincide con la dirección especificada en el campo **Dirección de correo electrónico**:

- **Permitir**: direcciones que se consideran seguras y de las que desea recibir mensajes.
- **Bloquear**: direcciones que se consideran no seguras o spam y de las que no desea recibir mensajes.
- **Excepción**: direcciones que siempre se comprueban en busca de spam y que pueden haberse alterado y utilizado para el envío de correo no deseado.

Dominio completo – seleccione esta opción para aplicar la regla al dominio completo del contacto (no solo a la dirección especificada en el campo **Dirección de correo electrónico**, sino a todas las direcciones del dominio *dirección.info*).

Dominios de nivel inferior – seleccione esta opción para aplicar la regla a los dominios de nivel inferior del contacto (*dirección.info* representa el dominio, mientras que *mi.dirección.info* representa un subdominio).

Resultado del procesamiento de las direcciones

Al agregar nuevas direcciones o cambiar la acción realizada para la dirección de correo electrónico, ESET Security Ultimate muestra mensajes de notificación. El contenido de los mensajes de notificación varía según la acción que está tratando de realizar.

Seleccione la casilla de verificación **No preguntar de nuevo** para realizar la acción automáticamente sin volver a mostrar el mensaje la próxima vez.

ThreatSense

ThreatSense está conformada por muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también brinda protección durante las primeras horas de propagación de una nueva amenaza. Utiliza una combinación de la exploración del código, la emulación del código, las firmas genéricas y las firmas de virus que funcionan conjuntamente para mejorar en forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar simultáneamente varios flujos de datos para maximizar la eficiencia y la tasa de detección. La tecnología de ThreatSense también elimina los rootkits de forma correcta.

Las opciones de configuración del motor ThreatSense le permiten especificar varios parámetros de exploración:

- Los tipos de archivos y las extensiones que se van a explorar

- La combinación de diversos métodos de detección.
- Los niveles de desinfección, etc.

Para ingresar a la ventana de configuración, haga clic en **ThreatSense** ubicado en Configuración avanzada de cualquier módulo que use la tecnología ThreatSense (ver abajo). Diferentes situaciones de seguridad pueden requerir diferentes configuraciones. Por este motivo, ThreatSense puede configurarse en forma individual para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Exploración en estado inactivo
- Exploración en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del acceso a la Web
- Exploración del equipo

Los parámetros de ThreatSense están sumamente optimizados para cada módulo y su modificación puede afectar el funcionamiento del sistema en forma significativa. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, solo los nuevos archivos creados se exploran con estos métodos). En consecuencia, es recomendable mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos excepto para la exploración del equipo.

Objetos para explorar

Esta sección le permite definir qué componentes y archivos del equipo se explorarán en busca de infiltraciones.

Memoria operativa – explora en busca de amenazas que atacan la memoria operativa del sistema.

Sectores de inicio/UEFI: explora los sectores de inicio para detectar la presencia de virus en el Master Boot Record. Lea más sobre UEFI en el glosario.

Archivos de correo electrónico – el programa es compatible con las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos – el programa es compatible con las siguientes extensiones, ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE entre muchas otras.

Archivos de autoextracción: los archivos de autoextracción (SFX) son los archivos que se pueden extraer a sí mismos.

Empaquetadores de tiempo de ejecución: después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el explorador puede reconocer varios tipos de empaquetadores adicionales mediante el uso de la emulación del código.

Opciones de exploración

Seleccione los métodos utilizados al explorar el sistema en busca de infiltraciones. Se encuentran disponibles las siguientes opciones:

Heurística – la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de esta tecnología radica en su capacidad de identificar software malicioso que antes no existía o que no era reconocido por la versión anterior del motor de detección. La desventaja es la probabilidad (muy reducida) de identificar falsos positivos.

Heurística avanzada/Firmas de ADN: la heurística avanzada está compuesta por un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que se crearon con lenguajes de programación de última generación. El uso de la heurística avanzada incrementa significativamente la capacidad de detección de amenazas de los productos de ESET. Las firmas tienen la capacidad de detectar e identificar los virus en forma confiable. Mediante el uso del sistema de actualizaciones automáticas, las nuevas firmas están disponibles en el transcurso de unas pocas horas tras el descubrimiento de una amenaza. La desventaja de las firmas es que solo detectan los virus que ya conocen (o las versiones ligeramente modificadas de estos virus).

Desinfección

La configuración de la desinfección determina el comportamiento de ESET Security Ultimate durante la desinfección de objetos. Existen cuatro niveles de desinfección:

ThreatSense incluye los siguientes niveles de corrección (es decir, desinfección).

Corrección ESET Security Ultimate

Nivel de desinfección	Descripción
Corregir siempre la detección	Intento de corregir la detección al limpiar objetos sin la intervención del usuario final. En algunos pocos casos (por ejemplo, en archivos de sistema), si la detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario conservar	Intento de corregir la detección al desinfectar objetos sin la intervención del usuario final. En algunos casos (por ejemplo, en archivos de sistema con archivos desinfectados o infectados), si una detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario preguntar	Intento de corregir la detección al desinfectar 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). Esta configuración se recomienda en la mayoría de los casos.
Preguntar siempre al usuario final	El usuario final visualiza una ventana interactiva al desinfectar objetos y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de hallar una detección.

Exclusiones

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de ThreatSense permite definir los tipos de archivos que se van a explorar.

Otros

Cuando se configuran los parámetros del motor ThreatSense para una exploración del equipo bajo demanda, las siguientes opciones en la sección **Otros** también están disponibles:

Explorar secuencias de datos alternativas (ADS) – las secuencias de datos alternativas usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección camuflándose como secuencias de datos alternativas.

Realizar exploraciones en segundo plano con baja prioridad – cada secuencia de exploración consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para los recursos del sistema, es posible activar la exploración en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos – El Registro de la exploración mostrará todos los archivos explorados en los archivos comprimidos de autoextracción, incluidos los que no estén infectados (podría generar muchos datos de registro de exploración e incrementar el tamaño del archivo del registro de exploración).

Habilitar la optimización inteligente – cuando la opción para habilitar la optimización inteligente está seleccionada, se usa la configuración más favorable para garantizar el nivel de exploración más eficiente, al mismo tiempo que mantiene la mayor velocidad de exploración. Los diversos módulos de protección realizan exploraciones en forma inteligente; para ello emplean distintos métodos de exploración y los aplican a tipos de archivos específicos. Si se deshabilita la optimización inteligente, solo se aplica la configuración definida por el usuario en el núcleo ThreatSense de esos módulos específicos al efectuar una exploración.

Preservar el último acceso con su fecha y hora – seleccione esta opción para preservar la hora de acceso original a los archivos explorados en vez de actualizarla (por ejemplo, para usarlos con sistemas que realizan copias de seguridad de datos).

Límites

La sección Límites permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

Configuración de los objetos

Tamaño máximo del objeto – define el tamaño máximo de los objetos que se van a explorar. El módulo antivirus determinado explorará solamente los objetos con un tamaño inferior al especificado. Los únicos que deberían modificar esta opción son los usuarios avanzados que tengan motivos específicos para excluir objetos de mayor tamaño de la exploración. Valor predeterminado: ilimitado.

Tiempo máximo de exploración para el objeto (seg.): define el valor máximo de tiempo para explorar un objeto en un contenedor (como un archivo RAR/ZIP o un correo electrónico con varios adjuntos). Esta configuración no rige para archivos independientes. Si en esta opción se ingresó un valor definido por el usuario y el tiempo ha transcurrido, la exploración se detendrá lo antes posible, sin importar si finalizó la exploración de cada uno de los archivos en un objeto de contenedor.
En el caso de un archivo con varios archivos grandes, la exploración se detendrá en cuanto se extraiga un archivo (por ejemplo, cuando la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo demora 5 segundos). El resto de los archivos del archivo general no se explorarán una vez que haya transcurrido esa cantidad de tiempo.

Para limitar el tiempo de exploración, incluidos los archivos más grandes, use las opciones **Tamaño máximo del objeto** y **Tamaño máximo del archivo incluido en el archivo comprimido** (no se recomienda debido a posibles riesgos para la seguridad).
Valor predeterminado: ilimitado.

Configuración de la exploración de archivos comprimidos

Nivel de anidado de archivos comprimidos – especifica la profundidad máxima de la exploración de archivos comprimidos. Valor predeterminado: 10.

Tamaño máximo del archivo incluido en el archivo comprimido – esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. El valor máximo es **3 GB**.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no existe ninguna razón para modificarlos.

Protección del acceso a la Web

La protección de acceso a la web permite configurar opciones avanzadas del módulo de protección de Internet. Las siguientes opciones están disponibles en Configuración avanzada > **Protecciones** > **Protección de acceso a la Web** > **Protección de acceso a la web**:

Habilitar la protección de acceso a la web – Cuando está deshabilitada, no se ejecuta la Protección del acceso a la web ni la Protección anti-phishing.

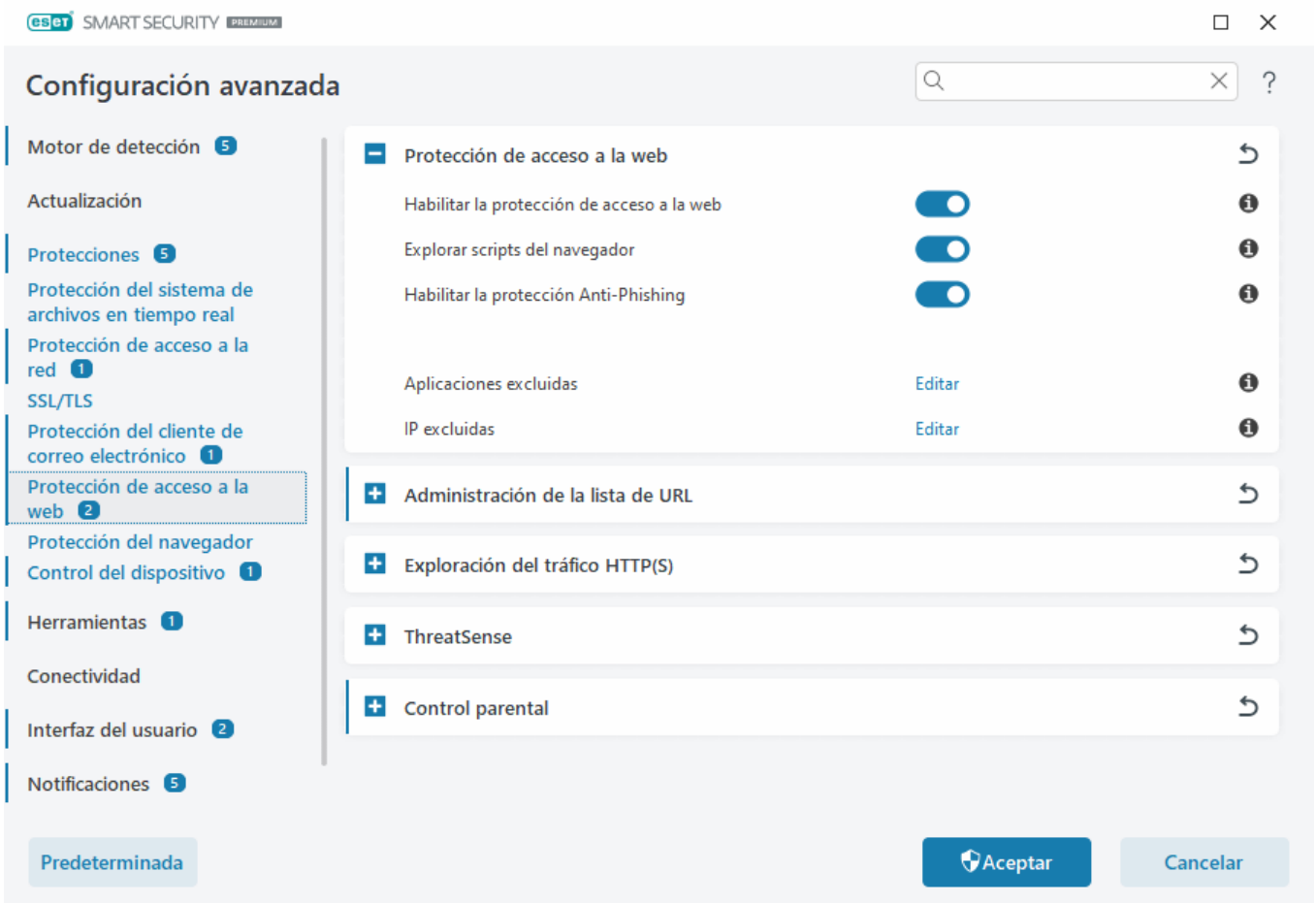
> Le recomendamos encarecidamente que deje habilitada la protección de acceso a la web y no excluya ninguna aplicación o dirección IP de forma predeterminada.

Explorar scripts del navegador: cuando está activado, el motor de detección comprueba todos los programas JavaScript ejecutados por los navegadores web.

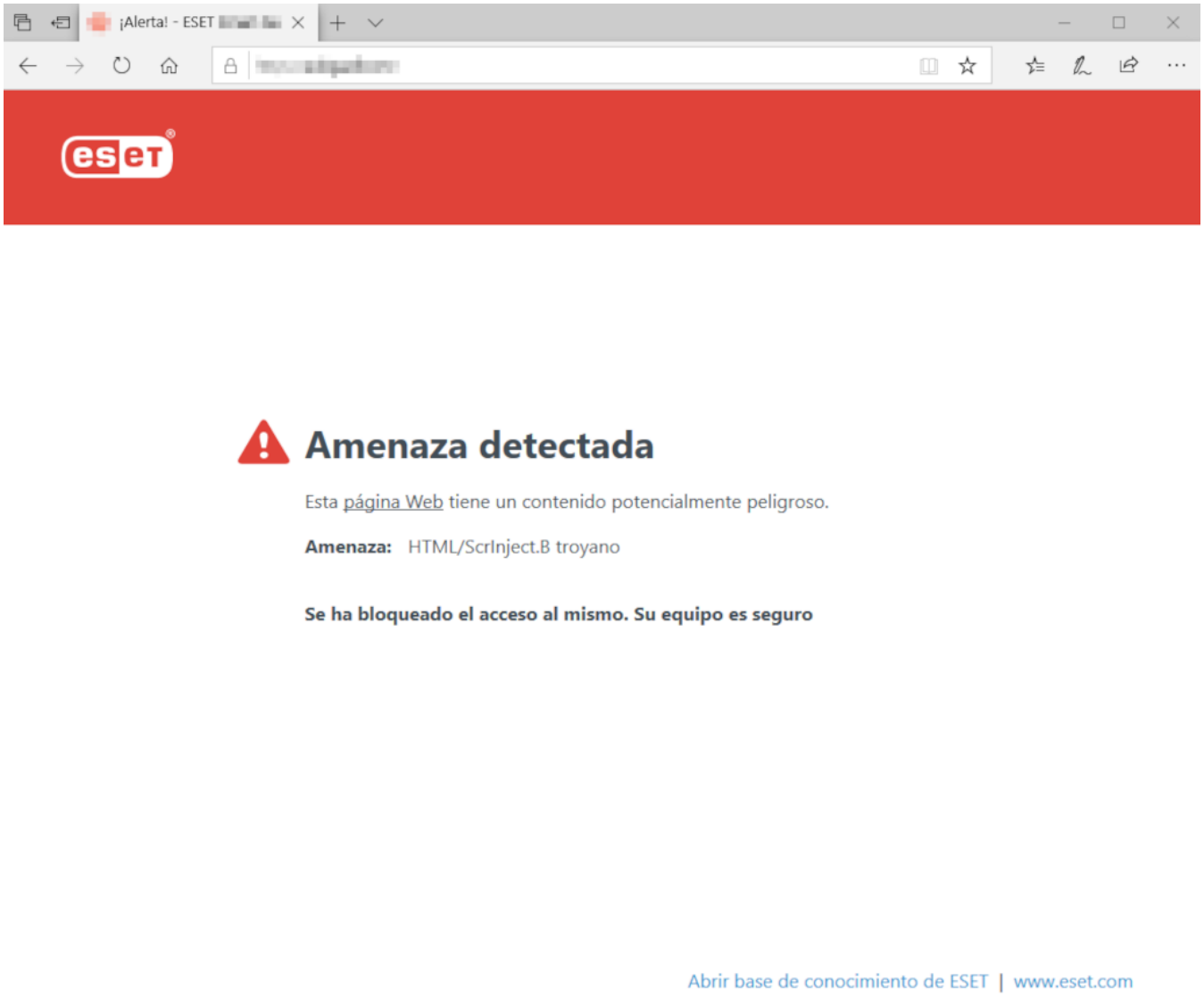
Habilitar protección antiphishing: cuando está habilitada, las páginas web de phishing se bloquean. Consulte Protección antiphishing para obtener más información.

Aplicaciones excluidas: permite excluir aplicaciones específicas de la exploración mediante la Protección de acceso a la Web. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.

IP excluidas: permite excluir direcciones remotas específicas de la exploración mediante la Protección de acceso a la Web. Útil cuando la protección de acceso a la Web causa problemas de compatibilidad.



Protección de acceso a la web mostrará al siguiente mensaje en su navegador cuando el sitio web esté bloqueado:



Instrucciones ilustradas

Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- Impedir que Protección de acceso a la web bloquee un sitio web seguro
- Bloquear un sitio web con ESET Security Ultimate

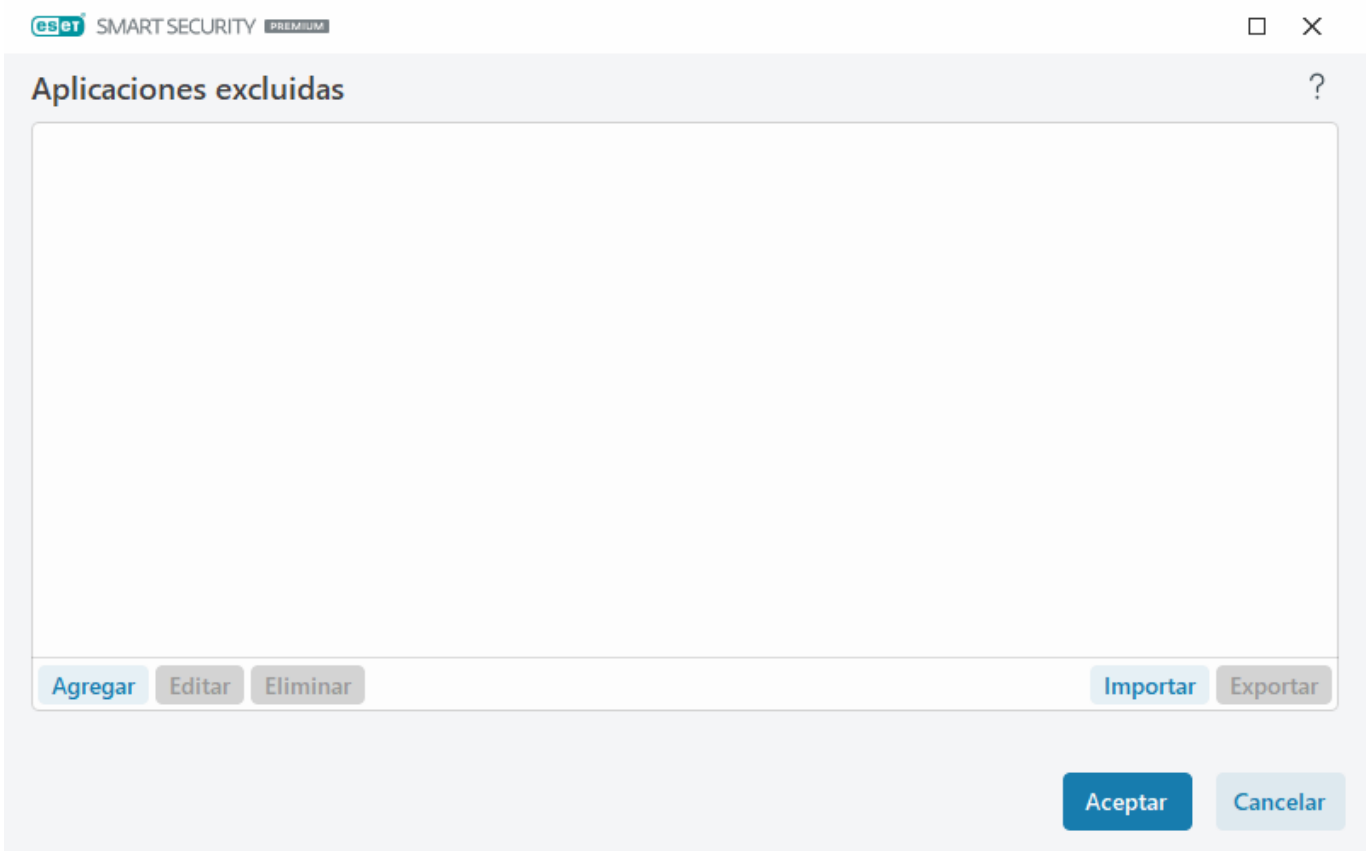
Aplicaciones excluidas

Para excluir la exploración de la comunicación para aplicaciones específicas, agréguelas a la lista. La comunicación HTTP(S)/POP3(S)/IMAP(S) de las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable usar esta opción solamente para las aplicaciones que no funcionen correctamente cuando se explora su comunicación.

Las aplicaciones y los servicios activos se mostrarán automáticamente en esta ventana al hacer clic en **Agregar**. Haga clic en **...** y navegue hasta una aplicación para agregar la exclusión manualmente.

Editar – edite las entradas seleccionadas de la lista.

Quitar – elimine las entradas seleccionadas de la lista.



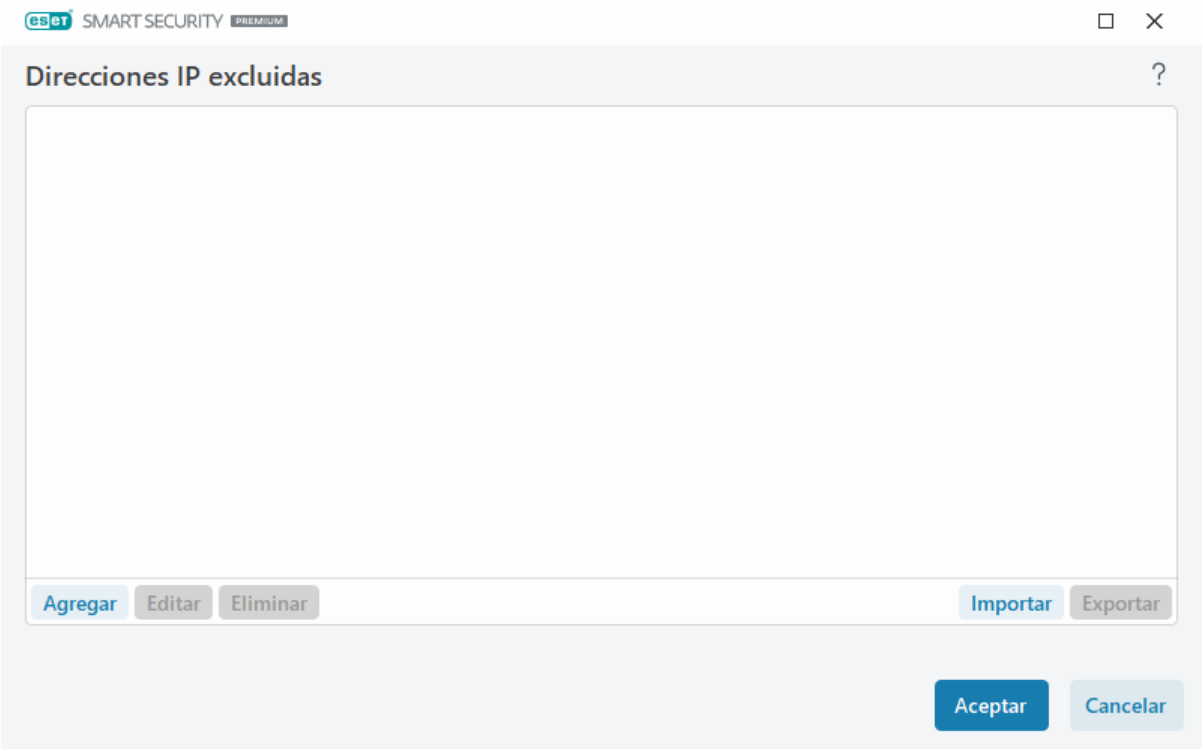
IP excluidas

Las entradas de la lista quedarán excluidas de la exploración. La comunicación HTTP(S)/POP3(S)/IMAP(S) desde o hacia las aplicaciones seleccionadas no se verificará en busca de amenazas. Es recomendable que únicamente use esta opción para direcciones confiables conocidas.

Haga clic en **Agregar** para agregar 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 **Quitar** para eliminar las entradas seleccionadas de la lista.



Ejemplos de direcciones IP

Agregar dirección IPv4:
Dirección única: agrega una dirección IP de un equipo individual (por ejemplo, *192.168.0.10*).
Rango de direcciones: escriba la primera y la última dirección IP para especificar el rango de IP de varios equipos (por ejemplo, *192.168.0.1 a 192.168.0.99*).
Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara. Por ejemplo, 255.255.255.0 es la máscara de red para 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 equipo individual (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Subred: la subred (un grupo de equipos) está definida por una dirección IP y una máscara (por ejemplo, *2002:c0a8:6301:1::1/64*).

Administración de la lista de URL

La **administración de la lista URL** en Configuración avanzada > **Protecciones** > **Protección de acceso a la Web** le permite especificar HTTP direcciones para bloquear, permitir o excluir de la exploración de contenido.

SSL/TLS debe estar habilitado si desea filtrar direcciones HTTPS además de HTTP. De lo contrario, solo se agregarán los dominios de los sitios HTTPS que haya visitado, y no se agregará la URL completa.

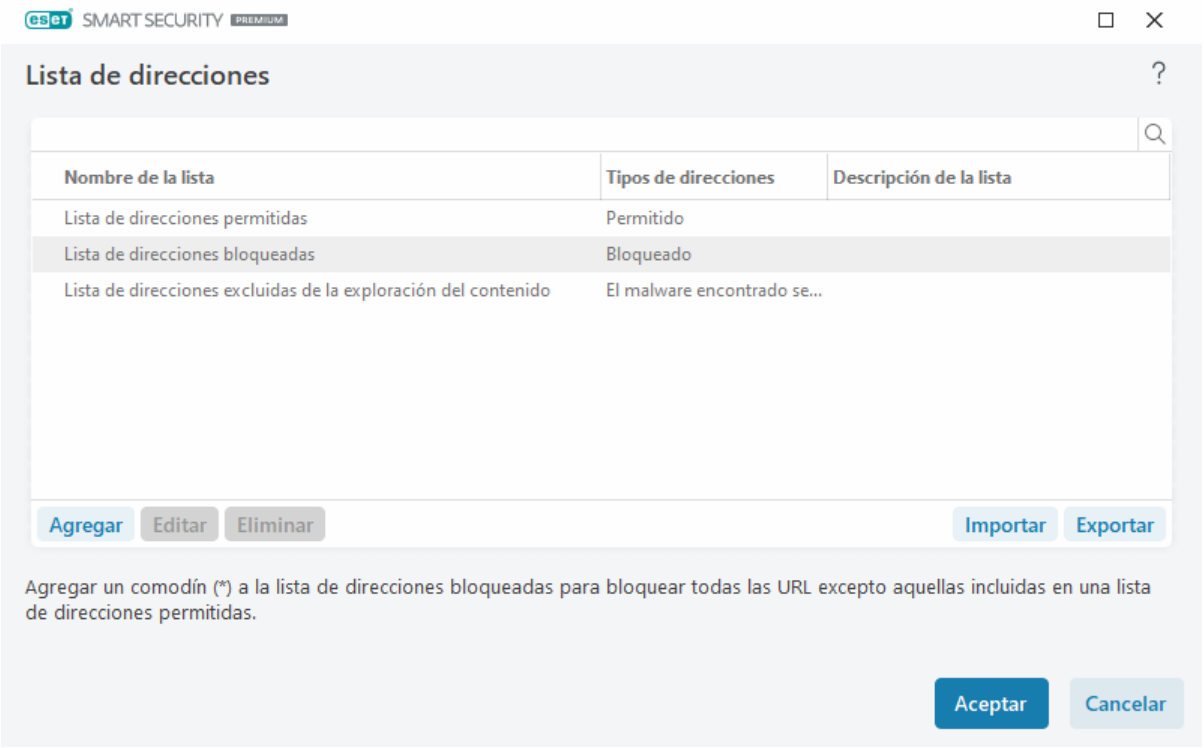
No será posible acceder a los sitios web incluidos en la **Lista de direcciones bloqueadas**, a menos que también estén incluidos en la **Lista de direcciones permitidas**. Los sitios web en la **Lista de direcciones excluidas de la exploración del contenido** no se exploran en busca de códigos maliciosos cuando se accede a los mismos.

Si desea bloquear todas las direcciones HTTP excepto las direcciones presentes en la **Lista de direcciones permitidas** activa, agregue un * a la **Lista de direcciones bloqueadas** activa.

Pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación) en las listas. El asterisco sustituye cualquier cadena de caracteres y el signo de interrogación sustituye cualquier símbolo. Cuando

especifique direcciones excluidas, debe tener especial cuidado, 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 Agregado de una máscara de dominio/dirección HTTP para conocer cómo todo un dominio, incluidos los subdominios, pueden hacerse coincidir de manera 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 **No explorar el tráfico con dominios en los que ESET confía** está habilitado es SSL/TLS, los dominios en la lista blanca administrados por ESET no se verán afectados por la configuración de administración de la lista de URL.



Elementos de control

Agregar – crea una nueva lista además de las predefinidas. Esto puede ser útil si desea separar de manera lógica los diferentes grupos de direcciones. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que una segunda lista puede contener su propia lista negra, lo que facilita la actualización de la lista externa mientras que mantiene intacta la suya.

Editar – modifica las listas existentes. Use esto para agregar o eliminar las direcciones.

Eliminar – elimina las listas existentes. Solo es posible para las listas creadas con la opción **Agregar**, no con las opciones predeterminadas.

Lista de direcciones

En esta sección, puede especificar las listas de direcciones HTTP(S) que se bloquearán, permitirán o excluirán de la verificación.

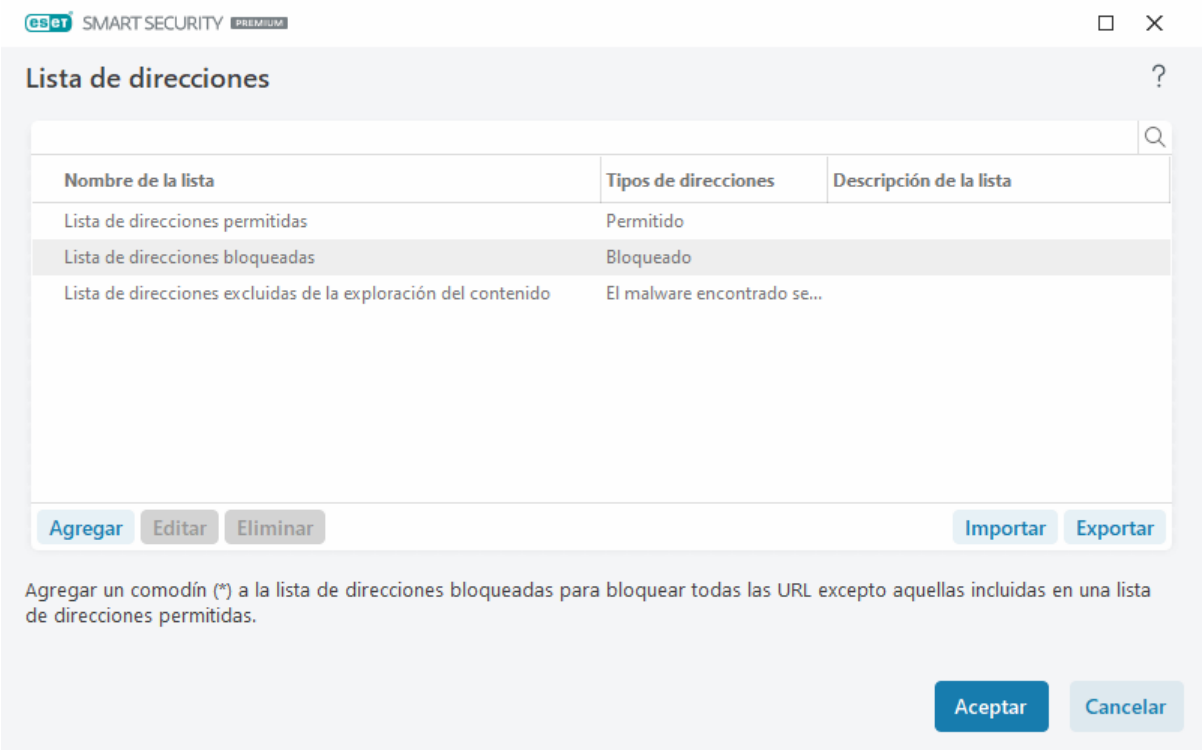
De forma predeterminada, se pueden utilizar estas tres listas:

• **Lista de direcciones excluidas de la exploración de contenidos**: no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.

• **Lista de direcciones permitidas** – si se habilita 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 que se encuentran en esta lista. Las direcciones de esta lista se permiten incluso si están incluidas en la lista de direcciones bloqueadas.

• **Lista de direcciones bloqueadas**: el usuario no tendrá acceso a las direcciones especificadas en esta lista, a menos que también aparezcan en la lista de direcciones permitidas.

Haga clic en **Agregar** para crear una lista nueva. Para eliminar las listas seleccionadas, haga clic en **Quitar**.



Instrucciones ilustradas

Los siguientes artículos de la base de conocimiento de ESET pueden estar disponibles solo en inglés:

- Impedir que Protección de acceso a la web bloquee un sitio web seguro
- Bloquear un sitio web con los productos hogareños de ESET Windows

Para obtener más información, consulte Administración de la lista de URL.

Crear nueva lista de direcciones

Este cuadro de diálogo le permite configurar una nueva lista de direcciones URL o máscaras que se bloquearán, se permitirán o se excluirán en la comprobación.

Puede configurar las siguientes opciones:

Tipo de lista de direcciones – hay tres tipos de listas disponibles:

• **El malware encontrado se ha ignorado** – no se comprobará la existencia de códigos maliciosos 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 permiten incluso si coinciden con las de la lista de direcciones bloqueadas.

Nombre de la lista – especifique el nombre de la lista. Este campo no estará disponible al editar una de las listas predefinidas.

Descripción de la lista – escriba una breve descripción de la lista (opcional). No está disponible al editar una de las listas predefinidas.

Para activar una lista, seleccione **Lista activa** junto a esa lista. Si desea recibir una notificación cuando se utilice una lista específica al acceder a sitios web, seleccione **Notificar cuando se aplique**. Por ejemplo, recibirá una notificación si un sitio web está bloqueado o permitido por estar incluido en una lista de direcciones bloqueadas o permitidas. Esta notificación incluirá el nombre de la lista que contiene el sitio web especificado.

Severidad de registro – información sobre la lista específica que se usa al acceder a sitios web y que se puede escribir en los archivos de registro.

Elementos de control

Agregar – agregue una dirección URL nueva a la lista (ingrese múltiples valores con separadores).

Editar – modifica la dirección existente en la lista. Solo está disponible para direcciones creadas con **Agregar**.

Quitar – elimina las direcciones existentes en la lista. Solo está disponible para direcciones creadas con **Agregar**.

Importar – importe un archivo con direcciones URL (valores separados por un salto de línea; por ejemplo, *.txt al usar codificación UTF-8).

Cómo agregar una máscara URL

Consulte las indicaciones de este cuadro de diálogo antes de ingresar la máscara de dominio/dirección deseada.

ESET Security Ultimate les permite a los usuarios bloquear el acceso a determinados sitios Web para evitar que el navegador de Internet muestre su contenido. Además, permite especificar las direcciones que se van a excluir de la verificación. Si se desconoce el nombre completo del servidor remoto o si el usuario desea especificar un grupo completo de servidores remotos, se pueden usar las máscaras para identificar dicho grupo. Las máscaras incluyen los símbolos “?” y “*”:

- use ? para sustituir un símbolo

- use * para sustituir una cadena de texto.

Por ejemplo, *.c?m se aplica a todas las direcciones cuya última parte comience con la letra c, termine con la letra m y contenga un símbolo desconocido entre las dos (.com, .cam, etc.).

Una primera secuencia “*.” se trata de modo especial si se utiliza al comienzo del nombre del dominio. Primero, el comodín * no coincide con carácter de barra (“/”) en este caso. Esto es para evitar evadir la máscara, por

ejemplo la máscara **.domain.com* no coincidirá con *http://anydomain.com/anypath#.domain.com* (dicho sufijo puede anexarse a cualquier URL sin afectar la descarga). Y segundo, el "*." también coincide con una cadena vacía en este caso especial. Esto es para permitir que coincida todo el dominio incluidos los subdominios usando una sola máscara. Por ejemplo la máscara **.domain.com* también coincide con *http://domain.com*. Utilizar **domain.com* sería incorrecto, ya que también coincidiría con *http://anotherdomain.com*.

Exploración del tráfico HTTP(S)

De forma predeterminada, ESET Security Ultimate está configurado para explorar el tráfico HTTP y HTTPS que utilizan los navegadores de Internet y otras aplicaciones. Debe deshabilitar la exploración de tráfico únicamente si tiene problemas con un software de terceros y desea saber si el problema es causado por ESET Security Ultimate.

Activar exploración del tráfico HTTP: el tráfico de HTTP se supervisa siempre en todos los puertos para todas las aplicaciones.

Habilitar la exploración del tráfico HTTPS: el tráfico HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Security Ultimate verifica la comunicación mediante los protocolos SSL (protocolo de capa de socket seguro) y TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en 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 está conformada por muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también brinda protección durante las primeras horas de propagación de una nueva amenaza. Utiliza una combinación de la exploración del código, la emulación del código, las firmas genéricas y las firmas de virus que funcionan conjuntamente para mejorar en forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar simultáneamente varios flujos de datos para maximizar la eficiencia y la tasa de detección. La tecnología de ThreatSense también elimina los rootkits de forma correcta.

Las opciones de configuración del motor ThreatSense le permiten especificar varios parámetros de exploración:

- Los tipos de archivos y las extensiones que se van a explorar
- La combinación de diversos métodos de detección.
- Los niveles de desinfección, etc.

Para ingresar a la ventana de configuración, haga clic en **ThreatSense** ubicado en Configuración avanzada de cualquier módulo que use la tecnología ThreatSense (ver abajo). Diferentes situaciones de seguridad pueden requerir diferentes configuraciones. Por este motivo, ThreatSense puede configurarse en forma individual para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Exploración en estado inactivo
- Exploración en el inicio

- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del acceso a la Web
- Exploración del equipo

Los parámetros de ThreatSense están sumamente optimizados para cada módulo y su modificación puede afectar el funcionamiento del sistema en forma significativa. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, solo los nuevos archivos creados se exploran con estos métodos). En consecuencia, es recomendable mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos excepto para la exploración del equipo.

Objetos para explorar

Esta sección le permite definir qué componentes y archivos del equipo se explorarán en busca de infiltraciones.

Memoria operativa – explora en busca de amenazas que atacan la memoria operativa del sistema.

Sectores de inicio/UEFI: explora los sectores de inicio para detectar la presencia de virus en el Master Boot Record. Lea más sobre UEFI en el glosario.

Archivos de correo electrónico – el programa es compatible con las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos – el programa es compatible con las siguientes extensiones, ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE entre muchas otras.

Archivos de autoextracción: los archivos de autoextracción (SFX) son los archivos que se pueden extraer a sí mismos.

Empaquetadores de tiempo de ejecución: después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el explorador puede reconocer varios tipos de empaquetadores adicionales mediante el uso de la emulación del código.

Opciones de exploración

Seleccione los métodos utilizados al explorar el sistema en busca de infiltraciones. Se encuentran disponibles las siguientes opciones:

Heurística – la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de esta tecnología radica en su capacidad de identificar software malicioso que antes no existía o que no era reconocido por la versión anterior del motor de detección. La desventaja es la probabilidad (muy reducida) de identificar falsos positivos.

Heurística avanzada/Firmas de ADN: la heurística avanzada está compuesta por un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que se crearon con lenguajes de programación de última generación. El uso de la heurística avanzada incrementa significativamente

la capacidad de detección de amenazas de los productos de ESET. Las firmas tienen la capacidad de detectar e identificar los virus en forma confiable. Mediante el uso del sistema de actualizaciones automáticas, las nuevas firmas están disponibles en el transcurso de unas pocas horas tras el descubrimiento de una amenaza. La desventaja de las firmas es que solo detectan los virus que ya conocen (o las versiones ligeramente modificadas de estos virus).

Desinfección

La configuración de la desinfección determina el comportamiento de ESET Security Ultimate durante la desinfección de objetos. Existen cuatro niveles de desinfección:

ThreatSense incluye los siguientes niveles de corrección (es decir, desinfección).

Corrección ESET Security Ultimate

Nivel de desinfección	Descripción
Corregir siempre la detección	Intento de corregir la detección al limpiar objetos sin la intervención del usuario final. En algunos pocos casos (por ejemplo, en archivos de sistema), si la detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario conservar	Intento de corregir la detección al desinfectar objetos sin la intervención del usuario final. En algunos casos (por ejemplo, en archivos de sistema con archivos desinfectados o infectados), si una detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario preguntar	Intento de corregir la detección al desinfectar 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). Esta configuración se recomienda en la mayoría de los casos.
Preguntar siempre al usuario final	El usuario final visualiza una ventana interactiva al desinfectar objetos y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de hallar una detección.

Exclusiones

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de ThreatSense permite definir los tipos de archivos que se van a explorar.

Otros

Cuando se configuran los parámetros del motor ThreatSense para una exploración del equipo bajo demanda, las siguientes opciones en la sección **Otros** también están disponibles:

Explorar secuencias de datos alternativas (ADS) – las secuencias de datos alternativas usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección camuflándose como secuencias de datos alternativas.

Realizar exploraciones en segundo plano con baja prioridad – cada secuencia de exploración consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye

una carga importante para los recursos del sistema, es posible activar la exploración en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos – El Registro de la exploración mostrará todos los archivos explorados en los archivos comprimidos de autoextracción, incluidos los que no estén infectados (podría generar muchos datos de registro de exploración e incrementar el tamaño del archivo del registro de exploración).

Habilitar la optimización inteligente – cuando la opción para habilitar la optimización inteligente está seleccionada, se usa la configuración más favorable para garantizar el nivel de exploración más eficiente, al mismo tiempo que mantiene la mayor velocidad de exploración. Los diversos módulos de protección realizan exploraciones en forma inteligente; para ello emplean distintos métodos de exploración y los aplican a tipos de archivos específicos. Si se deshabilita la optimización inteligente, solo se aplica la configuración definida por el usuario en el núcleo ThreatSense de esos módulos específicos al efectuar una exploración.

Preservar el último acceso con su fecha y hora – seleccione esta opción para preservar la hora de acceso original a los archivos explorados en vez de actualizarla (por ejemplo, para usarlos con sistemas que realizan copias de seguridad de datos).

Límites

La sección Límites permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

Configuración de los objetos

Tamaño máximo del objeto – define el tamaño máximo de los objetos que se van a explorar. El módulo antivirus determinado explorará solamente los objetos con un tamaño inferior al especificado. Los únicos que deberían modificar esta opción son los usuarios avanzados que tengan motivos específicos para excluir objetos de mayor tamaño de la exploración. Valor predeterminado: ilimitado.

Tiempo máximo de exploración para el objeto (seg.): define el valor máximo de tiempo para explorar un objeto en un contenedor (como un archivo RAR/ZIP o un correo electrónico con varios adjuntos). Esta configuración no rige para archivos independientes. Si en esta opción se ingresó un valor definido por el usuario y el tiempo ha transcurrido, la exploración se detendrá lo antes posible, sin importar si finalizó la exploración de cada uno de los archivos en un objeto de contenedor.
En el caso de un archivo con varios archivos grandes, la exploración se detendrá en cuanto se extraiga un archivo (por ejemplo, cuando la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo demora 5 segundos). El resto de los archivos del archivo general no se explorarán una vez que haya transcurrido esa cantidad de tiempo.
Para limitar el tiempo de exploración, incluidos los archivos más grandes, use las opciones **Tamaño máximo del objeto** y **Tamaño máximo del archivo incluido en el archivo comprimido** (no se recomienda debido a posibles riesgos para la seguridad).
Valor predeterminado: ilimitado.

Configuración de la exploración de archivos comprimidos

Nivel de anidado de archivos comprimidos – especifica la profundidad máxima de la exploración de archivos comprimidos. Valor predeterminado: 10.

Tamaño máximo del archivo incluido en el archivo comprimido – esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. El valor máximo es

3 GB.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no existe ninguna razón para modificarlos.

Control parental

La opción **Activar control parental** integra el control parental en ESET Security Ultimate. Haga clic en **Editar** junto a Cuentas de usuarios para asociar las cuentas de usuario de Windows usadas por Control parental para limitar el acceso de ciertos usuarios a contenido inapropiado o perjudicial en Internet.

Cuentas de usuarios

En Configuración avanzada > **Protecciones** > **Protección de acceso a la Web** > **Control parental** > **Cuentas de usuario** > **Editar** puede asociar las cuentas de usuario de Windows usadas por Control parental para limitar el acceso de ciertos usuarios a contenido inapropiado o perjudicial en Internet.

Columnas

Cuenta de usuario: nombre del usuario.

Habilitado: cuando se habilita, se activan los controles parentales para una cuenta de usuario específica.

Dominio: el nombre del dominio al cual pertenece un usuario.

Cumpleaños: la edad del usuario a quien pertenece esta cuenta.

Elementos de control

Agregar: se mostrará el diálogo Trabajar con cuentas de usuario.

Editar: esta opción permite editar las cuentas seleccionadas.

Quitar: eliminar la cuenta seleccionada.

Actualizar: si agregó un cuenta de usuario, ESET Security Ultimate puede actualizar la lista de cuentas de usuario sin necesidad de volver a abrir esta ventana.

Configuración de la cuenta de usuario

Esta ventana tiene tres pestañas:

General

Habilite el interruptor junto a **Activado** para activar el Control parental para la cuenta Windows seleccionada a continuación.

Primero debe **Seleccionar** una cuenta del Windows desde su equipo. Las restricciones establecidas en Control parental solamente afectan las cuentas estándares de Windows. Las cuentas administrativas pueden anular las

restricciones.

Si la cuenta la utiliza un padre, seleccione **Cuenta para padres**.

Defina la **fecha de nacimiento del niño** para la cuenta para determinar su nivel de acceso y establezca reglas de acceso para páginas web adecuadas para su edad.

Severidad de registro

ESET Security Ultimate guarda todos los sucesos importantes en un archivo de registro, que se puede ver directamente desde el menú principal. Haga clic en **Herramientas** > **Archivos de registro** y luego seleccione **Control parental** en el menú desplegable **Registro**.

- **Diagnóstico** – registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes de información, que incluyen las excepciones permitidas y bloqueadas, y todos los registros mencionados.
- **Advertencia** – registra los errores críticos y mensajes de advertencia.
- **Ninguno** – no se realizará registro alguno.

Excepciones

Crear una excepción puede permitir o denegar a un usuario el acceso a sitios Web que no están en la lista de excepciones. Esto es útil si desea controlar el acceso a sitios Web específicos en lugar de utilizar categorías. Las excepciones creadas para una cuenta se pueden copiar y usar en otra. Esto puede ser de ayuda si quiere crear reglas idénticas para niños de edades similares.

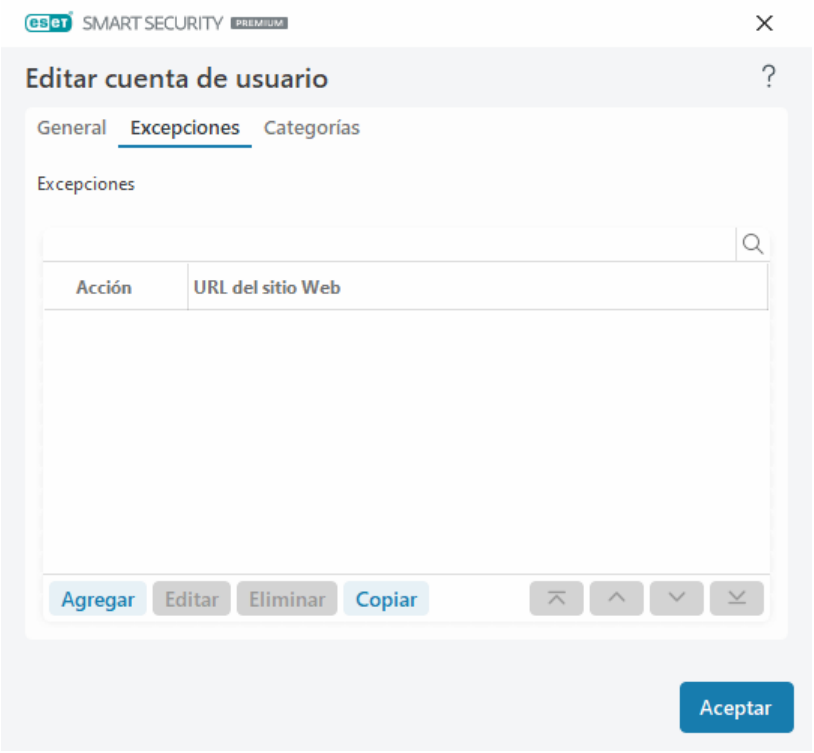
Haga clic en **Agregar** para crear una excepción nueva. Especifique la **Acción** (por ejemplo, **Bloquear**) utilizando el menú desplegable, ingrese la **URL del sitio Web** al cual se aplica esta excepción y luego haga clic en **ACEPTAR**. La excepción se agregará a la lista de excepciones existentes y se mostrará su estado.

Agregar: crea una excepción.

Editar: puede editar la **URL del sitio Web** o la **Acción** de la excepción seleccionada.

Eliminar: quita la excepción seleccionada.

Copiar: seleccione un usuario del menú desplegable desde el cual desea copiar una excepción creada.

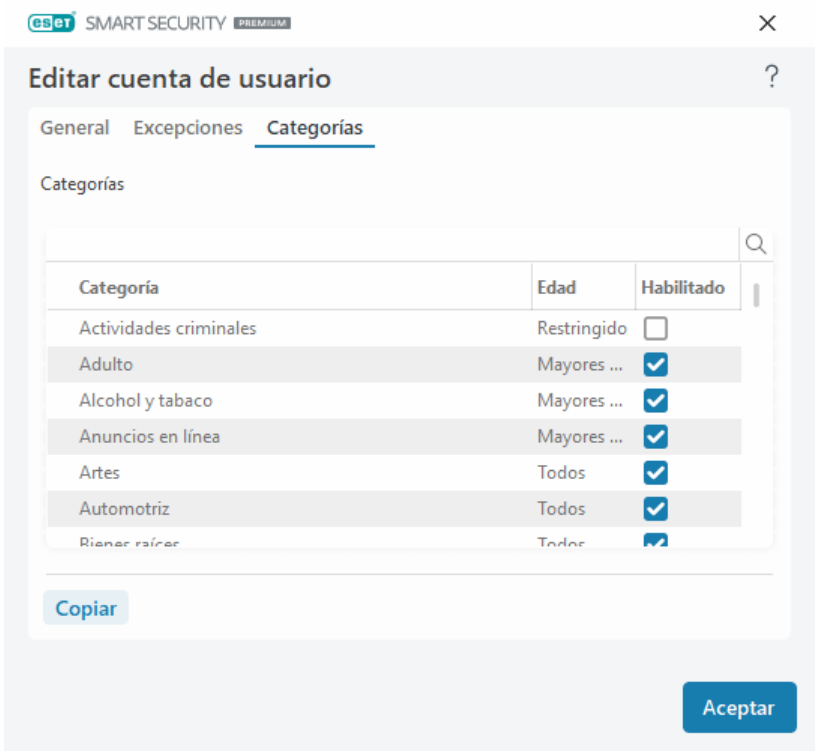


Las excepciones definidas sobrescriben las categorías definidas para las cuentas seleccionadas. Por ejemplo, si la categoría **Noticias** está bloqueada para una cuenta, pero usted definió una página Web de noticias como una excepción, la cuenta podrá acceder a esa página Web específica. Puede ver todos los cambios realizados desde la sección Excepciones.

Categorías

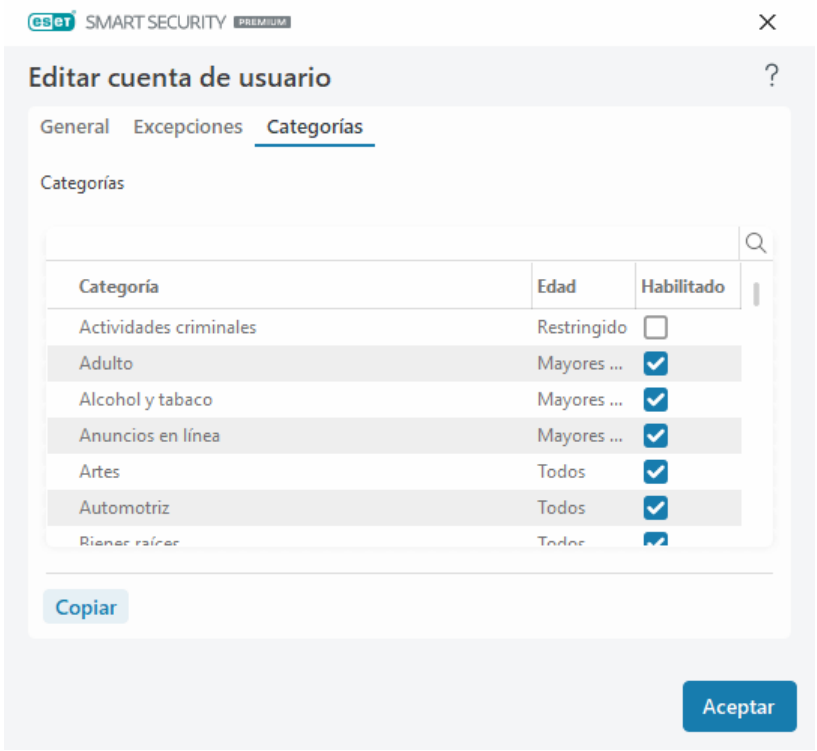
En la pestaña **Categorías**, puede definir las categorías generales de los sitios web que desea bloquear o permitir para cada cuenta. Seleccione la casilla de verificación junto a una categoría para habilitarla. Si deja vacía la casilla de verificación, no se permitirá el uso de la categoría para esa cuenta.

Copiar: le permite copiar una lista de categorías bloqueadas o permitidas de una cuenta modificada existente.



Categorías

Marque la casilla de verificación en la columna **Habilitado** junto a la categoría para activarla. Si deja la casilla vacía, no se permitirá el uso de la categoría para esa cuenta.



Estos son algunos ejemplos de categorías (grupos) con los que podrían no estar familiarizados los usuarios:

- **Varios**: por lo general, direcciones IP privadas (locales), como intranet, 127.0.0.0/8, 192.168.0.0/16, etc. Cuando recibe un código de error 403 o 404, el sitio Web también coincidirá con esta categoría.

- **No resuelto**: esta categoría incluye páginas Web no resueltas debido a un error de conexión con el motor de la base de datos de control parental.
- **No categorizado**: páginas Web desconocidas que aún no forman parte de la base de datos de control parental.
- **Dinámico**: páginas Web que redirigen a otras páginas en otros sitios web.

Protección del navegador

La protección del navegador es otra capa de protección para su seguridad y privacidad que protege la memoria del navegador de la inspección por parte de otros procesos, aumenta la protección contra los keyloggers y evita pegar cualquier dato relacionado con el pago en línea modificado por 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 de autorización de protección del navegador
- Marco del navegador

Banca y navegación seguras

Puede configurar Banca y navegación seguras en Configuración avanzada > **Protecciones** > **Protección del navegador** > **Banca y navegación seguras**.

Banca y navegación seguras

Habilitar Banca y navegación seguras: cuando Banca y navegación seguras está habilitada, 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 la extensión: desde el menú desplegable, puede seleccionar qué extensiones se permitirán instalar en un navegador protegido por ESET:

- **Extensiones esenciales:** solo las extensiones esenciales desarrolladas por un fabricante específico de navegadores.
- **Todas las extensiones:** todas las extensiones compatibles con un navegador específico.

> Cambiar el modo de instalación de extensiones no afecta las extensiones del navegador instaladas anteriormente:

Navegador seguro

Protección de memoria optimizada – Si se habilita, se protegerá la memoria del navegador seguro contra inspecciones de otros procesos.

Protección con el teclado: si se habilita, la información que ingrese con el teclado en el navegador seguro estará oculta para otras aplicaciones. Esta opción aumenta la protección contra registradores de pulsaciones.

Protección del portapapeles: si está habilitada, ESET Security Ultimate evitará pegar cualquier dato relacionado con los pagos en línea modificado por malware desde el portapapeles en el navegador seguro. Esto garantiza la protección contra posibles cambios realizados por software malintencionado.

Marco del navegador – Personalice la configuración de pantalla del marco del navegador en navegadores protegidos.

Lista de autorización de protección del navegador – Administre los archivos agregados a la lista de autorización de protección del navegador.

Seguridad y privacidad del navegador

Habilitar Seguridad y privacidad del navegador: si está deshabilitada, la extensión Seguridad y privacidad del navegador se desinstalará de todos los navegadores compatibles en todas las cuentas de Windows.

Mostrar notificaciones de Seguridad y privacidad del navegador: si está habilitada, ESET Security Ultimate mostrará las notificaciones de Seguridad y privacidad del navegador.

Explorador de scripts del navegador

Habilitar la exploración avanzada de los scripts del navegador: si está habilitada, el explorador de antivirus comprobará todos los programas JavaScript ejecutados por los navegadores de Internet.

00

Control de dispositivos

ESET Security Ultimate proporciona control de dispositivo (CD/DVD//USBetc.) automático. Este módulo permite bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado. Resulta útil si el administrador del equipo desea prevenir el uso de dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (HDD, disco USB extraíble)
- CD/DVD
- Impresora USB
- FireWire Almacenamiento

- Bluetooth Dispositivo
- Lector de tarjeta inteligente
- Dispositivo de imagen
- Módem
- LPT/COM puerto
- Dispositivo portátil (dispositivos con batería, como medios de comunicación, 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**.

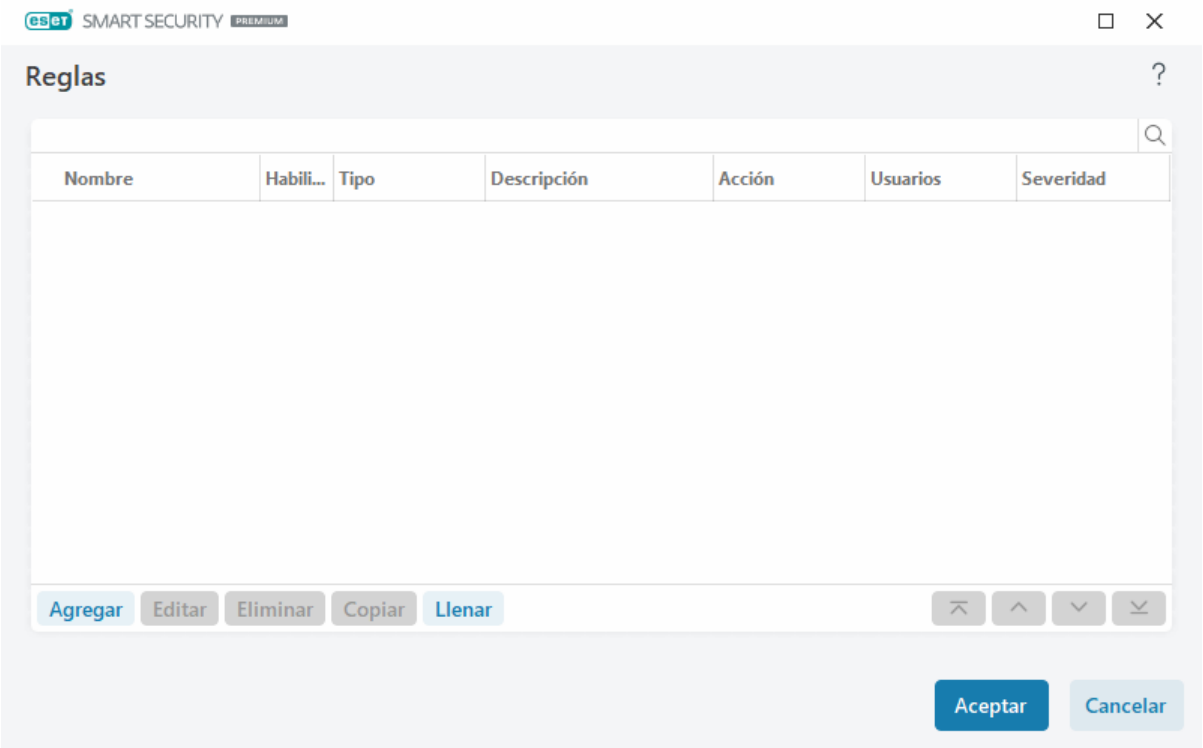
Haga clic en el interruptor **Habilitar control del dispositivo** para habilitar la función Control del dispositivo en ESET Security Ultimate; debe reiniciar el equipo para que este cambio surta efecto. Después de habilitar el Control del dispositivo, podrá definir las **Reglas** en la ventana Editor de reglas.

> Puede crear distintos grupos de dispositivos donde se aplicarán reglas diferentes. También puede crear solo un grupo de dispositivos para el que se aplicará la regla con la acción **Permitir** o **Bloquear escritura**. Esto garantiza que el Control de dispositivos bloquee los dispositivos no reconocidos cuando se conectan a su equipo.

Si se inserta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación y no se otorgará el acceso al dispositivo.

Editor de reglas del control del dispositivo

La ventana **Editor de reglas del control del dispositivo** muestra las reglas existentes y permite el control preciso de dispositivos externos que los usuarios conectan al equipo.

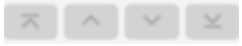


Los dispositivos específicos se pueden permitir o bloquear por usuario o grupo de usuarios y con base en los parámetros adicionales del dispositivo que se pueden especificar en la configuración de reglas. La lista de reglas contiene varias descripciones de una regla como nombre, tipo de dispositivo externo, acción a realizar después de conectar un dispositivo externo en su equipo y la severidad del registro. También consulte Agregar reglas de control del dispositivo.

Haga clic en **Agregar** o **Editar** para administrar una regla. Haga clic en **Copiar** para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML mostradas al hacer clic en una regla se pueden copiar en el portapapeles para ayudar a los administradores del sistema a exportar/importar estos datos y usarlos.

Al presionar **CTRL** y hacer clic, puede seleccionar varias reglas y aplicar acciones, tales como eliminarlas o moverlas hacia arriba o abajo de la lista, a todas las reglas seleccionadas. La casilla de verificación **Habilitada** deshabilita o habilita una regla; esto puede ser útil si desea conservar la regla.

Haga clic en **Llenar** para completar automáticamente los parámetros de los dispositivos de medios extraíbles conectados al equipo.

Las reglas se incluyen en la lista por orden de prioridad, con las reglas de prioridad más alta más cerca de la parte superior. Las reglas se pueden mover al hacer clic en  **Superior/Arriba/Abajo/Inferior**, y se pueden mover individualmente o en grupos.

Las entradas del registro se pueden ver en la ventana principal del programa > **Herramientas** > Archivos de registro.

El Registro del control de dispositivos registra todas las instancias en las que se activa el Control de dispositivos.

Dispositivos detectados

El botón **Llenar** proporciona una visión general de todos los dispositivos actualmente conectados con información acerca de: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible). Si desea ver todos los dispositivos ocultos, seleccione **Mostrar dispositivos ocultos**.

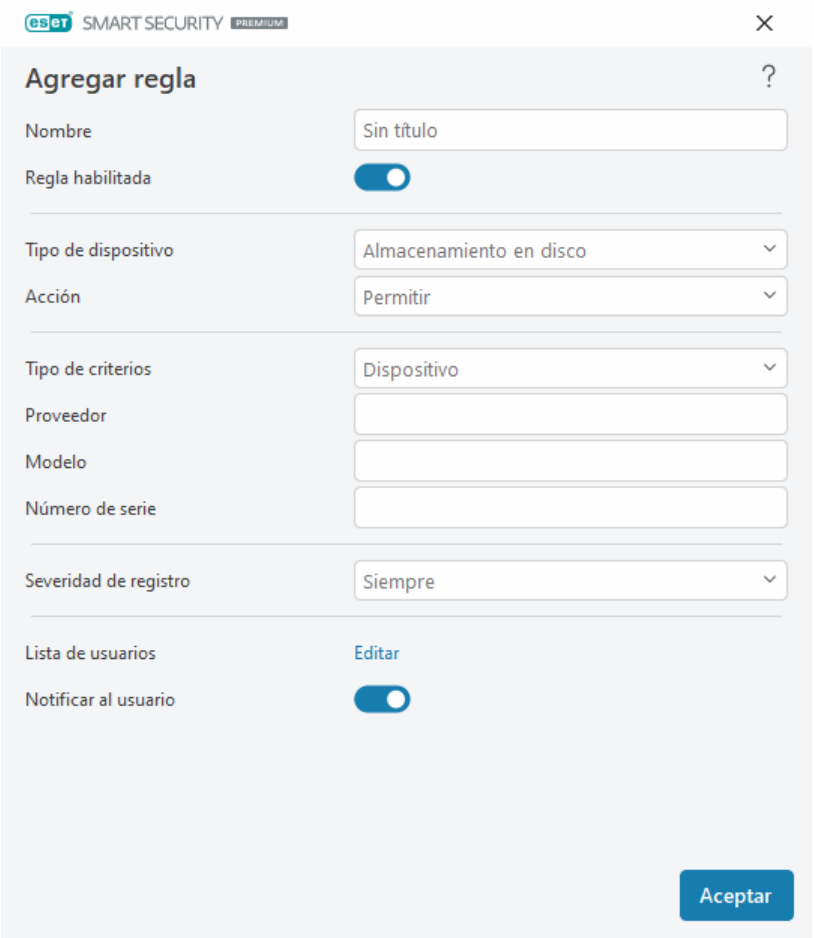
Seleccione un dispositivo de la lista de Dispositivos detectados y haga clic en **Aceptar** para agregar una regla de control de dispositivos con información predefinida (se puede ajustar toda la configuración).

Los dispositivos en modo de baja alimentación (suspensión) están marcados con un ícono 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).

Agregado de reglas del control del dispositivo

Una regla de control del dispositivo define la acción que se tomará cuando un dispositivo, que cumple con los criterios de las reglas, se conecte al equipo.



Ingrese una descripción de la regla en el campo **Nombre** para tener una mejor identificación. Haga clic en el interruptor junto a **Regla habilitada** para deshabilitar o habilitar esta regla; esto puede ser útil si no desea eliminar la regla permanentemente.

Tipo de dispositivo

Elija el tipo de dispositivo externo desde el menú desplegable (Almacenamiento en disco/Dispositivo portátil/Bluetooth/FireWire/...). La información sobre los tipos de dispositivos se recopila del sistema operativo y se puede ver en el administrador de dispositivos del sistema siempre y cuando un dispositivo esté conectado al equipo. Los dispositivos de almacenamiento incluyen los discos externos o los lectores de tarjetas de memoria convencionales conectados por medio de USB o FireWire. Los lectores de tarjetas inteligentes incluyen todos los lectores de tarjetas inteligentes con un circuito integrado, tal como las tarjetas SIM o las tarjetas de autenticación. Los ejemplos de dispositivos de imágenes son los módulos de exploración o cámaras. Debido a que estos dispositivos solo proporcionan información acerca de sus acciones y no proporcionan información acerca de los usuarios, solo se pueden bloquear en forma global.

Acción

El acceso a los dispositivos que no son de almacenamiento se puede permitir o bloquear. Por el contrario, las reglas para los dispositivos de almacenamiento le permiten seleccionar una de las siguientes configuraciones de derechos:

- **Permitir** – se permitirá el acceso total al dispositivo.
- **Bloquear** – se bloqueará el acceso al dispositivo.
- **Bloquear escritura** – solo se permitirá el acceso de lectura al dispositivo.
- **Advertir** – siempre que se conecte un dispositivo, se le notificará al usuario si está permitido/bloqueado, y se generará una entrada de registro. Los dispositivos no se recuerdan, pero sin embargo se mostrará una notificación durante las conexiones posteriores del mismo dispositivo.

Tenga en cuenta que no todas las Acciones (permisos) están disponibles para todos los tipos de dispositivos. Si es un tipo de dispositivo de almacenamiento, las cuatro Acciones estarán disponibles. Para los dispositivos de no almacenamiento, solo hay tres Acciones disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth, por lo que los dispositivos Bluetooth solo se pueden permitir, bloquear o advertir).

Tipo de criterios

Seleccione **Grupo de dispositivos** o **Dispositivo**.

A continuación, se muestran parámetros adicionales que se pueden usar para ajustar las reglas de diferentes dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor** – filtre por nombre o ID del proveedor.
- **Modelo** – el nombre determinado del dispositivo.
- **Número de serie** – los dispositivos externos generalmente tienen sus propios números de serie. En caso de un CD/DVD, este es el número de serie que corresponde al medio determinado, no a la unidad de CD.

> Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado de los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines (un signo de interrogación (?) representa un carácter único, mientras que un asterisco (*) representa una cadena de cero o más caracteres).

> Para ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo a su equipo, y luego verifique los detalles del dispositivo en el Registro del control de dispositivos.

Severidad de registro

ESET Security Ultimate guarda todos los sucesos importantes en un archivo de registro, que se puede ver directamente desde el menú principal. Haga clic en **Herramientas** > **Archivos de registro** y luego seleccione **Control del dispositivo** en el menú desplegable **Registro**.

- **Siempre** – registra todos los eventos.
- **Diagnóstico** – registra la información necesaria para ajustar el programa.
- **Información** – registra los mensajes de información, incluidos los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencia** – registra los errores críticos y mensajes de advertencia.
- **Ninguno** – no se realizará registro alguno.

Lista de usuarios

Las reglas se pueden limitar a ciertos usuarios o grupos de usuarios al agregarlos a la Lista de usuarios haciendo clic en **Editar** junto a **Lista de usuarios**.

- **Agregar** – abre los **Tipos de objetos: Usuarios o grupos** que permite seleccionar los usuarios deseados.
- **Quitar** – quita el usuario seleccionado del filtro.

> **Limitaciones de la lista de usuarios**
> La lista de usuarios no puede definirse para reglas con tipos de dispositivos específicos:
> - Impresora USB
> - Dispositivo Bluetooth
> - Lector de tarjeta inteligente
> - Dispositivo de imagen
> - Módem
> - Puerto LPT/COM

Notificar al usuario: Si se inserta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación.

Grupos de dispositivos

⚠ El dispositivo conectado a su equipo puede presentar un riesgo de 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 respectivo, y la parte izquierda de la ventana contiene los grupos creados. Seleccione un grupo para mostrar los dispositivos en el panel derecho.

Cuando abre la ventana Grupos de dispositivos y selecciona un grupo, puede agregar o eliminar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo. Como alternativa, puede hacer clic en el botón **Llenar**, y todos los dispositivos conectados a su equipo se incluirán en una lista en la ventana **Dispositivos detectados**. Seleccione un dispositivo de la lista que se completó para agregarlo al grupo con clic en

ACEPTAR.

Elementos de control

Agregar – puede agregar un grupo si escribe su nombre o un dispositivo a un grupo existente, en función de la parte de la ventana en la que haga clic en el botón.

Editar – le permite modificar el nombre del grupo seleccionado o los parámetros del dispositivo (proveedor, modelo, número de serie).

Eliminar – elimina el grupo o el dispositivo seleccionado, dependiendo de la parte de la ventana en la que haya hecho clic en el botón.

Importar – importa una lista de dispositivos desde un archivo de texto. Para importar dispositivos desde un archivo de texto, se requiere el formato correcto:

- Cada dispositivo se inicia en una línea nueva.
- **Proveedor**, **Modelo** y **Serie** deben estar presentes para cada dispositivo y separados con una coma.

Este es un ejemplo de contenido del archivo de texto:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exportar – exporta una lista de dispositivos hacia un archivo.

El botón **Llenar** proporciona una visión general de todos los dispositivos actualmente conectados con información acerca de: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible).

Agregar dispositivo

Haga clic en **Agregar** en la ventana derecha para agregar un dispositivo a un grupo existente. A continuación, se muestran parámetros adicionales que se pueden usar para ajustar las reglas de diferentes dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor** – filtre por nombre o ID del proveedor.
- **Modelo** – el nombre determinado del dispositivo.
- **Número de serie** – los dispositivos externos generalmente tienen sus propios números de serie. En caso de un CD/DVD, este es el número de serie que corresponde al medio determinado, no a la unidad de CD.
- **Descripción**— descripción del dispositivo para una mejor organización.

Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado de los campos de texto distinguen entre mayúsculas y minúsculas y admiten comodines (un signo de interrogación [?] representa un carácter único, mientras que un asterisco [*] representa una cadena de cero o más caracteres).

Haga clic en **Aceptar** para guardar los cambios. Haga clic en **Cancelar** para salir de la ventana **Grupos de dispositivos** sin guardar los cambios.

Tras crear un grupo de dispositivos, tendrá que agregar una nueva regla de control del dispositivo para el grupo de dispositivos creado y elegir la acción que se debe tomar.

Tenga en cuenta que no todas las Acciones (permisos) están disponibles para todos los tipos de dispositivos. Las cuatro acciones están disponibles si se trata de un dispositivo de tipo almacenamiento. Para los dispositivos de no almacenamiento, solo hay tres acciones disponibles (por ejemplo, **Bloquear escritura** no está disponible para Bluetooth; por lo tanto, los dispositivos Bluetooth solo se pueden permitir, bloquear o advertir).

Protección de la cámara web

Protección de cámara web le permite ver procesos y aplicaciones que le dan acceso a la cámara web de su equipo. Se mostrará una ventana de notificación si una aplicación intenta acceder a su cámara. Puede **permitir** o **bloquear** el 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 pueden modificarse en Configuración avanzada > **Protecciones** > **Control de dispositivos** > **Protección de la cámara web**.

Si desea activar la función Protección de la cámara web en ESET Security Ultimate, active el interruptor junto a **Habilitar protección de la cámara web**.

Una vez que se habilita la protección de la cámara web, se activan las **Reglas**, lo cual le permite abrir la ventana Editor de reglas.

A fin de desactivar alertas para aplicaciones que tengan una regla modificada, pero que aún tengan una firma digital válida (por ejemplo, una actualización de la aplicación), active el interruptor junto a **Desactivar las alertas de acceso a la cámara web para las aplicaciones modificadas**.

Editor de reglas de protección de la cámara web

Esta ventana muestra las reglas existentes y permite el control de las aplicaciones y los procesos que tienen acceso a la cámara web de su equipo en base a la acción adoptada.

Están disponibles las siguientes opciones:

- **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 ilustradas
Cómo crear y modificar reglas de cámara web en ESET Security Ultimate.

ThreatSense

ThreatSense está conformada por muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también brinda protección durante las primeras horas de propagación de una nueva amenaza. Utiliza una combinación de la exploración del código, la emulación del código, las firmas genéricas y las firmas de virus que funcionan conjuntamente para mejorar en forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar simultáneamente varios flujos de datos para maximizar la eficiencia y la tasa de detección. La tecnología de ThreatSense también elimina los rootkits de forma correcta.

Las opciones de configuración del motor ThreatSense le permiten especificar varios parámetros de exploración:

- Los tipos de archivos y las extensiones que se van a explorar
- La combinación de diversos métodos de detección.
- Los niveles de desinfección, etc.

Para ingresar a la ventana de configuración, haga clic en **ThreatSense** ubicado en Configuración avanzada de cualquier módulo que use la tecnología ThreatSense (ver abajo). Diferentes situaciones de seguridad pueden requerir diferentes configuraciones. Por este motivo, ThreatSense puede configurarse en forma individual para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Exploración en estado inactivo
- Exploración en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del acceso a la Web
- Exploración del equipo

Los parámetros de ThreatSense están sumamente optimizados para cada módulo y su modificación puede afectar el funcionamiento del sistema en forma significativa. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, solo los nuevos archivos creados se exploran con estos métodos). En consecuencia, es recomendable mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos excepto para la exploración del equipo.

Objetos para explorar

Esta sección le permite definir qué componentes y archivos del equipo se explorarán en busca de infiltraciones.

Memoria operativa – explora en busca de amenazas que atacan la memoria operativa del sistema.

Sectores de inicio/UEFI: explora los sectores de inicio para detectar la presencia de virus en el Master Boot

Record. Lea más sobre UEFI en el glosario.

Archivos de correo electrónico – el programa es compatible con las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos – el programa es compatible con las siguientes extensiones, ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE entre muchas otras.

Archivos de autoextracción: los archivos de autoextracción (SFX) son los archivos que se pueden extraer a sí mismos.

Empaquetadores de tiempo de ejecución: después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el explorador puede reconocer varios tipos de empaquetadores adicionales mediante el uso de la emulación del código.

Opciones de exploración

Seleccione los métodos utilizados al explorar el sistema en busca de infiltraciones. Se encuentran disponibles las siguientes opciones:

Heurística – la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de esta tecnología radica en su capacidad de identificar software malicioso que antes no existía o que no era reconocido por la versión anterior del motor de detección. La desventaja es la probabilidad (muy reducida) de identificar falsos positivos.

Heurística avanzada/Firmas de ADN: la heurística avanzada está compuesta por un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que se crearon con lenguajes de programación de última generación. El uso de la heurística avanzada incrementa significativamente la capacidad de detección de amenazas de los productos de ESET. Las firmas tienen la capacidad de detectar e identificar los virus en forma confiable. Mediante el uso del sistema de actualizaciones automáticas, las nuevas firmas están disponibles en el transcurso de unas pocas horas tras el descubrimiento de una amenaza. La desventaja de las firmas es que solo detectan los virus que ya conocen (o las versiones ligeramente modificadas de estos virus).

Desinfección

La configuración de la desinfección determina el comportamiento de ESET Security Ultimate durante la desinfección de objetos. Existen cuatro niveles de desinfección:

ThreatSense incluye los siguientes niveles de corrección (es decir, desinfección).

Corrección ESET Security Ultimate

Nivel de desinfección	Descripción
Corregir siempre la detección	Intento de corregir la detección al limpiar objetos sin la intervención del usuario final. En algunos pocos casos (por ejemplo, en archivos de sistema), si la detección no se puede corregir, se deja al objeto informado en su ubicación original.

Nivel de desinfección	Descripción
Corregir la detección si es seguro, de lo contrario conservar	Intento de corregir la detección al desinfectar objetos sin la intervención del usuario final. En algunos casos (por ejemplo, en archivos de sistema con archivos desinfectados o infectados), si una detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario preguntar	Intento de corregir la detección al desinfectar 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). Esta configuración se recomienda en la mayoría de los casos.
Preguntar siempre al usuario final	El usuario final visualiza una ventana interactiva al desinfectar objetos y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de hallar una detección.

Exclusiones

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de ThreatSense permite definir los tipos de archivos que se van a explorar.

Otros

Cuando se configuran los parámetros del motor ThreatSense para una exploración del equipo bajo demanda, las siguientes opciones en la sección **Otros** también están disponibles:

Explorar secuencias de datos alternativas (ADS) – las secuencias de datos alternativas usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección camuflándose como secuencias de datos alternativas.

Realizar exploraciones en segundo plano con baja prioridad – cada secuencia de exploración consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para los recursos del sistema, es posible activar la exploración en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos – El Registro de la exploración mostrará todos los archivos explorados en los archivos comprimidos de autoextracción, incluidos los que no estén infectados (podría generar muchos datos de registro de exploración e incrementar el tamaño del archivo del registro de exploración).

Habilitar la optimización inteligente – cuando la opción para habilitar la optimización inteligente está seleccionada, se usa la configuración más favorable para garantizar el nivel de exploración más eficiente, al mismo tiempo que mantiene la mayor velocidad de exploración. Los diversos módulos de protección realizan exploraciones en forma inteligente; para ello emplean distintos métodos de exploración y los aplican a tipos de archivos específicos. Si se deshabilita la optimización inteligente, solo se aplica la configuración definida por el usuario en el núcleo ThreatSense de esos módulos específicos al efectuar una exploración.

Preservar el último acceso con su fecha y hora – seleccione esta opción para preservar la hora de acceso original a los archivos explorados en vez de actualizarla (por ejemplo, para usarlos con sistemas que realizan copias de seguridad de datos).

Límites

La sección Límites permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

Configuración de los objetos

Tamaño máximo del objeto – define el tamaño máximo de los objetos que se van a explorar. El módulo antivirus determinado explorará solamente los objetos con un tamaño inferior al especificado. Los únicos que deberían modificar esta opción son los usuarios avanzados que tengan motivos específicos para excluir objetos de mayor tamaño de la exploración. Valor predeterminado: ilimitado.

Tiempo máximo de exploración para el objeto (seg.): define el valor máximo de tiempo para explorar un objeto en un contenedor (como un archivo RAR/ZIP o un correo electrónico con varios adjuntos). Esta configuración no rige para archivos independientes. Si en esta opción se ingresó un valor definido por el usuario y el tiempo ha transcurrido, la exploración se detendrá lo antes posible, sin importar si finalizó la exploración de cada uno de los archivos en un objeto de contenedor.
En el caso de un archivo con varios archivos grandes, la exploración se detendrá en cuanto se extraiga un archivo (por ejemplo, cuando la variable definida por el usuario es de 3 segundos, pero la extracción de un archivo demora 5 segundos). El resto de los archivos del archivo general no se explorarán una vez que haya transcurrido esa cantidad de tiempo.
Para limitar el tiempo de exploración, incluidos los archivos más grandes, use las opciones **Tamaño máximo del objeto** y **Tamaño máximo del archivo incluido en el archivo comprimido** (no se recomienda debido a posibles riesgos para la seguridad).
Valor predeterminado: ilimitado.

Configuración de la exploración de archivos comprimidos

Nivel de anidado de archivos comprimidos – especifica la profundidad máxima de la exploración de archivos comprimidos. Valor predeterminado: 10.

Tamaño máximo del archivo incluido en el archivo comprimido – esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. El valor máximo es **3 GB**.

> No se recomienda cambiar los valores predeterminados; en circunstancias normales, no existe ninguna razón para modificarlos.

Niveles de desinfección

Para cambiar la configuración del nivel de desinfección de un módulo de protección deseado, 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 incluye los siguientes niveles de corrección (es decir, desinfección).

Corrección ESET Security Ultimate

Nivel de desinfección	Descripción
Corregir siempre la detección	Intento de corregir la detección al limpiar objetos sin la intervención del usuario final. En algunos pocos casos (por ejemplo, en archivos de sistema), si la detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario conservar	Intento de corregir la detección al desinfectar objetos sin la intervención del usuario final. En algunos casos (por ejemplo, en archivos de sistema con archivos desinfectados o infectados), si una detección no se puede corregir, se deja al objeto informado en su ubicación original.
Corregir la detección si es seguro, de lo contrario preguntar	Intento de corregir la detección al desinfectar 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). Esta configuración se recomienda en la mayoría de los casos.
Preguntar siempre al usuario final	El usuario final visualiza una ventana interactiva al desinfectar objetos y debe seleccionar una acción de corrección (por ejemplo, eliminar o ignorar). Este nivel está diseñado para los usuarios más avanzados que conocen los pasos a seguir en caso de hallar una detección.

Extensiones de archivos que no se analizarán

Las extensiones de archivo que no se analizarán forman parte de ThreatSense. Para configurar las extensiones de archivo excluidas, haga clic en **ThreatSense** de la Configuración avanzada de cualquier módulo que utilice tecnología ThreatSense.

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de ThreatSense permite definir los tipos de archivos que se van a explorar.

> No debe confundirse con Exclusiones de procesos, Exclusiones HIPS o Exclusiones de archivo/carpeta.

En forma predeterminada, se exploran todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos de la exploración.

A veces es necesario excluir ciertos tipos de archivos cuando su exploración impide el funcionamiento correcto del programa que está usando ciertas extensiones. Por ejemplo, puede ser recomendable excluir las extensiones `.edb`, `.eml` y `.tmp` al usar los servidores de Microsoft Exchange.

> Para agregar una nueva extensión a la lista, haga clic en **Agregar**. Ingrese la extensión en el campo vacío (por ejemplo, tmp) y haga clic en **Aceptar**. Cuando selecciona **Ingresar múltiples valores**, puede agregar varias extensiones de archivo delimitadas por líneas, comas, o punto y coma (por ejemplo, seleccione **Punto y coma** del 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 **Windows Explorer** > **Ver** (pestaña).

Parámetros ThreatSense adicionales

Para editar esta configuración, abra Configuración avanzada > **Protecciones** > **Protección del sistema de archivos en tiempo real** > **Parámetros ThreatSense adicionales**.

Parámetros de ThreatSense adicionales para archivos creados o modificados recientemente.

La probabilidad de infección en los archivos recién creados o modificados es comparativamente superior a la de los archivos existentes. Por este motivo, el programa comprueba estos archivos con parámetros de exploración adicionales. ESET Security Ultimate usa heurística avanzada, que puede detectar nuevas amenazas antes de que se actualice el motor de detección junto con métodos de exploración basados en firmas.

Además de los archivos recién creados, la exploración también se realiza en **Archivos comprimidos de autoextracción** (.sfx) y **Empaquetadores de tiempo de ejecución** (archivos ejecutables comprimidos internamente). De forma predeterminada, los archivos se exploran hasta el nivel 10 de anidamiento y se comprueban independientemente de su tamaño real. Para modificar la configuración de la exploración de archivos, anule la selección de la opción **Configuración predeterminada de exploración de archivos**.

Parámetros adicionales de ThreatSense para los archivos ejecutados

Heurística avanzada para la ejecución de archivos: de forma predeterminada, se utiliza la Heurística avanzada cuando se ejecutan los archivos. Cuando está habilitada, recomendamos mantener la Optimización inteligente y ESET LiveGrid® habilitados para mitigar el impacto en el rendimiento del sistema.

Heurística avanzada al ejecutar archivos de medios extraíbles: la heurística avanzada emula un código en un entorno virtual y evalúa su comportamiento antes de permitir la ejecución del código desde los medios extraíbles.

Herramientas

Puede configurar opciones avanzadas para funciones que ofrecen seguridad adicional y ayudan a simplificar la administración de ESET Security Ultimate en Configuración avanzada > **Herramientas**.

- Actualización de Microsoft Windows®
- ESET CMD
- Archivos de registro
- Modo de juego
- Diagnósticos

Actualización de Microsoft Windows®

La funcionalidad Windows Update es un componente importante para proteger a los usuarios ante software malicioso. Por ese motivo, es imprescindible instalar las actualizaciones de Microsoft Windows en cuanto estén

disponibles. ESET Security Ultimate lo mantendrá notificado sobre las actualizaciones faltantes según el nivel que haya especificado en Configuración avanzada > **Herramientas**. Se encuentran disponibles los siguientes niveles:

- **Sin actualizaciones** – no se ofrecerá la descarga de ninguna actualización del sistema.
- **Actualizaciones opcionales** – las actualizaciones marcadas como de baja prioridad y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones recomendadas** – las actualizaciones marcadas como comunes y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones importantes** – las actualizaciones marcadas como importantes y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones críticas** – solo se ofrecerá la descarga de las actualizaciones críticas.

Cuadro de diálogo: actualizaciones del sistema

Si hay actualizaciones para su sistema operativo, ESET Security Ultimate muestra una notificación en la ventana principal del programa > **Vista general**. Haga clic en **Más información** para abrir la ventana de actualizaciones del sistema.

La ventana de actualizaciones del sistema muestra la lista de actualizaciones disponibles que ya están preparadas para su descarga e instalación. El tipo de actualización aparece junto a su nombre.

Haga doble clic en cualquier fila de actualización para mostrar la ventana Actualizar información 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 sobre la actualización

La ventana de actualizaciones del sistema muestra la lista de actualizaciones disponibles que ya están preparadas para su descarga e instalación. El nivel de prioridad de la actualización aparece junto al nombre de la actualización.

Haga clic en **Ejecutar la actualización de sistema** para comenzar la descarga e instalación de las actualizaciones de sistema operativo.

Haga un clic derecho en cualquier línea de actualización y, a continuación, haga clic en **Mostrar información** para abrir una nueva ventana con información adicional.

ESET CMD

Esta es una característica que habilita los comandos avanzados ecmd. Le permite exportar e importar la configuración mediante la línea de comando (ecmd.exe). Hasta ahora, solo era posible exportar configuraciones usando la interfaz gráfica del usuario, GUI. ESET Security Ultimate la configuración puede exportarse al archivo.*xml*.

Cuando haya habilitado ESET CMD, existen dos métodos de autorización disponibles:

- **Ninguno** – sin autorización. No le recomendamos este método porque permite la importación de cualquier configuración no firmada, lo cuál es un riesgo potencial.

- **Contraseña de configuración avanzada**: se requiere una contraseña para importar una configuración de un archivo .xml, este archivo debe estar firmado (consulte la firma del archivo de configuración .xml más abajo). La contraseña especificada en Configuración de acceso se debe brindar antes de poder importar una nueva configuración. Si no tiene acceso a la configuración habilitada, su contraseña no coincide o el archivo de configuración .xml no está firmado, la configuración no se importará.

Una vez habilitado ESET CMD, puede usar la línea de comandos para exportar/importar ESET Security Ultimate configuraciones. Puede hacerlo manualmente o crear una secuencia de comandos con fines de automatización.

Para utilizar comandos avanzados de ecmd, debe ejecutarlos con privilegios de administrador o abrir el Símbolo de comandos de Windows (cmd) utilizando **Ejecutar como administrador**. Caso contrario, obtendrá el mensaje **Error executing command**. Además, al exportar una configuración, debe existir la carpeta de destino. El comando de exportar sigue funcionando cuando la configuración ESET CMD se encuentra apagada.

Exportar comando de configuración:
```
ecmd /getcfg c:\config\settings.xml
```

Importar comando de configuración:
```
ecmd /setcfg c:\config\settings.xml
```

Los comandos ecmd avanzados solo pueden ejecutarse localmente.

Firmar un archivo de configuración.*xml*:

1. Descargar el XmlSignTool ejecutable.

2. Abra el símbolo del sistema de Windows (cmd) mediante **Ejecutar como administrador**.

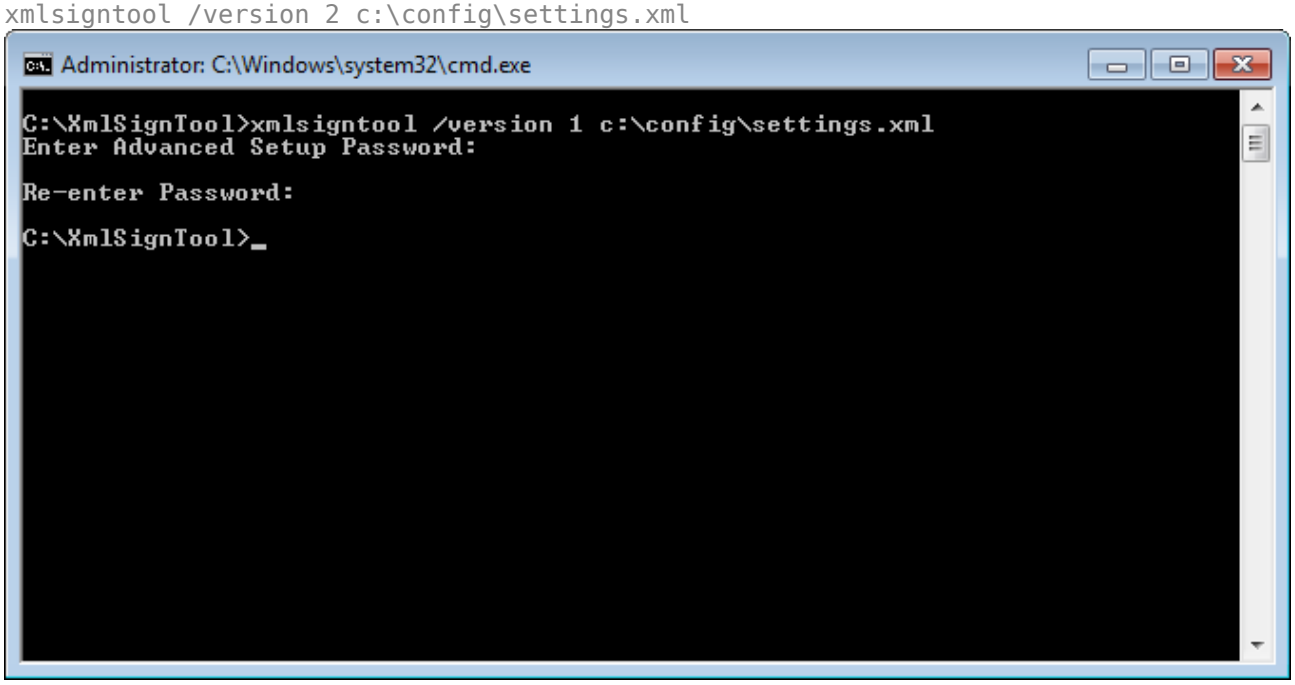
3. Navegar a la ubicación de guardar de `xmlsigntool.exe`

4. Ejecute un comando para firmar el archivo de configuración.*xml*, uso: `xmlsigntool /version 1|2 <xml_file_path>`

El valor del `/version` parámetro depende de su versión de ESET Security Ultimate. Use `/version 1` para versiones anteriores de ESET Security Ultimate que 11.1. Use `/version 2` para la versión actual de ESET Security Ultimate.

5. Ingrese y vuelva a escribir su contraseña de Configuración avanzada cuando XmlSignTool lo solicite. Su archivo de configuración.*xml* ahora se encuentra firmado y se podrá utilizar para importar en otra instancia de ESET Security Ultimate con ESET CMD utilizando el método de autorización con contraseña.

Firme el comando de archivo de configuración exportado:
`xmlsigntool /version 2 c:\config\settings.xml`



Si cambia su contraseña de la Configuración de acceso y desea importar la configuración firmada anteriormente con una contraseña antigua, necesita volver a firmar el archivo de configuración *.xml* usando la contraseña actual. Esto le permite usar un archivo de configuración anterior sin exportarlo a otro equipo que ejecute ESET Security Ultimate antes de la importación.

No se recomienda habilitar ESET CMD sin una autorización, ya que esto permitirá la importación de cualquier configuración no firmada. Establezca la contraseña en Configuración avanzada > **Interfaz de usuario** > **Configuración de acceso** para evitar las modificaciones no autorizadas de los usuarios.

Archivos de registro

Puede encontrar la configuración de registro de ESET Security Ultimate en Configuración avanzada > **Herramientas** > **Archivos de registro**. La sección Archivos de registros se usa para definir cómo se administrarán los registros. El programa elimina en forma automática los registros más antiguos para ahorrar espacio en el disco rígido. Especifique las siguientes opciones para los archivos de registro:

Nivel de detalle mínimo para los registros – especifica el nivel mínimo de detalle de los sucesos que se registrarán:

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo** – registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias** – registra los errores críticos y los mensajes de advertencia.
- **Errores** – se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico** – registra solo los errores críticos (error al iniciar la protección antivirus, Firewall, etc.).

Todas las conexiones bloqueadas se grabarán cuando seleccione el nivel de detalle Diagnóstico.

Se eliminarán automáticamente las entradas de registro anteriores a la cantidad de días especificada en el campo **Eliminar automáticamente historiales anteriores a (días)**.

Optimizar archivos de registro automáticamente: si se selecciona esta opción, se desfragmentarán automáticamente los archivos de registro si el porcentaje es mayor al valor especificado en el campo **Si la cantidad de historiales no utilizados excede X (%)**.

Haga clic en **Optimizar** para comenzar la desfragmentación de los archivos de registro. Durante este proceso, se eliminan todas las entradas de registro vacías, lo que mejora el rendimiento y la velocidad de procesamiento de los registros. Esta mejora se observa más claramente cuanto mayor es el número de entradas de los registros.

Habilitar protocolo del texto habilita el almacenamiento de los registros en otro formato de archivo distinto del de los Archivos de registro:

- **Directorio de destino**: el directorio donde se almacenarán los archivos de registro (solo se aplica a texto/CSV). Cada sección de registro tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, virlog.txt para la sección de archivos de registro **Detecciones**, si usa un formato de archivo de texto sin formato 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 tabulaciones. Lo mismo se aplica para el formato del archivo **CSV** separado por comas. Si elige **Evento**, los registros se almacenarán en el registro Windows Event (se puede ver mediante el Visor de eventos en el Panel de control) en lugar del archivo.

- **Eliminar todos los archivos de registro** – borra todos los registros almacenados seleccionados actualmente en el menú desplegable **Tipo**. Se mostrará una notificación acerca de la eliminación correcta de los registros.

Para ayudar a resolver los problemas más rápidamente, ESET le puede solicitar que proporcione los registros de su equipo. El ESET Log Collector le facilita la recopilación de la información necesaria. Para obtener más información acerca del ESET Log Collector, visite nuestro artículo de la Base de conocimiento de ESET.

Modo de juego

El modo de juego es una característica para los usuarios que requieren utilizar el software en forma ininterrumpida, que no desean que las ventanas de alerta y notificaciones los molesten y que quieren minimizar el uso de la CPU. El modo de juego también se puede utilizar durante las presentaciones que la actividad del programa antivirus no puede interrumpir. Al habilitar esta característica, todas las ventanas emergentes se deshabilitan y la actividad de las tareas programadas se detiene por completo. La protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

Puede habilitar o deshabilitar el Modo de juego en la ventana principal del programa en **Configuración** > **Protección del equipo** con un clic en  o  junto a **Modo de juego**. Habilitar el Modo de juego constituye un riesgo potencial para la seguridad; por ese motivo, el ícono de estado de protección ubicado en la barra de tareas se pondrá naranja y mostrará una advertencia. Esta advertencia también aparecerá en la ventana principal del programa, donde aparecerá en naranja el **Modo de juego activo**.

Active **Habilitar el modo de juego al ejecutar aplicaciones en modo de pantalla completa automáticamente** en Configuración avanzada > **Herramientas** > **Modo de juego** para que este modo inicie cada vez que inicie una aplicación en pantalla completa y se detenga después de salir de la aplicación.

Active **Deshabilitar el modo de juego automáticamente después** para definir el tiempo que debe transcurrir para que el modo de juego se deshabilite automáticamente.

Si el firewall está en el modo interactivo y el modo de juego se encuentra habilitado, quizá surjan inconvenientes para conectarse a Internet. Esto puede ocasionar problemas si comienza un juego que se conecta a Internet. Bajo circunstancias normales, el programa le solicitaría que confirme dicha acción (si no se definió ninguna regla o excepción para la comunicación); pero en el modo de juego, la interacción del usuario está deshabilitada. Para permitir la comunicación, defina una regla para cualquiera de las aplicaciones que puedan presentar este problema o use un Modo de filtrado diferente en el Firewall. Recuerde que, si el modo de juego está habilitado, al intentar abrir una página o aplicación que constituya un riesgo para la seguridad, es posible que se bloquee sin que aparezca ninguna explicación o advertencia, ya que la interacción con el usuario está deshabilitada.

Diagnósticos

Los diagnósticos proporcionan el volcado de memoria de los procesos de ESET (por ejemplo, ekrn). Si una aplicación se bloquea, se generará un volcado. Esto puede ayudar a los desarrolladores a depurar y reparar distintos problemas ESET Security Ultimate.

Haga clic en el menú desplegable junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Deshabilitar** para deshabilitar esta característica.

- **Mini** (predeterminado): registra el grupo de datos útiles más reducido posible que pueda ayudar a identificar por qué se bloqueó la aplicación en forma inesperada. Este tipo de archivo de volcado puede ser útil cuando el espacio sea limitado. Sin embargo, debido a la cantidad limitada de información incluida, es posible que los errores que no se hayan provocado directamente por el subproceso activo en el momento del problema no se descubran al analizar este archivo.

- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene inesperadamente. Un volcado de memoria completa puede incluir datos de los procesos que estaban activos cuando se recopiló la memoria de volcado.

Directorio de destino – ubicación donde se va a generar la volcado de memoria durante el bloqueo.

Abrir carpeta de diagnósticos: haga clic en **Abrir** para abrir este directorio dentro de una nueva ventana 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 registro avanzado en mensajes de marketing: registrar todos los eventos relacionados con los mensajes de marketing del producto.

Habilitar el registro avanzado del motor Antispam: registra todos los eventos que ocurren durante el análisis antispam. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados al motor de Antispam de ESET.

Habilitar el registro avanzado del motor Anti-Theft: registra todos los eventos que ocurren en Anti-Theft para permitir el diagnóstico y la resolución de problemas.

Habilitar el registro avanzado de protección del navegador: registre todos los eventos que se producen en Banca y navegación seguras.

Habilitar el registro avanzado de exploración: registra todos los eventos que tienen lugar durante la exploración de archivos y carpetas mediante la exploración del equipo.

Habilitar el registro avanzado del control parental: registra todos los eventos que ocurren en Control del dispositivo. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados al control del dispositivo.

Habilitar el registro avanzado de Direct Cloud: registra todos los eventos que ocurren en ESET LiveGrid®. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con ESET LiveGrid®.

Habilitar el registro avanzado de protección de documentos: graba todos los eventos que ocurren en la protección de documentos para diagnosticar y solucionar problemas.

Activar registro avanzado de 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.

Habilitar el registro avanzado de ESET LiveGuard: registra todos los eventos que ocurren en ESET LiveGuard para permitir el diagnóstico y la resolución de problemas.

Activar registro avanzado del núcleo: registra todos los eventos que tienen lugar en el núcleo de ESET (ekrn).

Habilitar el registro avanzado de licencias: registra todas las comunicaciones del producto con la activación de ESET o los servidores de ESET License Manager.

Habilitar seguimiento de memoria: registra todos los eventos que ayudarán a los desarrolladores a diagnosticar pérdidas de memoria.

Habilitar el registro avanzado del Firewall: registra todos los datos de red que pasan a través del firewall en formato PCAP para ayudar a que los desarrolladores diagnostiquen y corrijan problemas relacionados con el firewall.

Activar registro avanzado del explorador del tráfico de red: registra todos los datos que pasan a través del explorador del tráfico de red en el formato PCAP para ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el explorador del tráfico de red.

Habilitar el registro avanzado de sistemas operativos: registra información adicional acerca del sistema operativo, como los procesos en ejecución, actividad del CPU y operaciones de disco. Esto puede ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el producto ESET ejecutado en su sistema operativo.

Habilitar el registro avanzado del control parental: registra todos los eventos que ocurren durante el control parental. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados al control

parental.

Activar registro avanzado de la mensajería push: registrar todos los sucesos que tienen lugar durante la mensajería push.

Habilitar el registro avanzado de protección del sistema de archivos en tiempo real: registra todos los eventos que tienen lugar durante la exploración de archivos y carpetas mediante la protección del sistema de archivos en tiempo real.

Habilitar el registro avanzado del motor de actualización: registra todos los eventos que ocurren durante el proceso de actualización. Esto puede ayudar a los desarrolladores a diagnosticar y solucionar problemas relacionados con el motor de actualizaciones.

Los archivos de registro se encuentran en *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Soporte técnico

Al ponerse en contacto con el soporte técnico de ESET desde ESET Security Ultimate, puede enviar datos de configuración del sistema. Seleccione **Enviar siempre** desde el menú desplegable **Enviar datos de configuración del sistema** para enviar los datos automáticamente, o bien, seleccione **Preguntar antes de enviar** para que se le solicite el envío antes de que se envíen los datos.

Conectividad

En redes específicas, la comunicación entre su equipo e Internet puede tener como intermediario un servidor proxy. Si está utilizando un servidor proxy, debe definir la siguiente configuración. De lo contrario, ESET Security Ultimate y sus módulos no se pueden actualizar automáticamente. En ESET Security Ultimate, la configuración del servidor proxy está disponible en dos secciones diferentes de la Configuración avanzada.

La configuración global del servidor proxy puede establecerse en Configuración avanzada > **Conectividad** > **Servidor proxy**. La especificación del servidor proxy en esta etapa define la configuración global del servidor proxy para todo ESET Security Ultimate. Todos los módulos que requieran una conexión a Internet utilizarán los parámetros aquí ingresados.

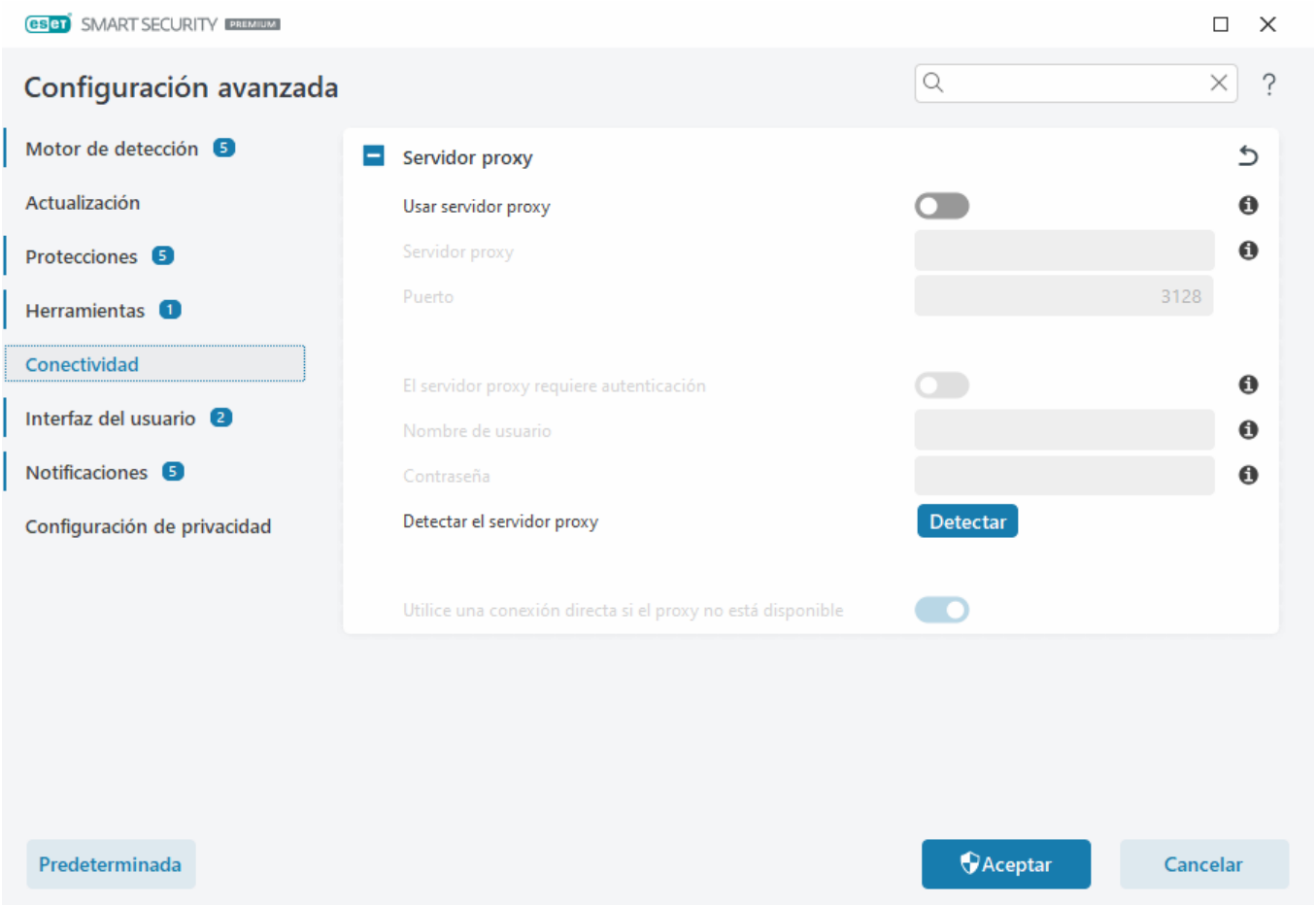
Para especificar la configuración global del servidor proxy, habilite **Usar servidor proxy** y escriba la dirección del **servidor proxy** junto con el número de **puerto** del servidor proxy.

Si la comunicación con el servidor proxy requiere autenticación, seleccione **El servidor proxy requiere autenticación** e ingrese 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 Security Ultimate copiará los parámetros especificados en Opciones de Internet para Internet Explorer o Google Chrome.

> En la configuración del **Servidor proxy**, debe ingresar su Nombre de usuario y Contraseña en forma manual.

Use conexión directa si el proxy no está disponible – Si ESET Security Ultimate está configurado para usar proxy y no puede llegar al proxy, ESET Security Ultimate evadirá el proxy y se comunicará directamente con los servidores ESET.

La configuración del servidor proxy también puede configurarse en Configuración avanzada > **Actualizar** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** seleccionando **Conexión a través de un servidor proxy** del menú desplegable **Modo de proxy**. Esta configuración se aplica solo para actualizaciones y se recomienda para equipos portátiles que reciben actualizaciones de módulos desde ubicaciones remotas. Para obtener más información, consulte Configuración avanzada de actualizaciones.



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 y los efectos visuales del programa en la pantalla Configuración avanzada de los elementos de la interfaz del usuario.

Si desea disfrutar del máximo nivel de seguridad del software de seguridad, proteja la configuración con una contraseña para impedir la desinstalación o cualquier cambio no autorizado con la herramienta Configuración de acceso.

> Para configurar el comportamiento de las notificaciones del sistema, las alertas de detección y los estados de la aplicación, consulte la sección Notificaciones.

Elementos de la interfaz del usuario

Puede ajustar el entorno de trabajo (GUI) de ESET Security Ultimate según sus necesidades en Configuración avanzada > **Interfaz del usuario** > **Elementos de la interfaz del usuario**.

Modo de color— seleccione el esquema de colores de la GUI de ESET Security Ultimate en el menú desplegable:

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

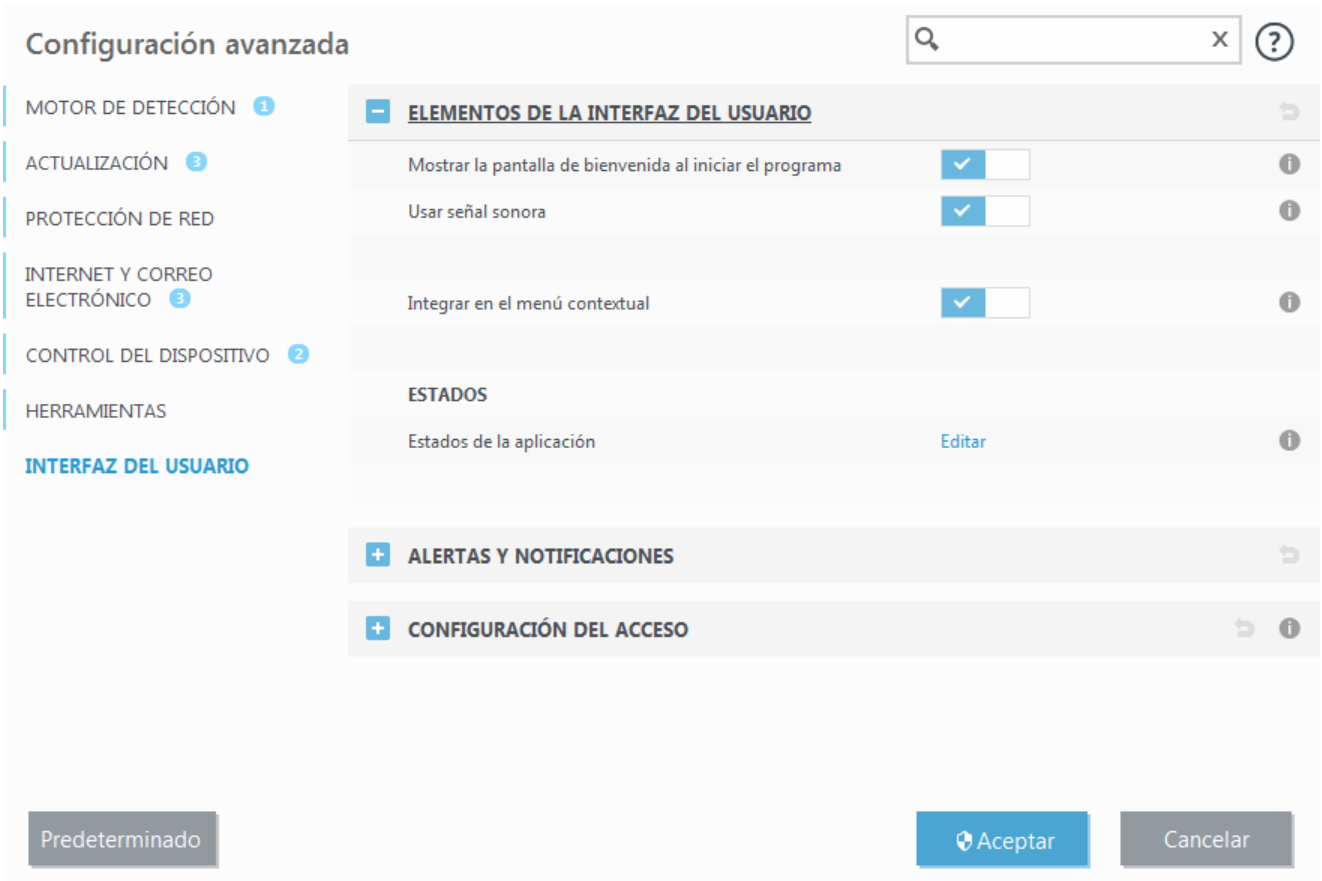
> También puede seleccionar el esquema de colores de la interfaz gráfica de usuario de ESET Security Ultimate en la esquina superior derecha de la ventana principal del programa.

Mostrar la pantalla de bienvenida al iniciar el programa – muestra la pantalla de bienvenida de ESET Security Ultimate durante el inicio.

Usar señal acústica: reproduce un sonido cuando se producen eventos importantes durante una exploración, por ejemplo al detectar una amenaza o al finalizar la exploración.

Fondo transparente— habilita 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 – integrar los elementos de control de ESET Security Ultimate al menú contextual.



Configuración del acceso

Las configuraciones ESET Security Ultimate son una parte crucial de su política de seguridad. Las modificaciones no autorizadas pueden poner potencialmente en peligro la estabilidad y la protección del sistema. Para evitar modificaciones no autorizadas, los parámetros de configuración y la desinstalación de ESET Security Ultimate pueden protegerse con una contraseña. La configuración de acceso se puede configurar en Configuración avanzada > **Interfaz del usuario** > **Configuración de acceso**.

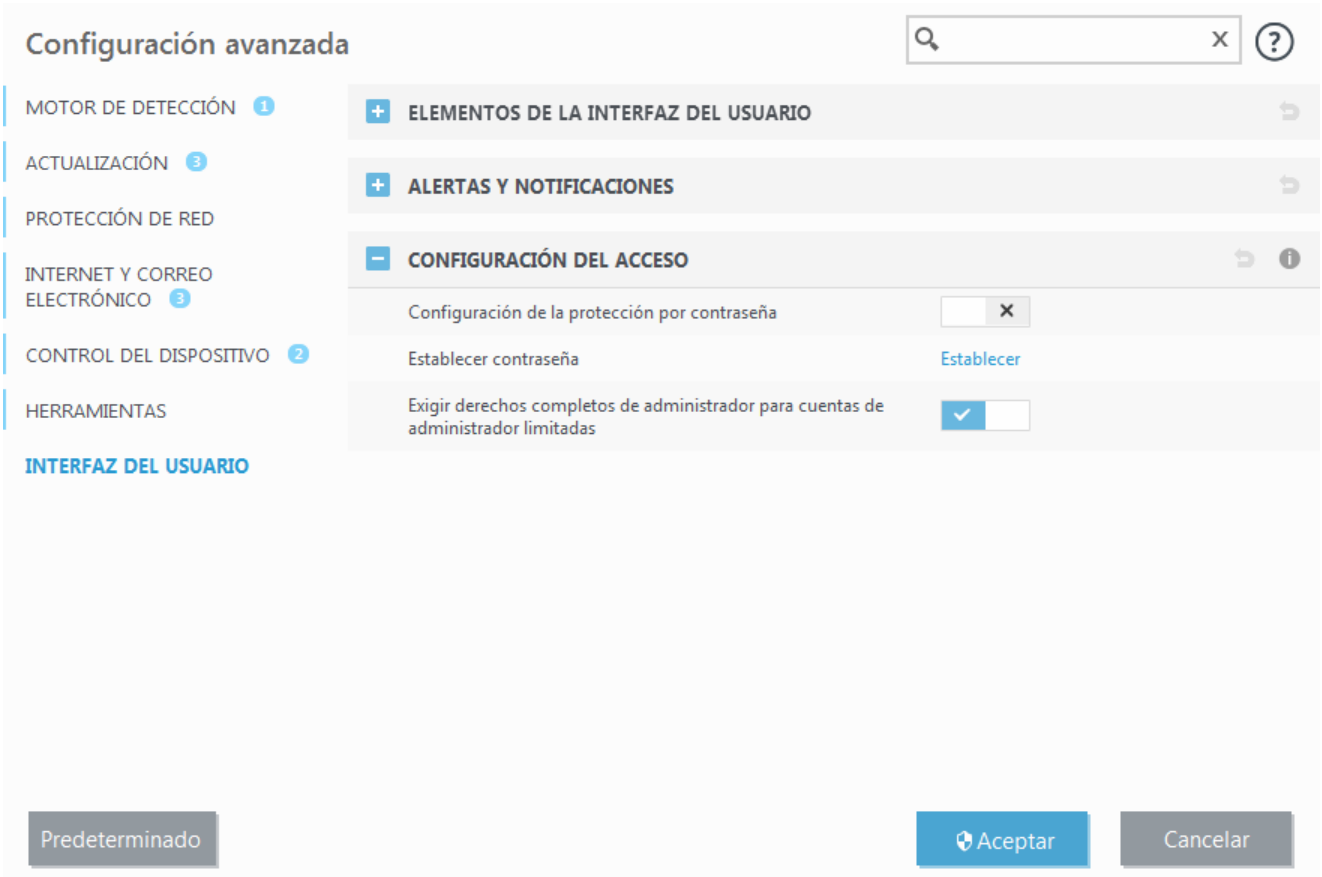
Para establecer una contraseña para proteger los parámetros de configuración y desinstalación de ESET Security Ultimate, haga clic en **Establecer** junto a **Proteger la configuración con una contraseña**.

Cuando quiera acceder a la Configuración avanzada protegida, aparecerá la ventana para escribir la contraseña. Si no la recuerda o la pierde, haga clic en la opción **Restaurar contraseña** a continuación y escriba la dirección de correo electrónico que utilizó para el registro de la suscripción. ESET le enviará un correo electrónico con el código de verificación y las instrucciones acerca de cómo restablecer su contraseña.

- Cómo desbloquear la configuración avanzada

Para cambiar la contraseña, haga clic en **Cambiar contraseña** junto a **Proteger la configuración con una contraseña**.

Para quitar la contraseña, haga clic en **Quitar** junto a **Proteger la configuración con una contraseña**.



Contraseña para configuración avanzada

Para proteger la Configuración avanzada de ESET Security Ultimate y evitar modificaciones no autorizadas, ingrese su nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**. Haga clic en **Aceptar**.

Cuando desee cambiar una contraseña existente:

1. Escriba su contraseña anterior en el campo **Contraseña anterior**.
2. Ingrese su nueva contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**.
3. Haga clic en **Aceptar**.

Esta contraseña será necesaria para acceder a Configuración avanzada.

Si olvidó su contraseña, consulte Desbloquear su contraseña de configuración en productos para hogar de ESET.

Para recuperar la clave de activación de ESET perdida, la fecha de vencimiento de su suscripción u otra información de suscripción para ESET Security Ultimate, consulte Perdí mi clave de activación.

Asistencia para lectores de pantalla

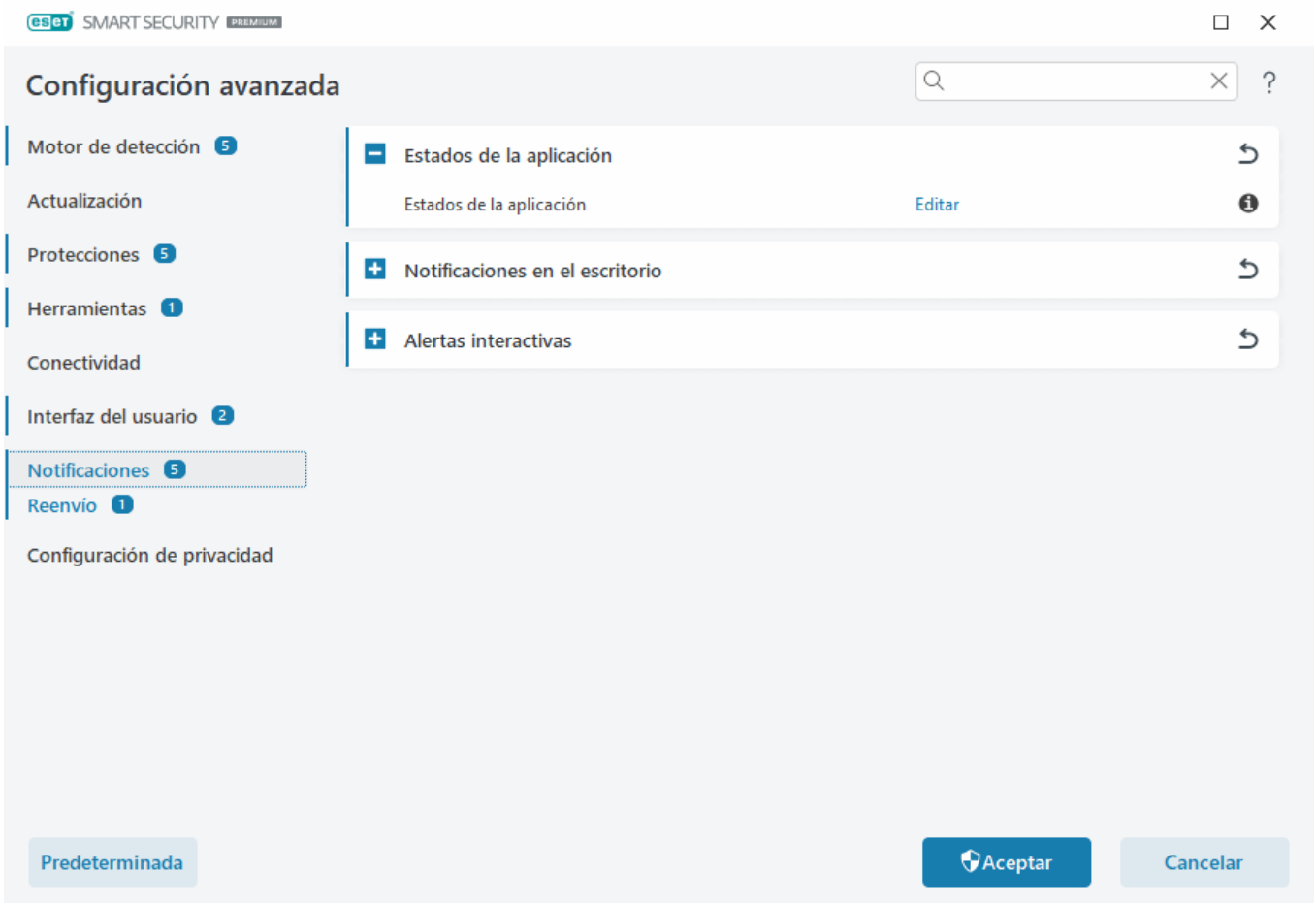
ESET Security Ultimate puede utilizarse junto con los lectores de pantalla para permitir que los usuarios de ESET con visión deficiente naveguen en el producto o configuren los ajustes. Los siguientes son los lectores de pantalla compatibles (JAWS, NVDA, Narrator).

Para garantizar que el software lector de pantalla pueda acceder a la GUI ESET Security Ultimate correctamente, siga las instrucciones en el Artículo de nuestra base de conocimiento.

Notificaciones

Para administrar las notificaciones de ESET Security Ultimate, abra Configuración avanzada > **Notificaciones**. Puede configurar los siguientes tipos de notificaciones:

- Estados de la aplicación – notificaciones que se muestran en la ventana principal del programa > **Vista 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 **Modificar** para seleccionar los estados de la aplicación que se mostrarán en la sección de inicio de la ventana principal del programa > **Vista general**.

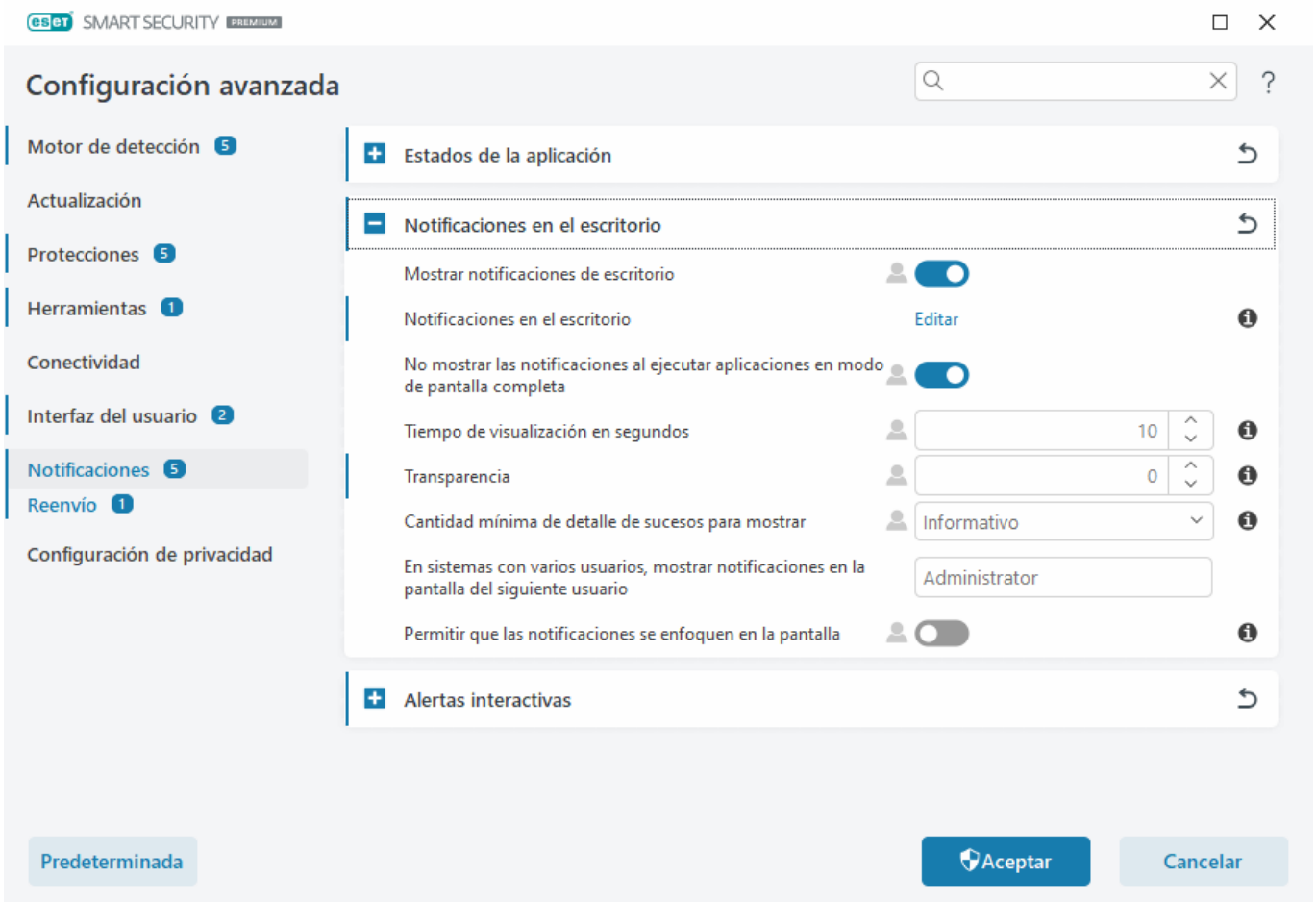
Ventana de diálogo: estados de la aplicación

En este cuadro de diálogo, puede seleccionar los estados de aplicación que se mostrarán. Por ejemplo, cuando pone en pausa la protección antivirus y antispyware o activa el modo de juego.

El estado de la aplicación también se mostrará si su producto no está activado o si la suscripción ha vencido.

Notificaciones en el escritorio

Las notificaciones en el escritorio se representan mediante una pequeña ventana de notificación 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, conexión de nuevos dispositivos, finalización de tareas de análisis de virus o nuevas amenazas encontradas.



Mostrar notificaciones en el escritorio: recomendamos mantener esta opción activada, para que el producto pueda informarle cuando ocurra un suceso nuevo.

Notificaciones en el escritorio: haga clic en **Editar** para activar o desactivar las Notificaciones en el escritorio específicas.

No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa: elimina todas las notificaciones que no son interactivas al ejecutar aplicaciones en modo de pantalla completa.

Tiempo de visualización en segundos: defina la duración de visibilidad de la notificación. El valor debe estar entre 3 y 30 segundos.

Transparencia: defina 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 eventos a mostrar: defina 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 historiales antes mencionados.
- **Informativo** – muestra los mensajes de información, como los eventos de red no estándar, que incluyen los mensajes de actualizaciones correctas, y todos los registros antes mencionados.
- **Advertencias:** muestra mensajes de advertencia, errores y errores graves (por ejemplo, falló la actualización).

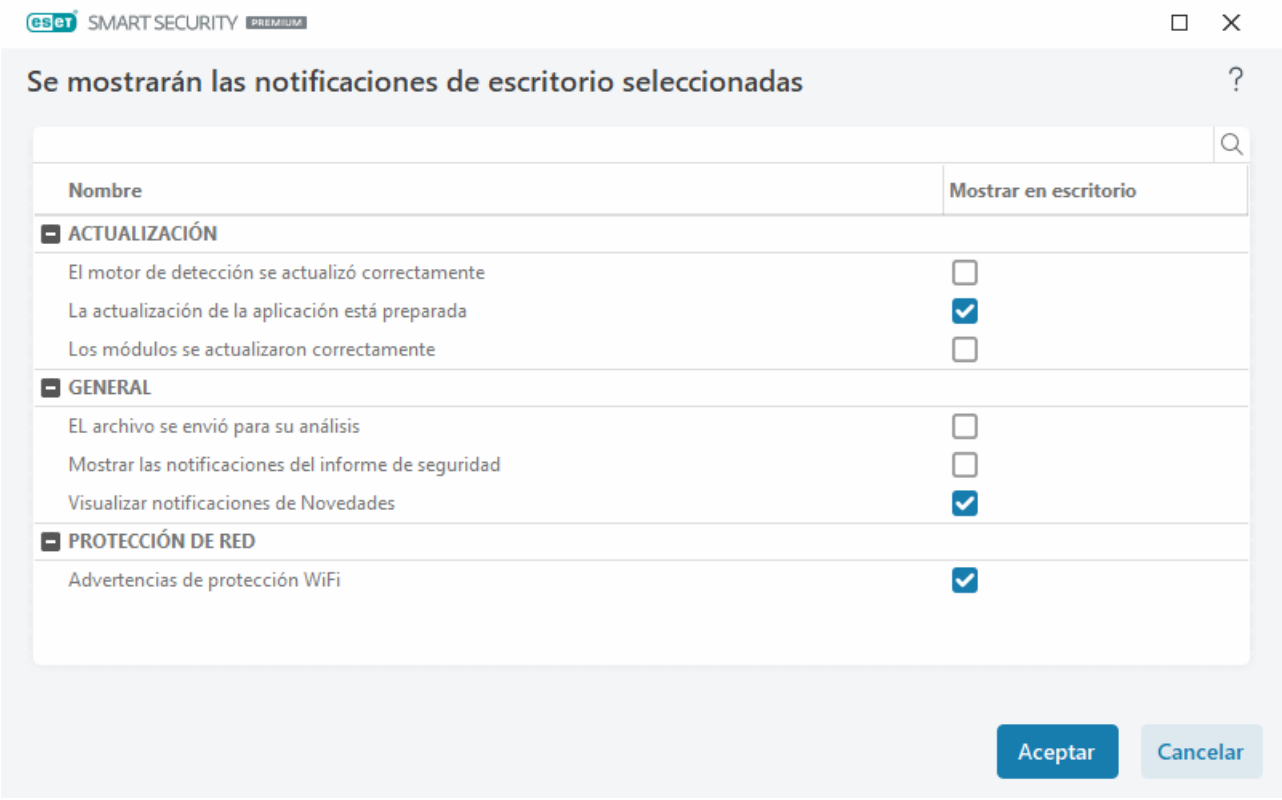
- **Errores:** muestra errores (por ejemplo, la protección de documentos no iniciada) y errores graves.
- **Crítico:** muestra solo los errores críticos (error al iniciar la protección antivirus o sistema infectado, etc.).

En sistemas con varios usuarios, mostrar notificaciones en la pantalla de este usuario: permite que la cuenta seleccionada reciba notificaciones en el escritorio. Por ejemplo, si no utiliza la cuenta de administrador, escriba el nombre completo de la cuenta y se mostrarán las notificaciones en el escritorio de la cuenta especificada. Solo puede recibir notificaciones en el escritorio una cuenta de usuario.

Permitir que las notificaciones se enfoquen en la pantalla: permite que las notificaciones se enfoquen en la pantalla; se puede acceder a esta opción 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 la Configuración avanzada > **Notificaciones** > **Notificaciones en el escritorio**. Haga clic en **Modificar** junto a **Notificaciones en el escritorio** y marque la casilla de verificación **Mostrar** correspondiente.



General

Mostrar las notificaciones del informe de seguridad: reciba una notificación cuando se genera un nuevo Informe de seguridad.

Mostrar las notificaciones de novedades: notificaciones sobre todas las características nuevas y mejoradas de la versión más reciente del producto.

El archivo se ha enviado para su análisis: reciba una notificación cada vez que ESET Security Ultimate envía un archivo para su análisis.

Inspector de red

Notificar sobre dispositivos de red recién descubiertos: 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: recibe una notificación al intentar conectarse a una red Wi-Fi con una contraseña débil o sin contraseña.

Actualización

Se prepara la actualización de la aplicación: reciba una notificación cuando haya una actualización de una nueva versión de ESET Security Ultimate preparada.

El Motor de detección se ha actualizado correctamente: reciba una notificación cuando el producto actualiza los módulos del Motor de detección.

Los módulos se han actualizado correctamente: reciba una notificación cuando el producto actualiza los componentes del programa.

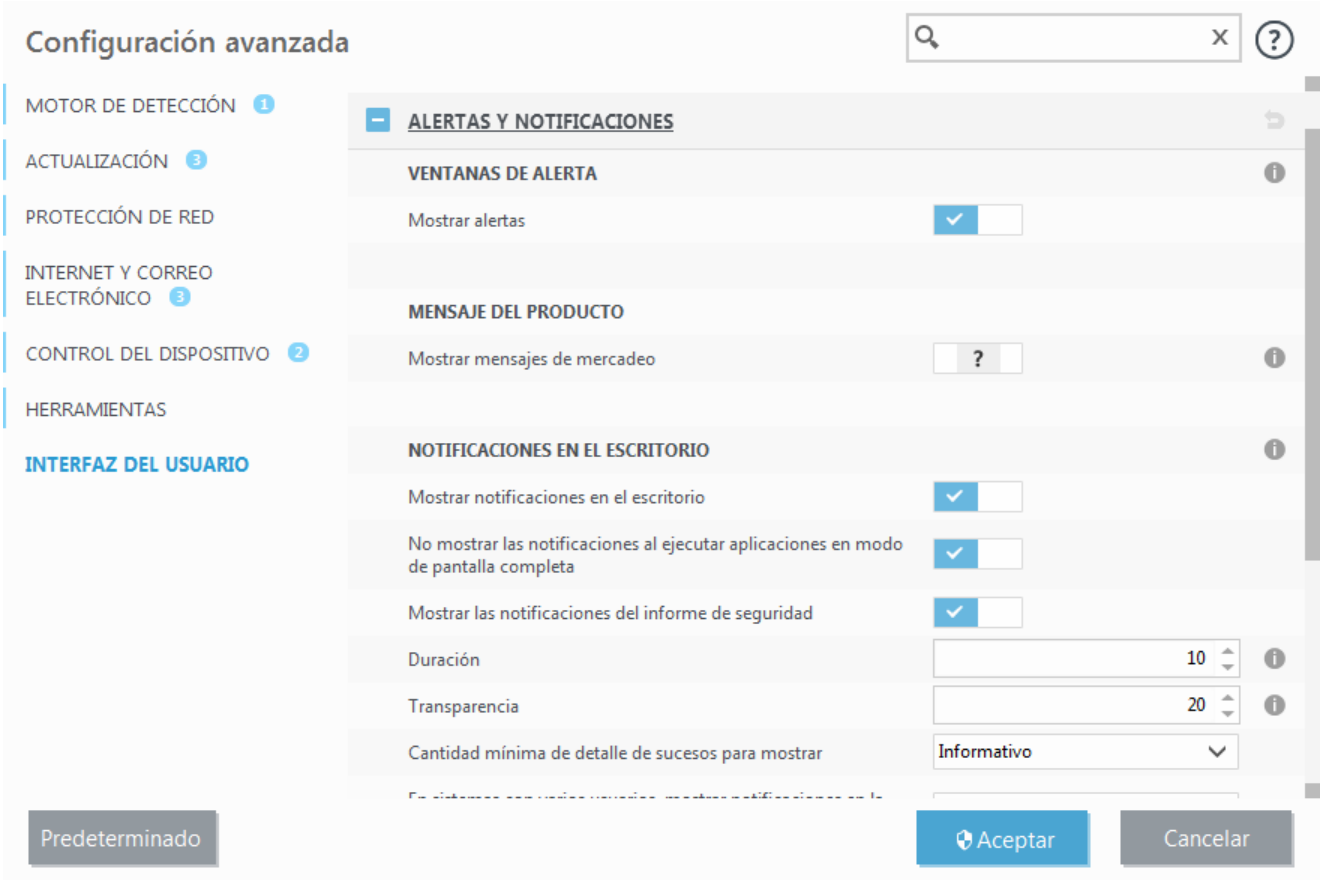
Para definir las configuraciones generales de las notificaciones de escritorio, por ejemplo, durante cuánto tiempo se mostrará un mensaje o la cantidad mínima de detalles para mostrar de los sucesos, consulte Notificaciones de escritorio en Configuración avanzada > **Notificaciones**.

Alertas interactivas

¿Necesita información sobre alertas y notificaciones comunes?

- Amenaza detectada
- La dirección se ha bloqueado
- Producto no activado
- Cambiar a un producto con más funciones
- Cambiar a un producto con menos funciones
- Está disponible la actualización
- La información sobre la actualización no es consistente
- Resolución de problemas para el mensaje «error de actualización de módulos»
- Resolver errores de actualización de módulos
- Se bloqueó una amenaza de red
- Certificado de sitio web revocado

La sección **Alertas interactivas** de Configuración avanzada > **Notificaciones** le permite configurar cómo gestiona ESET Security Ultimate los cuadros de mensajes y las alertas interactivas para detecciones (por ejemplo, un sitio web potencial de phishing) cuando un usuario debe tomar una decisión.



Alertas interactivas

Si desactiva la opción **Mostrar alertas interactivas**, se ocultarán todas las ventanas de alerta y los cuadros de diálogo del navegador. Solo es adecuado para una serie de situaciones muy específicas. Recomendamos mantener esta opción activada.

Mensajería del producto

La mensajería del producto ha sido diseñada para informar a los usuarios de ESET acerca de noticias y otras comunicaciones. El envío de mensajes de marketing requiere el consentimiento de un usuario. Los mensajes de marketing no se envían a un usuario de forma predeterminada (se muestra como un signo de interrogación). Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no está interesado en recibir material de marketing de ESET, desactive la opción **Mostrar mensajes de marketing**.

Cuadros de mensajes

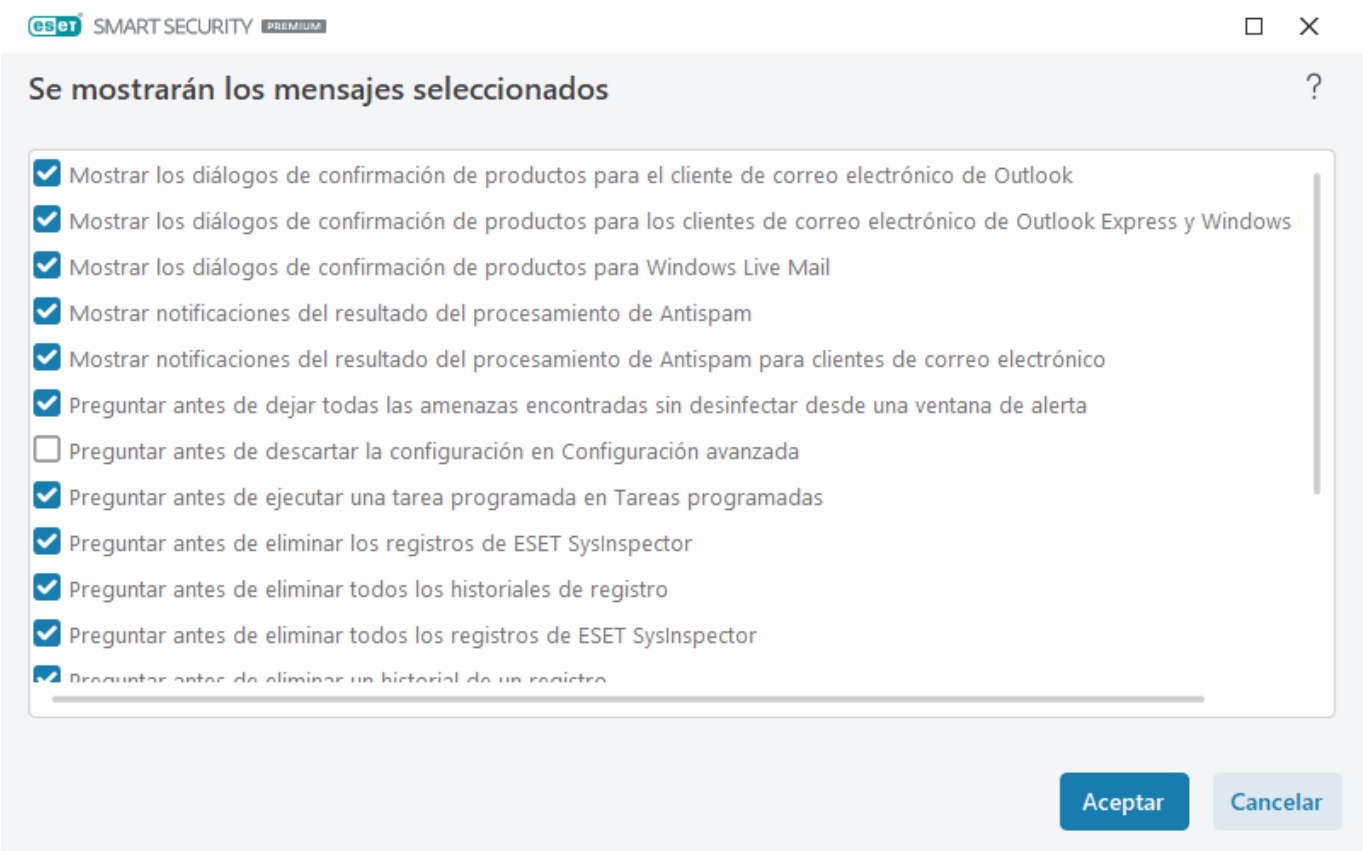
Para cerrar las casillas de mensajes automáticamente después de un período de tiempo determinado, seleccione **Cerrar cuadros de mensajes automáticamente**. Si no se cierran manualmente, las ventanas de alerta se cerrarán automáticamente una vez que transcurra el tiempo especificado.

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 **Modificar** para mostrar 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 la Configuración avanzada > **Notificaciones** > **Alertas interactivas** y haga clic en **Modificar** junto a **Mensajes de confirmación**.



Esta ventana de diálogo muestra mensajes de confirmación que ESET Security Ultimate mostrará antes de que se realice alguna acción. Seleccione o anule la selección de la casilla de verificación junto a cada mensaje de confirmación para permitirlo o deshabilitarlo.

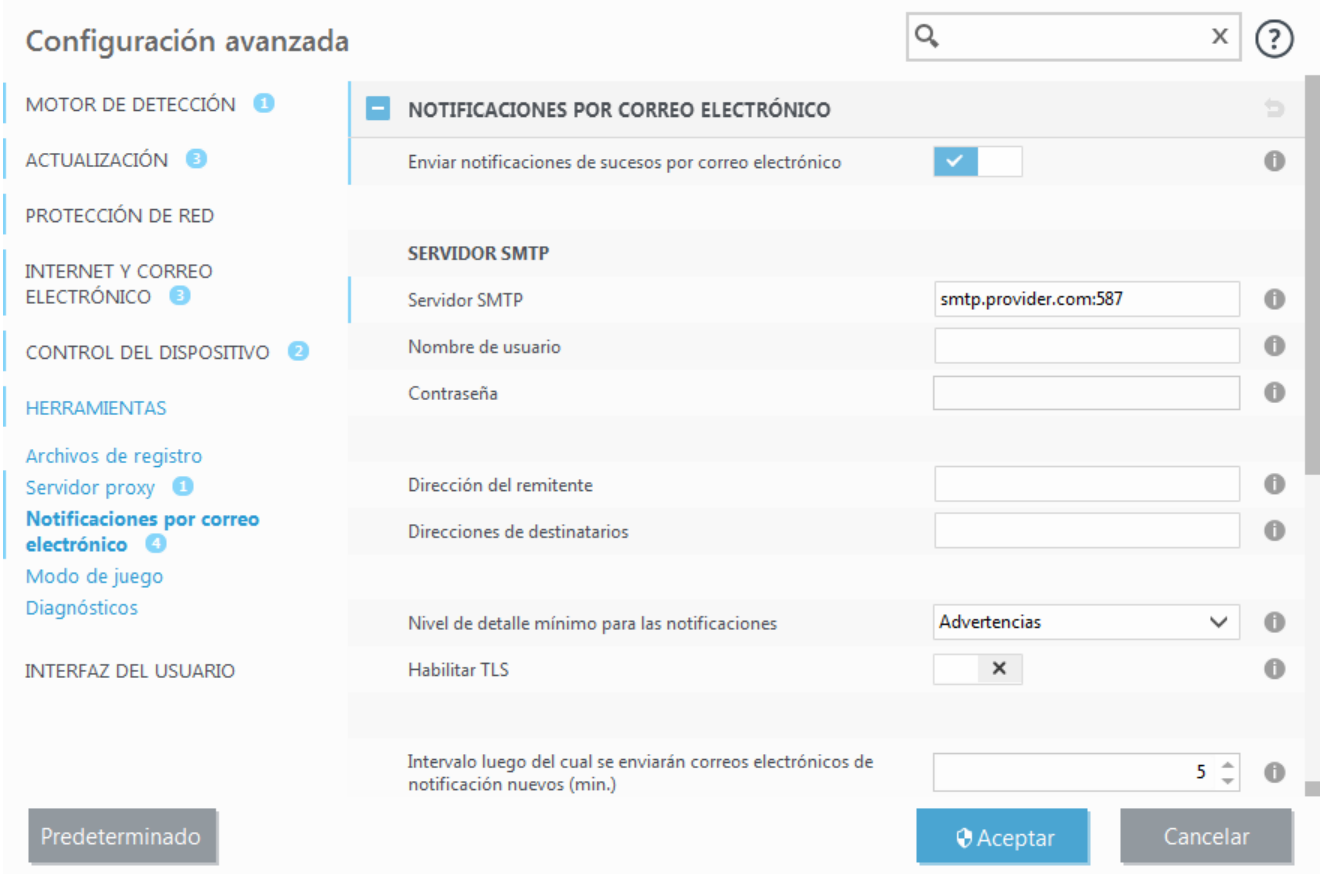
Obtenga más información sobre la función específica relacionada con los mensajes de confirmación:

- Preguntar antes de eliminar ESET SysInspectorregistros
- Preguntar antes de eliminar todos los ESET SysInspectorregistros
- Preguntar antes de eliminar un objeto de cuarentena
- Preguntar antes de descartar la configuración en Configuración avanzada
- Preguntar antes de dejar todas las amenazas encontradas sin desinfectar desde una ventana de alerta
- Preguntar antes de eliminar un historial de un registro
- Preguntar antes de eliminar una tarea programada en Tareas programadas
- 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 de la exploración
- Preguntar antes de ejecutar una tarea programada en Tareas programadas
- Mostrar notificaciones del resultado del procesamiento de Antispam
- Mostrar notificaciones del resultado del procesamiento de Antispam para clientes de correo electrónico
- Mostrar cuadros de diálogo de confirmación del producto para los clientes de correo electrónico de 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 de Outlook

Reenvío

ESET Security Ultimate puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Abra la Configuración avanzada **Notificaciones** > **Reenviar** y habilite la opción **Reenviar notificaciones al correo electrónico** para activar las notificaciones por correo electrónico.



En el menú desplegable **Nivel de detalle mínimo para las notificaciones**, puede seleccionar el nivel de gravedad a partir del cual se enviarán las notificaciones.

- **Diagnóstico** – registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.

• **Informativo** – registra los mensajes de información, como los eventos de red no estándar, que incluyen los mensajes de actualizaciones correctas, y todos los registros antes mencionados.

• **Advertencias:** registra los errores críticos y los mensajes de advertencia (por ejemplo, falló la actualización).

• **Errores** – se registrarán los errores (no se inició la protección de documentos) y los errores críticos.

• **Crítico**: registra únicamente los errores graves (por ejemplo, Error al iniciar la protección antivirus o Amenaza encontrada).

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 provocar que muchos mensajes de correo electrónico se reciban en un breve periodo de tiempo.

Intervalo luego del cual se enviarán correos electrónicos de notificación nuevos (min.) – intervalo en minutos luego del cual se enviarán notificaciones nuevas al correo electrónico. Si establece este valor en 0, las notificaciones se enviarán inmediatamente.

Dirección del remitente – define la dirección del remitente que se mostrará en el encabezado de los correos electrónicos de notificación.

Direcciones de destinatarios: defina las direcciones de destinatarios mostradas en el encabezado de los mensajes de correo electrónico de notificación. Se admiten varios valores. Utilice punto y coma como separador.

Servidor SMTP

SMTP servidor: el SMTP servidor utilizado para enviar notificaciones (p. ej., smtp.provider.com:587, el puerto predeterminado es 25).

Los servidores SMTP con cifrado TLS son admitidos por ESET Security Ultimate.

Nombre de usuario y **contraseña** – si el servidor SMTP requiere autenticación, se deben completar estos campos con un nombre de usuario y una contraseña válidos para acceder 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 electrónico del destinatario. Se debe completar el servidor SMTP, el nombre de usuario, la contraseña, la dirección del remitente y las direcciones del destinatario.

Formato de mensajes

Las comunicaciones entre el programa y el usuario remoto o el administrador del sistema se llevan a cabo por medio de los correos electrónicos o los mensajes de la LAN (mediante el servicio de mensajería de Windows). El **formato predeterminado** de las notificaciones y los mensajes de alerta será óptimo para la mayoría de las situaciones. En ciertas circunstancias, es posible que necesite cambiar el formato de los mensajes de sucesos.

Formato de mensajes de sucesos – formato de los mensajes de sucesos que se muestran en los equipos remotos.

Formato de mensajes de advertencias sobre amenazas: los mensajes de notificación y alerta de amenazas tienen

un formato predefinido de forma predeterminada. Recomendamos mantener el formato predefinido. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba cambiar el formato de los mensajes.

Conjunto de caracteres – convierte un mensaje de correo electrónico en una codificación de caracteres ANSI en base a la configuración regional de Windows (por ejemplo, windows-1250, Unicode (UTF-8), ACSII 7-bit, o japonés (ISO-2022-JP)). Por lo tanto, "á" se cambiará por "a" y un símbolo desconocido por "?".

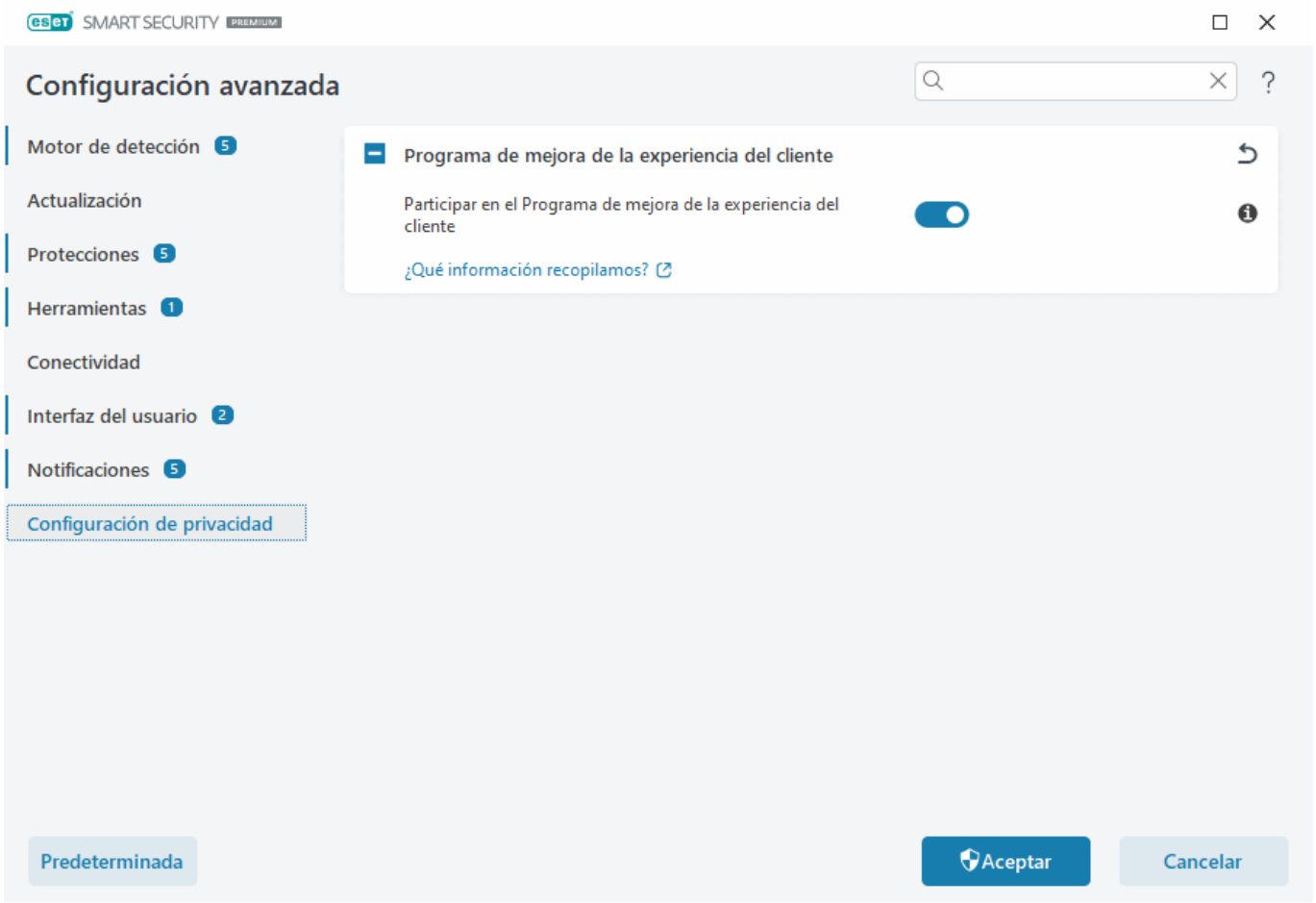
Usar la codificación de Entrecomillado imprimible: el origen del mensaje de correo electrónico se codificará en el formato Entrecomillado imprimible ((QP)) que usa los caracteres de ASCII y puede transmitir correctamente los caracteres nacionales especiales por correo electrónico en el formato de 8 bits (áéíóú).

- **%TimeStamp%**: fecha y la hora del suceso
- **%Scanner%**: módulo pertinente
- **%ComputerName%**: nombre del equipo en el que se produjo la alerta
- **%ProgramName%**: programa que generó la alerta
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectados.
- **%VirusName%**: identificación de la infección
- **%Action%** : Acción tomada sobre la infiltración
- **%ErrorDescription%**: descripción de un suceso no causado por un virus

Las palabras clave **%InfectedObject%** y **%VirusName%** no solo se utilizan en mensajes de alerta de amenazas, y **%ErrorDescription%** solo se utiliza en mensajes de sucesos.

Configuración de privacidad

Abra Configuración avanzada > **Configuración de privacidad**.



Programa de mejora de la experiencia del cliente

Active el interruptor junto a **Participar en el Programa de mejora de la experiencia del cliente** para unirse al Programa de mejora de la experiencia del cliente. Al unirse, le proporcionará a ESET información anónima relativa al uso de productos de ESET. Los datos recopilados nos ayudarán a mejorar su experiencia y nunca se compartirán con terceros. ¿Qué información recopilamos?

Revertir a la configuración predeterminada

En **Configuración avanzada**, haga clic en Predeterminada para revertir toda la configuración del programa para todos los módulos. Se restablecerá el estado que tendrían después de una nueva instalación.

Consulte también Importar y exportar configuración.

Restauración de todas las configuraciones en la sección actual

Haga clic en la flecha curva para restaurar todas las configuraciones de la sección actual a los valores predeterminados definidos por ESET.

Tenga en cuenta que cualquier cambio que se haya hecho se perderá después de hacer clic en **Revertir a predeterminado**.

Restaurar el contenido de las tablas – cuando se habilitan, las reglas, las tareas o los perfiles que se hayan agregado de manera manual o automática se perderán.

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.

Por lo general, esto significa que el usuario que intentó modificar los parámetros del programa:

- tiene derechos de acceso insuficientes o no tiene los privilegios del sistema operativo necesarios para modificar los archivos de configuración y el registro del sistema.
  > Para realizar las modificaciones deseadas, el administrador del sistema debe iniciar sesión.

- recientemente habilitó el Modo de aprendizaje en HIPS o Firewall e intentó hacer cambios en Configuración avanzada.
  > Para guardar la configuración y evitar el conflicto de configuración, cierre Configuración avanzada sin guardar y vuelva a intentar hacer los cambios deseados.

La segunda causa más común puede ser que el programa ya no funcione correctamente, que esté dañado y que deba reinstalarse.

Exploración de la línea de comandos.

El módulo antivirus de ESET Security Ultimate se puede iniciar mediante una línea de comandos; ya sea en forma manual (con el comando “ecls”) o con un archivo de procesamiento por lotes (“bat”).

Uso del módulo de exploración de la línea de comandos de ESET:

```
ecls [OPTIONS..] FILES..
```

Se pueden usar los siguientes parámetros y modificadores desde la línea de comandos durante la ejecución del módulo de exploración bajo demanda:

Opciones

/base-dir=CARPETA	cargar módulos desde FOLDER
/quar-dir=CARPETA	FOLDER de cuarentena
/exclude=MÁSCARA	excluir de la exploración los archivos que coinciden con MASK
/subdir	explorar las subcarpetas (predeterminado)
/no-subdir	no explorar las subcarpetas
/max-subdir-level=NIVEL	subnivel máximo de carpetas dentro de las carpetas que se van a explorar
/symlink	seguir los vínculos simbólicos (predeterminado)
/no-symlink	saltear los vínculos simbólicos
/ads	explorar ADS (predeterminado)
/no-ads	no explorar ADS

/log-file=ARCHIVO	registrar salida en FILE
/log-rewrite	sobrescribir archivo de salida (predeterminado: añadir)
/log-console	registrar resultados en la consola (predeterminado)
/no-log-console	no registrar resultados en la consola
/log-all	también incluir en el registro los archivos no infectados
/no-log-all	no registrar los archivos no infectados (predeterminado)
/aind	mostrar indicador de actividad
/auto	explorar y desinfectar todos los discos locales automáticamente

Opciones del módulo de exploración

/files	explorar los archivos (predeterminado)
/no-files	no explorar los archivos
/memory	explorar la memoria
/boots	explorar los sectores de inicio
/no-boots	no explorar los sectores de inicio (predeterminado)
/arch	explorar los archivos comprimidos (predeterminado)
/no-arch	no explorar los archivos comprimidos
/max-obj-size=TAMAÑO	solo explorar los archivos menores que SIZE megabytes (predeterminado 0 = ilimitado)
/max-arch-level=NIVEL	subnivel máximo de archivos comprimidos dentro de los archivos comprimidos (anidados) que se van a explorar
/scan-timeout=LÍMITE	explorar los archivos comprimidos durante LIMIT segundos como máximo
/max-arch-size=TAMAÑO	solo explorar los archivos en un archivo comprimido si son menores que SIZE (predeterminado 0 = ilimitado)
/max-sfx-size=TAMAÑO	solo explorar archivos dentro de un archivo comprimido de autoextracción si son menores que SIZE megabytes (predeterminado 0 = ilimitado)
/mail	explorar los archivos de correo electrónico (predeterminado)
/no-mail	no explorar los archivos de correo electrónico
/mailbox	explorar los buzones de correo (predeterminado)
/no-mailbox	no explorar los buzones de correo
/sfx	explorar los archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no explorar los archivos comprimidos de autoextracción
/rtp	explorar los empaquetadores de tiempo de ejecución (predeterminado)
/no-rtp	no explorar los empaquetadores de tiempo de ejecución
/unsafe	explorar en búsqueda de aplicaciones potencialmente no seguras
/no-unsafe	no explorar en búsqueda de aplicaciones potencialmente no seguras (predeterminado)
/unwanted	explorar en búsqueda de aplicaciones potencialmente no deseadas
/no-unwanted	no explorar en búsqueda de aplicaciones potencialmente no deseadas (predeterminado)
/suspicious	explorar en busca de aplicaciones sospechosas (predeterminado)

/no-suspicious	no explorar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	habilitar la heurística (predeterminado)
/no-heur	deshabilitar la heurística
/adv-heur	habilitar la heurística avanzada (predeterminado)
/no-adv-heur	deshabilitar la heurística avanzada
/ext-exclude=EXTENSIONES	excluir de la exploración las EXTENSIONES de archivos delimitadas por dos puntos
/clean-mode=MODO	usar el MODO de desinfección para objetos infectados Se encuentran disponibles las siguientes opciones: • `none` (predeterminado): no se realizará desinfección automática alguna. • `standard`: ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados. • `estricta`: ecls.exe intentará desinfectar o eliminar en forma automática los archivos infectados sin la intervención del usuario (no se le notificará antes de que se eliminen los archivos). • `rigurosa`: ecls.exe eliminará los archivos sin intentar desinfectarlos, independientemente de qué archivo sea. • `eliminar`: ecls.exe eliminará los archivos sin intentar desinfectarlos, pero se abstendrá de eliminar los archivos importantes, como los archivos del sistema de Windows.
/quarantine	copiar los archivos infectados (si fueron desinfectados) a cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar los archivos infectados a cuarentena

Opciones generales

/help	mostrar la ayuda y salir
/version	mostrar información de la versión y salir
/preserve-time	preservar el último acceso con su fecha y hora

Códigos de salida

0	no se detectó ninguna amenaza
1	se detectó una amenaza y se desinfectó
10	algunos archivos no se pudieron explorar (pueden ser amenazas)
50	amenaza detectada
100	error

Los códigos de salida mayores que 100 significan que el archivo no se exploró, por lo que puede estar infectado.

Preguntas frecuentes

A continuación, encontrará algunas de las preguntas más frecuentes y los problemas más comunes. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

- Cómo actualizar ESET Security Ultimate
- ESET Security Ultimate ha detectado una amenaza
- Cómo quitar un virus del equipo
- Cómo permitir la comunicación para una aplicación específica
- Cómo habilitar el control parental en una cuenta
- Cómo crear una nueva tarea en Tareas programadas
- Cómo programar una tarea de exploración (semanal)
- Cómo desbloquear la configuración avanzada
- Cómo resolver la desactivación del producto desde ESET HOME

Si su problema no está incluido en la lista anterior, intente buscar en la Ayuda en línea de ESET Security Ultimate.

Si no encuentra una solución a su problema o pregunta en la Ayuda en línea de ESET Security Ultimate, puede visitar nuestra Base de conocimiento de ESET, la cual se actualiza regularmente. A continuación, se incluyen vínculos a nuestros artículos de la base de conocimiento más populares:

- ¿Cómo renovar mi suscripción?
- Recibí un error de activación mientras se instalaba el producto de ESET. ¿Qué significa esto?
- Activar mi producto hogareño de ESET Windows con la clave de activación
- Desinstalar o volver a instalar mi producto hogareño de ESET
- Recibo el mensaje de que mi instalación de ESET finalizó de manera prematura
- ¿Qué necesito hacer luego de renovar mi suscripción? (Usuarios locales)
- ¿Qué sucede si cambio mi dirección de correo electrónico?
- Transferir mi producto ESET a un nuevo equipo o dispositivo
- Cómo iniciar Windows en Modo seguro o Modo seguro con conexión de red
- Impedir que se bloquee un sitio web seguro
- Permita que el software de los lectores de pantalla acceda a la GUI de ESET

En caso de ser necesario, también puede ponerse en contacto con Soporte técnico para consultar sus preguntas o problemas.

Cómo actualizar ESET Security Ultimate

La actualización de ESET Security Ultimate se puede realizar en forma manual o automática. Para iniciar la actualización, haga clic en **Actualizar** en la ventana del programa principal y luego haga clic en **Comprobar si hay actualizaciones**.

La configuración predeterminada de la instalación crea una tarea de actualización automática que se ejecuta a cada hora. Si necesita cambiar dicho intervalo, vaya a **Herramientas** > Tareas programadas.

Cómo quitar un virus del equipo

Si su equipo muestra síntomas de infección por malware; por ejemplo, funciona más lento o con frecuencia no responde, se recomienda hacer lo siguiente:

1. Desde la ventana principal del programa, haga clic en **Exploración del equipo**.

2. Haga clic en **Explorar el equipo** para iniciar la exploración del sistema.

3. Una vez finalizada la exploración, consulte el registro con la cantidad de archivos explorados, infectados y desinfectados.

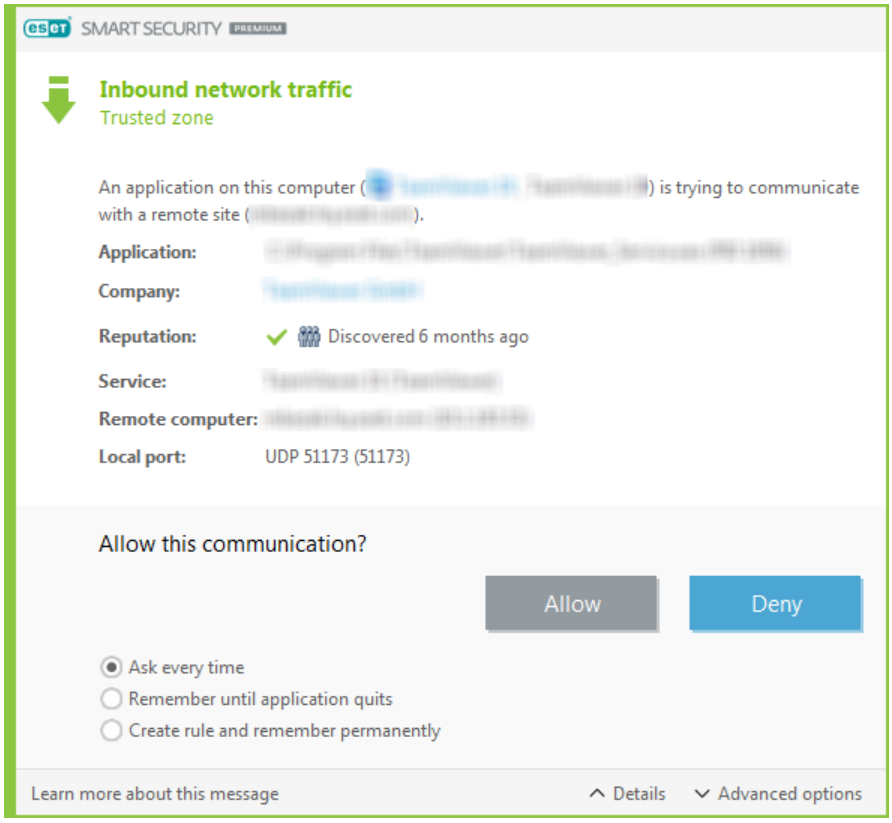
4. Si solo quiere explorar una parte seleccionada del disco, haga clic en **Exploración personalizada** y seleccione los objetos para explorar en busca de virus.

Para obtener más información, consulte:

- Artículo de la base de conocimiento de ESET
- Cuarentena

Cómo permitir la comunicación para una aplicación específica

Si se detecta una nueva conexión en el modo interactivo y no hay ninguna regla coincidente, el programa le solicitará que **permita** o **deniegue** la conexión. Si desea que ESET Security Ultimate realice la misma acción cada vez que la aplicación intente establecer una conexión, seleccione la casilla de verificación **Crear regla y recordar permanentemente**.



En la configuración del firewall puede crear nuevas reglas de firewall para las aplicaciones antes de que las detecte ESET Security Ultimate. Abra la ventana principal del programa > **Configuración** > **Protección de red** > haga clic en junto a **Firewall** > **Configurar** > **Avanzado** > **Reglas** > **Editar**.

Haga clic en el botón **Agregar** y en la pestaña **General**, ingrese el nombre, la dirección y el protocolo de comunicación para la regla. Esta ventana permite definir la acción que se tomará cuando se aplique la regla.

Ingrese la ruta al archivo ejecutable de la aplicación y el puerto de comunicación local en la pestaña **Local**. Haga clic en la pestaña **Remoto** para ingresar la dirección y el puerto remotos (de ser necesario). La nueva regla creada se aplicará en cuanto la aplicación vuelva a intentar comunicarse.

Cómo habilitar el control parental en una cuenta

Para activar el control parental en una cuenta de usuario específica, siga los pasos a continuación:

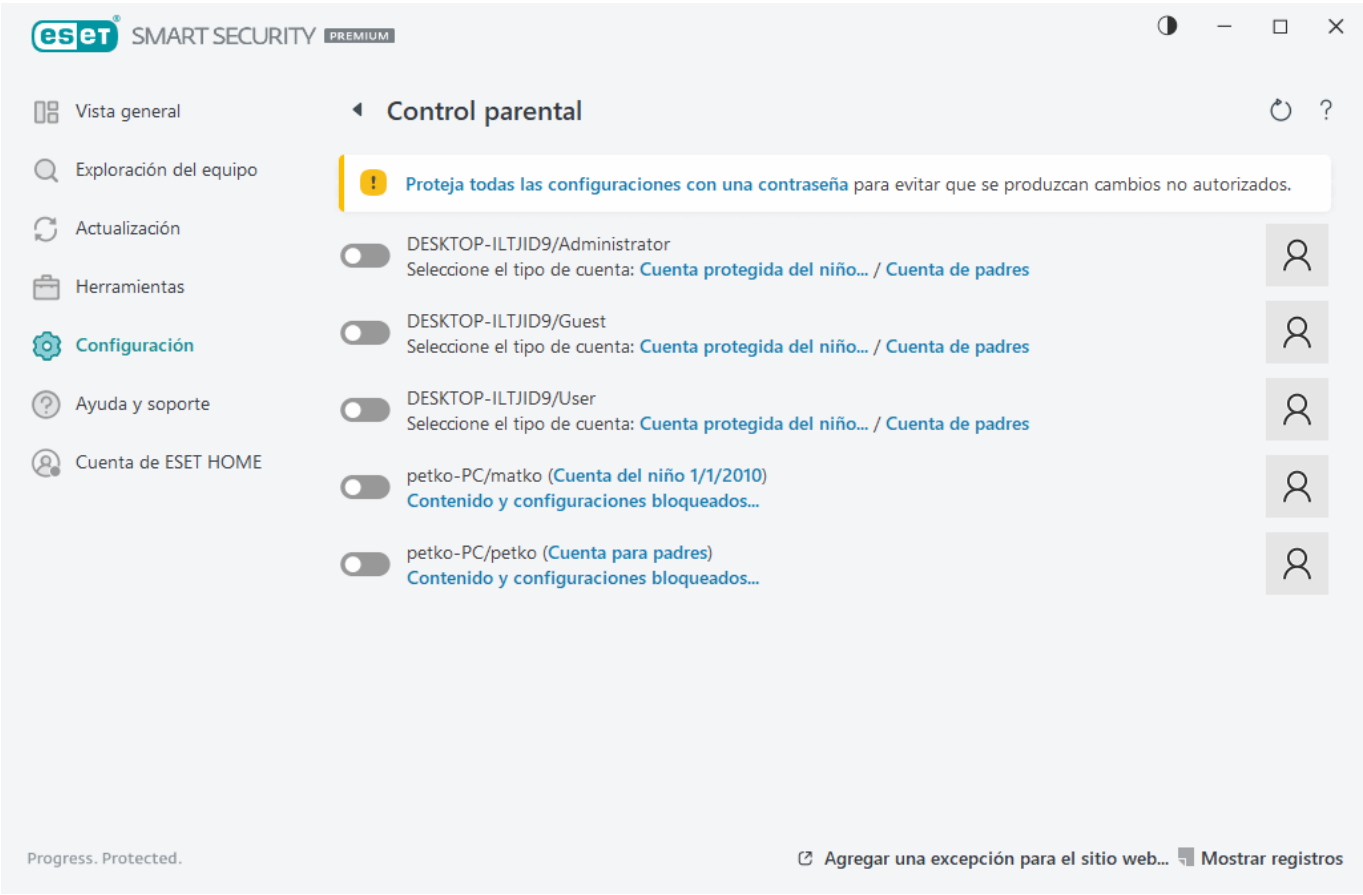
1. De manera predeterminada, el control parental está deshabilitado en ESET Security Ultimate. Existen dos métodos para activar el Control parental:

   • Haga clic en el ícono interruptor en **Configuración** > **Protección de internet** > **Control parental** de la ventana principal del programa y cambie el estado del Control parental a habilitado.

   • Abra Configuración avanzada > **Protecciones** > **Protección de acceso a la web** > **Control parental** y, a continuación, habilite el interruptor junto a **Habilitar control parental**.

2. Haga clic en **Configuración** > **Protección de internet** > **Control parental** de la ventana principal del programa. Incluso si aparece **Habilitado** junto al **Control parental**, debe configurar ese control para la cuenta deseada; para ello, haga clic en el símbolo de la flecha y luego, en la siguiente ventana, debe seleccionar **Proteger cuenta para niños** o **Cuenta primaria**. En la siguiente ventana, seleccione la fecha de nacimiento

para determinar el nivel de acceso y las páginas web recomendadas para la edad. El Control parental ahora estará habilitado para la cuenta especificada del usuario. Haga clic en **Contenido y configuración bloqueados** debajo del nombre de la cuenta para personalizar las categorías que desea permitir o bloquear en la pestaña Categorías. Para permitir o bloquear páginas web personalizadas que no coincidan con ninguna categoría, haga clic en la pestaña Excepciones.



Cómo crear una nueva tarea en Tareas programadas

Para crear una nueva tarea en **Herramientas** > **Tareas programadas**, haga clic en **Agregar tarea** o haga clic derecho y seleccione **Agregar** en el menú contextual. Hay cinco tipos de tareas programadas disponibles:

- **Ejecutar aplicación externa** – programa la ejecución de una aplicación externa.
- **Mantenimiento de registros** – los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.
- **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.
- **Crear una instantánea de estado del equipo**: crea una instantánea del equipo de ESET SysInspector, que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Exploración del equipo a pedido**: realiza una exploración del equipo de los archivos y las carpetas de su equipo.

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

Dado que la **Actualización** es una de las tareas programadas de uso frecuente, a continuación se explicará cómo agregar una nueva tarea de actualización.

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Ingrese el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Se encuentran disponibles las siguientes opciones: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**. Seleccione **Omitir tarea al ejecutar con alimentación de la batería** para reducir los recursos del sistema mientras un equipo portátil se ejecuta con alimentación de la batería. La tarea se ejecutará en la fecha y hora especificadas en los campos de **Ejecución de la tarea**. A continuación, defina la acción a tomar en caso de que la tarea no se pueda realizar o completar a la hora programada. Se encuentran disponibles las siguientes opciones:

- **A la próxima hora programada**
- **Lo antes posible**
- **Inmediatamente, si el tiempo desde la última ejecución excede un valor específico** (el intervalo se puede definir con el uso del cuadro de desplazamiento del **Tiempo desde la última ejecución [horas]**)

En el siguiente paso, se muestra una ventana de resumen con información acerca de la tarea actual programada. Haga clic en **Finalizar** cuando haya terminado de realizar los cambios.

Aparecerá una ventana de diálogo desde donde se le permite seleccionar los perfiles que se usarán para la tarea programada. Aquí puede configurar el perfil principal y el alternativo. El perfil alternativo se utiliza si la tarea no se puede completar con el perfil principal. Confirme haciendo clic en **Finalizar** y la nueva tarea programada se agregará a la lista de tareas actualmente programadas.

Cómo programar una exploración semanal del equipo

Para programar una tarea de rutina, abra la ventana principal del programa y haga clic en **Herramientas** > **Tareas programadas**. La siguiente guía le indicará cómo programar una tarea que explorará sus unidades locales todas las semanas. Lea nuestro artículo de la base de conocimiento para obtener instrucciones más detalladas.

Para programar una tarea de exploración:

1. Haga clic en **Agregar** en la pantalla principal de Tareas programadas.

2. Escriba un nombre para la tarea y seleccione **Exploración del equipo a pedido** desde el menú desplegable **Tipo de tarea**.

3. Seleccione **Semanalmente** para establecer la frecuencia.

4. Configure el día y la hora en que se ejecutará la tarea.

5. Seleccione **Ejecutar la tarea lo antes posible** para realizar la tarea más tarde en caso de que su ejecución no se haya iniciado por algún motivo (por ejemplo, porque el equipo estaba apagado).

6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.

7. En el menú desplegable **Destino**, seleccione **Unidades locales**.

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

Cómo desbloquear la configuración avanzada protegida por contraseña

Cuando quiera acceder a la Configuración avanzada protegida, aparecerá la ventana para escribir la contraseña. Si no la recuerda o la pierde, haga clic en **Restaurar contraseña** y escriba la dirección de correo electrónico que usó para el registro de la suscripción. ESET le enviará un correo electrónico con el código de verificación. Escriba el código de verificación y luego ingrese y confirme la nueva contraseña. El código de verificación tiene una validez de siete días.

Restaurar la contraseña a través de su cuenta ESET HOME: use esta opción si la suscripción que se usa para la activación está asociada a su cuenta ESET HOME. Escriba la dirección de correo electrónico que usa para iniciar sesión en su cuenta ESET HOME.

Si no recuerda su dirección de correo electrónico o tiene dificultades para restablecer la contraseña, haga clic en **Ponerse en contacto con el servicio de soporte técnico**. Se lo redirigirá al sitio web de ESET para que se ponga en contacto con nuestro Departamento de Soporte Técnico.

Generar código para soporte técnico: esta opción generará un código para Soporte Técnico. Copie el código proporcionado por Soporte Técnico y haga clic en **Tengo un código de verificación**. Escriba el código de verificación y, a continuación, ingrese 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 hogareños de Windows ESET.

Cómo resolver la desactivación del producto desde ESET HOME

Producto no activado

Este mensaje de error aparece cuando el propietario de la suscripción desactiva ESET Security Ultimate desde el portal ESET HOME o la suscripción compartida con su cuenta ESET HOME ya no se ha compartido. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Security Ultimate.
- Póngase en contacto con el propietario de la suscripción si tiene información de que el propietario de la suscripción ha desactivado su ESET Security Ultimate o que ya no se comparte la suscripción 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 ESET HOME. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Security Ultimate.

- Póngase en contacto con el propietario de la suscripción si tiene información de que se ha desactivado su ESET Security Ultimate y 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 actividades de ESET HOME. Si encuentra alguna actividad sospechosa, cambie la contraseña de su cuenta 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 ESET HOME. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Security Ultimate.

- Póngase en contacto con el propietario de la suscripción si tiene información de que se ha desactivado su ESET Security Ultimate y 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 actividades de ESET HOME. Si encuentra alguna actividad sospechosa, cambie la contraseña de su cuenta ESET HOME y póngase en contacto con el servicio de soporte técnico de ESET.

Producto no activado

Este mensaje de error aparece cuando el propietario de la suscripción desactiva ESET Security Ultimate desde el portal ESET HOME o la suscripción compartida con su cuenta ESET HOME ya no se ha compartido. Para resolver este problema:

- Haga clic en **Activar** y utilice uno de los Métodos de activación para activar ESET Security Ultimate.

- Póngase en contacto con el propietario de la suscripción si tiene información de que el propietario de la suscripción ha desactivado su ESET Security Ultimate o que ya no se comparte la suscripción con usted. El propietario puede resolver el problema en ESET HOME.

0

Programa de mejora de la experiencia del cliente

Al unirse a nuestro Programa de mejora de la experiencia del cliente, usted le provee a ESET información anónima relacionada con el uso de nuestros productos. Para obtener más información sobre el procesamiento de datos, consulte nuestra Política de privacidad.

Su consentimiento

La participación en el Programa es voluntaria y se basa en su consentimiento. Luego de unirse, la participación es pasiva, lo que significa que no se requiere ninguna acción de su parte. Usted podrá revocar su consentimiento al modificar la configuración del producto cuando lo desee. Al hacerlo, evitará que sigamos procesando sus datos anónimos.

Puede revocar su consentimiento en cualquier momento al cambiar la configuración del producto:

- Cambie la configuración del Programa de mejora de la experiencia del cliente en los productos hogareños de ESET Windows

¿Qué tipo de información recolectamos?

Datos de la interacción con el producto

Estos datos nos informan sobre cómo se utilizan nuestros productos. Gracias a esto sabemos, por ejemplo, cuáles funcionalidades se utilizan frecuentemente, qué configuraciones modifican los usuarios o cuánto tiempo pasan utilizando nuestros productos.

Datos acerca de dispositivos

Recopilamos esta información para comprender en qué dispositivos y dónde se utilizan nuestros productos. Algunos ejemplos típicos son el modelo de dispositivo, el país, la versión y el nombre del sistema operativo.

Datos de diagnóstico de errores

También se recopilan datos acerca del error y de la situación de la falla. Por ejemplo, qué error se ha producido y qué acciones derivaron en él.

¿Por qué recopilamos esta información?

Estos datos anónimos nos hacen posible mejorar nuestros productos para usted, el usuario. Además, nos ayudan a convertirlos en más relevantes, fáciles de usar y sin fallas como sea posible.

¿Quién controla esta información?

ESET, spol. s r.o. es el único controlador de los datos recopilados en el programa. Esta información no se comparte con terceros.

Acuerdo de licencia de usuario final

Vigente a partir del 19 de octubre de 2021.

IMPORTANTE: Lea los términos y las condiciones del producto de aplicación que se especifican abajo antes de descargarlo, instalarlo, copiarlo o usarlo. **AL DESCARGAR, INSTALAR, COPIAR O UTILIZAR EL SOFTWARE, USTED DECLARA SU CONSENTIMIENTO CON LOS TÉRMINOS Y CONDICIONES Y RECONOCE QUE HA LEÍDO LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de Licencia de Usuario Final

Los términos de este Acuerdo de licencia para el usuario final ("Acuerdo") ejecutado por y entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, registrado en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, n.° de entrada 3586/B, número de registro de negocio: 31333532 ("ESET" o el "Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tienen derecho a usar el Software definido en el Artículo 1 de este Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet,

descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, descarga, copia o uso del Software, acepta los términos y condiciones de este Acuerdo y la Política de privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de privacidad, de inmediato 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 LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

1. **Software.** Tal como se utiliza en este Acuerdo, el término "Software" significa: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todos los contenidos de los discos, CD-ROMs, DVDs, correos electrónicos y cualquier adjunto, u otros medios con los cuales se provee este Acuerdo, incluyendo el formulario del código objeto del software provisto en soporte digital, por medio de correo electrónico o descargado a través de la Internet; (iii) cualquier material escrito explicativo relacionado y cualquier otra documentación posible relacionada con el Software, sobre todo cualquier descripción del Software, sus especificaciones, cualquier descripción de las propiedades u operación del software, cualquier descripción del ambiente operativo en el cual se utiliza el Software, instrucciones de uso o instalación del Software o cualquier descripción del modo de uso del Software ("Documentación"); (iv) copias del Software, parches para posibles errores del Software, adiciones al Software, extensiones del Software, versiones modificadas del Software y actualizaciones de los componentes del Software, si existieran, con la autorización que le da a Usted el Proveedor con arreglo al Artículo 3 de este Acuerdo. El Software será provisto exclusivamente en la forma de código objeto ejecutable.

2. **Instalación, equipo y clave de licencia**. El Software suministrado en un soporte digital, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. El Software debe instalarse en un equipo correctamente configurado que cumpla, como mínimo, con los requisitos especificados en la Documentación. La metodología de instalación se describe en la Documentación. No puede haber ningún programa informático ni Hardware que pudiera afectar al Software instalado en el equipo en el que instala el Software. El equipo hace referencia al Hardware que incluye, pero no se limita, a equipos personales, equipos portátiles, estaciones de trabajo, equipos de bolsillo, teléfonos inteligentes, dispositivos electrónicos portátiles o cualquier otro dispositivo para el que se diseñe el Software y en el que vaya a instalarse y/o utilizarse. La clave de licencia se refiere a una secuencia única de símbolos, letras números o caracteres especiales que se le brinda al Usuario final para permitirle el uso del Software de manera legal, así como de una versión específica de este o para brindarle una extensión de los términos de la Licencia en conformidad con el presente 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.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) **Disposición sobre la cantidad de licencias.** El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático,

o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("AUC"). Si un AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software en la medida en que el Usuario final tenga derecho a usar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

c) **Home/Business Edition.** La versión Home Edition del Software solo se usará en entornos privados o no comerciales para uso en el hogar y familiar exclusivamente. Debe obtener una versión Business Edition del software para poder usarla en un entorno comercial, así como en servidores, transmisores y puertas de enlace de correo o de Internet.

d) **Término de la Licencia.** El derecho a utilizar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El software clasificado como "OEM" solo se puede usar en el equipo con el que se ha obtenido. No puede transferirse a otro equipo.

f) **Software NFR y versión de prueba.** Al Software clasificado como "No apto para la reventa", "NFR" o "Versión de prueba" no se le podrá asignar un pago y puede utilizarse únicamente para hacer demostraciones o evaluar las características del Software.

g) **Rescisión de la Licencia.** La Licencia se rescindirá automáticamente al finalizar el período para el cual fue otorgada. Si Usted no cumple con alguna de las disposiciones de este Acuerdo, el Proveedor tendrá el derecho de anular el Acuerdo, sin perjuicio de cualquier derecho o recurso judicial disponible para el Proveedor en dichas eventualidades. En el caso de cancelación de la Licencia, Usted deberá borrar, destruir o devolver de inmediato por su propia cuenta el Software y todas las copias de seguridad a ESET o al punto de venta donde obtuvo el Software. Tras la finalización de la Licencia, el Proveedor podrá cancelar el derecho del Usuario Final a utilizar las funciones del Software que requieran conexión a los servidores del Proveedor o de terceros.

4. **Funciones con recopilación de información y requisitos para la conexión a Internet.** Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para llevar a cabo las siguientes funciones del Software:

a) **Actualizaciones del Software.** El Proveedor podrá publicar periódicamente actualizaciones o actualizaciones del Software ("Actualizaciones"), 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 aprovisionar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el equipo o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La entrega de todas las actualizaciones puede estar sujeta a la Política de fin de la vida útil ("Política EOL"), disponible en https://go.eset.com/eol_home. No se proporcionarán actualizaciones una vez que el Software o

cualquiera de sus funciones lleguen a la fecha de fin de su vida útil, como se define en la Política EOL.

b) **Envío de infiltraciones e información al Proveedor**. El Software contiene funciones que reúnen muestras de virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URL, paquetes de IP y marcos de Ethernet ("Infiltraciones") y luego los envía al Proveedor, incluidas, entre otras, la información sobre el proceso de instalación, el equipo o la plataforma en los cuales se instala el Software y la información sobre las operaciones y la funcionalidad del Software ("Información"). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados.

La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.

ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor. El Usuario final debe activar esta función durante la instalación del Software.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo.

Los detalles sobre la privacidad, la protección de la información personal y sus derechos como parte interesada pueden encontrarse en la Política de Privacidad, disponible en el sitio web del Proveedor y a la que se puede acceder de manera directa desde el proceso de instalación. También puede acceder a ella desde la sección de ayuda del Software.

5. **Ejercicio de los derechos del 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 sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar el Software, Usted tiene la obligación de cumplir con las siguientes restricciones:

a) Puede crear una copia del Software en un soporte de almacenamiento permanente de datos como una copia de seguridad para archivar, siempre que su copia de seguridad para archivar no esté instalada ni se utilice en

ningún equipo. Cualquier otra copia que realice del Software constituirá un incumplimiento de este Acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el Software, o transferir los derechos de su uso o copias realizadas del Software de ninguna otra forma a lo establecido en este Acuerdo.

c) No puede vender, sublicenciar, arrendar o alquilar el Software, ni usarlo para suministrar servicios comerciales.

d) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar el Software, ni intentar obtener el código fuente del Software de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.

e) Usted acepta que solo usará el Software de forma que se cumplan todas las leyes aplicables en la jurisdicción en la que lo utilice, incluyendo, pero sin limitarse a, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

g) Usted acepta no ejercer ninguna actividad que implique el uso de la clave de Licencia de manera contraria a los términos de este Acuerdo ni que implique proporcionar la clave de Licencia a personas que no estén autorizadas a hacer uso del Software, como la transferencia de la clave de Licencia usada o no. en cualquier forma, así como la reproducción no autorizada, o la distribución de claves de Licencia duplicadas o generadas. Asimismo, no utilizará el Software como resultado del uso de una clave de Licencia obtenida de una fuente que no sea el Proveedor.

7. **Copyright**. El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciatarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciatarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del Proveedor en relación con el incumplimiento 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 medios duales, varias copias**. En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. 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 desde la fecha en que Usted acepta los términos

de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Su derecho a usar el Software y cualquiera de sus funciones puede estar sujeto a la Política EOL. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil definida en la Política EOL, se terminará su derecho a usar el Software. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. **Sin más obligaciones**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O LICENCIADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE CUALQUIER VALOR ESPECIAL, DIRECTO, INSONDADO, ACCIDENTAL, ECONÓMICO, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, QUE SIN EMBARGO DERIVEN O SURJAN POR CONTRATO, AGRAVIOS, NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD QUE DERIVE DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, AUNQUE EL PROVEEDOR, SUS LICENCIADORES O FILIALES RECIBAN INFORMACIÓN DE 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. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

15. **Soporte técnico**. ESET o los terceros autorizados por ESET suministrarán soporte técnico a discreción propia, sin ninguna garantía ni declaración. Cuando el software o cualquiera de sus funciones lleguen a la fecha de fin de la vida útil definida en la Política EOL, no se proporcionará soporte técnico. El Usuario final deberá crear una copia de seguridad de todos los datos existentes, software y prestaciones de los programas en forma previa al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET no pueden aceptar la responsabilidad por el daño o pérdida de datos, propiedad, software o hardware, o pérdida de beneficios debido al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET se reservan el derecho de decidir si la solución del problema excede el alcance del soporte técnico. ESET se reserva el derecho de rechazar, suspender o dar por finalizado el suministro de soporte técnico a discreción propia. Se puede solicitar información sobre la Licencia y cualquier otro tipo de información a fin de brindar soporte técnico conforme a la Política de Privacidad.

16. **Transferencia de la Licencia**. El Software puede transferirse de un sistema informático a otro, a menos que

esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a usar el Software en una de las siguientes maneras: (i) a través de un certificado de licencia emitido por el Proveedor o por un tercero designado por el Proveedor; (ii) a través de un acuerdo de licencia por escrito, en caso de haberse establecido dicho acuerdo; (iii) a través de la presentación de un correo electrónico enviado por el Proveedor donde se incluyan los detalles de la Licencia (nombre de usuario y contraseña). Se puede solicitar información sobre la Licencia y datos sobre el Usuario final a para llevar a cabo la verificación de la autenticidad del Software conforme a la Política de Privacidad.

18. **Licencias para autoridades públicas y el gobierno de los Estados Unidos**. Se deberá suministrar el Software a las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

19. **Cumplimiento del control comercial**.

a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras ("Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen

i. toda ley que controle, restrinja o imponga requisitos de licencia a la exportación, reexportación o transferencia de productos, software, tecnología o servicios, establecida o adoptada por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas y

ii. cualquier sanción, restricción, embargo, prohibición de exportación o importación, prohibición de transferencia de fondos o activos o prohibición de prestación de servicios, ya sea de índole económica, financiera, comercial o de otro tipo, o toda medida equivalente impuesta por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas.

(actos legales mencionados en los puntos i y ii. anteriormente, denominados "Leyes de control comercial").

b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición del Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme al Acuerdo

podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

20. **Avisos**. Todos los avisos y devoluciones de software o documentación deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle cualquier cambio de este Acuerdo, las Políticas de privacidad, la Política de EOL y la Documentación de acuerdo con el artículo. 22 del Acuerdo. ESET puede enviarle correos electrónicos, notificaciones en la aplicación a través del Software o publicar la comunicación en nuestro sitio web. Acepta recibir comunicaciones legales de ESET de forma electrónica, lo que incluye comunicaciones sobre cambios de Términos, Términos especiales o Políticas de privacidad, cualquier contrato de trabajo o aceptación o invitación a tratar, 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 conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo, Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

22. **Disposiciones generales**. Si alguna disposición de este Acuerdo no es válida o aplicable, no afectará la validez de las demás disposiciones del Acuerdo, que seguirán siendo válidas y ejecutables bajo las condiciones aquí estipuladas. Este acuerdo se ha ejecutado en inglés. En el caso de que se prepare cualquier traducción del acuerdo para su comodidad o con cualquier otro fin, o en caso de discrepancia entre las versiones en diferentes idiomas de este acuerdo, prevalecerá la versión en inglés.

ESET se reserva el derecho de realizar cambios en el Software, así como de revisar los términos de este Acuerdo, sus Anexos, la Política de privacidad, la Política y la Documentación de EOL o cualquier parte de ellos, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar cambios del Software o el comportamiento comercial de ESET, (ii) por cuestiones legales, normativas o de seguridad; o (iii) para evitar abusos o daños. Se le notificará cualquier revisión del Acuerdo por correo electrónico, notificación en la aplicación o por otros medios electrónicos. Si no está de acuerdo con los cambios de texto del Acuerdo, puede rescindirlo de acuerdo con el Artículo 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 de texto se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el acuerdo entero entre el proveedor y Usted relacionado con el Software y reemplaza a cualquier representación, discusión, garantía, comunicación o publicidad previa relacionadas con el Software.

ANEXO AL ACUERDO

Evaluación de seguridad de los dispositivos conectados a la red. Se aplican disposiciones adicionales a la Evaluación de seguridad de los dispositivos conectados a la red como se muestra a continuación:

El Software contiene una función para verificar la seguridad de la red local del Usuario final y la seguridad de los dispositivos en la red local, lo que requiere el nombre de la red local e información acerca de los dispositivos en la red local, como presencia, tipo, nombre, dirección IP y dirección MAC en conexión con la información de licencia. La información también incluye tipo de seguridad inalámbrica y tipo de cifrado inalámbrico para los dispositivos

del enrutador. Esta función también puede proporcionar información relacionada con la disponibilidad de la solución de software de seguridad para asegurar los dispositivos en la red local.

Protección contra el uso indebido de datos. Se aplican disposiciones adicionales a la protección contra el uso indebido de datos como se muestra a continuación:

El Software contiene una función que evita la pérdida o el uso indebido de datos críticos directamente relacionados con el robo de un equipo. Esta función se puede desactivar en los parámetros predeterminados del Software. Hay que crear una Cuenta ESET HOME para activarla, a través de la cual se activa la recopilación de datos en caso de robo del equipo. Si activa esta función del Software, se recopilará la información acerca del equipo robado y se enviará al Proveedor. Esta información puede incluir datos relacionados con la ubicación de red del equipo, datos relacionados con el contenido que se muestra en la pantalla del equipo, datos acerca de la configuración del equipo o datos grabados mediante una cámara conectada al equipo (en adelante denominados “Datos”). El Usuario final podrá usar los Datos obtenidos por esta función y proporcionados a través de la Cuenta ESET HOME exclusivamente para rectificar una situación adversa causada por el robo de un equipo. Para la única finalidad de esta función, el Proveedor procesa los Datos según se especifica en la Política de Privacidad y conforme a los reglamentos legales pertinentes. El Proveedor permitirá al Usuario final acceder a los Datos durante el período requerido para alcanzar el objetivo para el que se obtuvieron los datos, que no podrá superar el período de retención especificado en la Política de Privacidad. La protección contra el uso indebido de datos será usada exclusivamente con equipos y cuentas para los que el Usuario final tenga acceso legítimo. Cualquier uso ilegal será informado a la autoridad competente. El Proveedor cumplirá con las leyes relevantes y asistirá a las autoridades encargadas del cumplimiento de la ley en caso de uso indebido. Usted acepta y reconoce que es responsable de proteger la contraseña de acceso a la Cuenta ESET HOME y acuerda no divulgar la contraseña a un tercero. El Usuario Final es responsable por cualquier actividad realizada la función de protección contra el uso indebido de datos de la Cuenta ESET HOME, ya sea autorizada o no. Si su cuenta de ESET HOME se ve comprometida, notifíquelo inmediatamente al Proveedor. Las disposiciones adicionales para la protección contra el uso indebido de datos solo podrán aplicarse a los usuarios finales de ESET Internet Security y ESET Smart Security Premium.

ESET Secure Data. Se aplican disposiciones adicionales a ESET Secure Data como se muestra a continuación:

1. Definiciones. En estas disposiciones adicionales de ESET Secure Data, los términos a continuación significan lo siguiente:

a) “Información” Todo tipo de datos que se cifran o descrifran mediante el uso del software.

b) "Productos" el software y la documentación de ESET Secure Data;

c) "ESET Secure Data", el software que se usa para el cifrado y descifrado de datos electrónicos;

Toda referencia al plural deberá incluir el singular, así como toda referencia al género masculino deberá incluir el femenino y el neutro, y viceversa. Las palabras que no tengan una definición específica deberán utilizarse en conformidad con las definiciones estipuladas por este Acuerdo.

2. Declaración de Usuario final adicional. Usted reconoce y acepta que:

a) Es su responsabilidad proteger, mantener y realizar copias de seguridad de la Información;

b) Debe realizar copias de seguridad completas de toda la información y los datos (incluidos, por ejemplo, información y datos críticos) en su equipo antes de instalar del ESET Secure Data;

c) Debe conservar un registro seguro de las contraseñas y demás información que se usa para la configuración y uso del ESET Secure Data. También debe realizar copias de seguridad de todas las claves de cifrado, códigos de

licencia, archivos clave y demás datos generados en un medio de almacenamiento separado;

d) Usted es responsable del uso de los Productos. El Proveedor no será responsable por pérdidas, reclamos o daños sufridos como consecuencia de cualquier cifrado o descifrado no autorizado o equivocado de información o datos independientemente del lugar o del modo en que se almacena dicha información o dichos datos;

e) A pesar de que el Proveedor siguió todos los pasos posibles para garantizar la integridad y seguridad de ESET Secure Data, los Productos (o cualquiera de ellos) no se deben usar en áreas que sean dependientes de un nivel de seguridad a prueba de fallos o que sean potencialmente peligrosas o riesgosas, incluso, por ejemplo, instalaciones nucleares, navegación aérea, sistemas de control o comunicación, sistemas de armas o defensa y sistemas de soporte vital o control vital;

f) Es su responsabilidad garantizar que el nivel de seguridad y cifrado provisto por el producto sea adecuado para sus requisitos;

g) Usted es responsable del uso de los Productos o cualquiera de ellos, que incluyen, pero no se limitan a, asegurar que dicho uso cumpla con las leyes y normativas vigentes de la República Eslovaca o de otro país, región o estado donde se utiliza el producto. Antes de usar los productos, debe asegurarse de que no constituye una contravención de un embargo gubernamental (en la República Eslovaca o en otro país);

h) ESET Secure Data puede contactar al Proveedor en distintas oportunidades para verificar la información de la licencia, parches disponibles, paquetes de servicio y otras actualizaciones que pueden mejorar, modificar o realizar la operación de ESET Secure Data. El software puede enviar información general del sistema relacionada con la funcionalidad del software en conformidad con la Política de Privacidad.

i) El Proveedor no será responsable por pérdidas, daños, gastos o reclamos generados por pérdidas, robos, mal uso, corrupción, daños o destrucciones de contraseñas, información de configuración, claves de cifrado, códigos de activación de licencias o demás datos generados o almacenados durante el uso del software.

Las disposiciones adicionales de ESET Secure Data solo se podrán aplicar a los usuarios finales de ESET Smart Security Premium.

Password Manager Software. Se aplican disposiciones adicionales al software Password Manager como se muestra a continuación:

1. Declaración de Usuario final adicional. Usted reconoce y acepta que no:

a) Utilizará el software de Password Manager para operar cualquier aplicación de misión crítica donde pudiera estar en peligro la vida humana o las propiedades. Usted comprende que el software de Password Manager no está diseñado para dichos propósitos y que su falla en dichos casos podría llevar a la muerte, lesiones personales o daños graves a la propiedad o el medio ambiente por los cuales el Proveedor no será responsable.

EL SOFTWARE DE PASSWORD MANAGER NO ESTÁ DISEÑADO, LICENCIADO NI ES APTO PARA SU USO EN ENTORNOS PELIGROSOS QUE REQUIEREN CONTROLES A PRUEBA DE FALLAS, INCLUIDOS, POR EJEMPLO, EL DISEÑO, LA CONSTRUCCIÓN, EL MANTENIMIENTO O LA OPERACIÓN DE INSTALACIONES NUCLEARES, SISTEMAS DE NAVEGACIÓN O COMUNICACIÓN AÉREOS, CONTROL DE TRÁFICO AÉREO Y SISTEMAS DE SOPORTE VITAL O DE ARMAS. EL PROVEEDOR ESPECÍFICAMENTE NIEGA TODA GARANTÍA EXPRESA O IMPLÍCITA DE IDONEIDAD PARA DICHOS PROPÓSITOS.

b) Utilizará el software de Password Manager de manera que viole este acuerdo o las leyes de la República Eslovaca o su jurisdicción. En concreto, no puede usar el software Password Manager para crear ni promover contenido ilegal, lo que incluye la carga de datos de contenido dañino o que pueda usarse para actividades ilegales o que infrinjan de algún modo la ley o los derechos de terceros (incluidos todos los derechos de

propiedad intelectual), lo que incluye, entre otras cosas, cualquier intento de acceder a las cuentas del Almacenamiento (a los efectos de estos términos adicionales del software Password Manager, por “Almacenamiento” se hace referencia al espacio de almacenamiento de datos administrado por el Proveedor o un tercero que no sea el Proveedor y el Usuario a efectos de activar la sincronización y copia de seguridad de los datos del usuario) o cualquier cuenta y datos de otros usuarios del software Password Manager o del Almacenamiento. Si usted viola cualquiera de estas disposiciones, el Proveedor tiene derecho a finalizar inmediatamente este acuerdo y trasladarle los costos de cualquier acción, como así también a tomar las medidas necesarias para evitar que Usted continúe usando el software de Password Manager sin la posibilidad de reembolso.

2. LIMITACIÓN DE RESPONSABILIDAD. EL SOFTWARE DE PASSWORD MANAGER ES PROVISTO "COMO ESTÁ". NO SE EXPRESA NI IMPLICA NINGÚN TIPO DE GARANTÍA. USTED USA EL SOFTWARE BAJO SU PROPIO RIESGO. EL PRODUCTOR NO ES RESPONSABLE POR PÉRDIDAS DE DATOS, DAÑOS, LIMITACIÓN DE DISPONIBILIDAD DE SERVICIO, INCLUIDOS DATOS ENVIADOS POR EL SOFTWARE DE PASSWORD MANAGER A UN ALMACENAMIENTO EXTERNO POR PROPÓSITOS DE SINCRONIZACIÓN Y COPIA DE SEGURIDAD DE DATOS. EL CIFRADO DE DATOS CON EL USO DEL SOFTWARE DE PASSWORD MANAGER NO IMPLICA NINGUNA RESPONSABILIDAD DEL PROVEEDOR RESPECTO A LA SEGURIDAD DE DICHOS DATOS. USTED ACUERDA EXPRESAMENTE QUE LOS DATOS ADQUIRIDOS, USADOS, CIFRADOS, ALMACENADOS, SINCRONIZADOS O ENVIADOS MEDIANTE EL SOFTWARE DE PASSWORD MANAGER TAMBIÉN PUEDEN ALMACENARSE EN SERVIDORES DE TERCEROS (SE APLICA SOLO AL USO DEL SOFTWARE DE PASSWORD MANAGER DONDE LOS SERVICIOS DE SINCRONIZACIÓN Y COPIA DE SEGURIDAD FUERON HABILITADOS). SI EL PROVEEDOR, A SU PROPIA DISCRECIÓN, SELECCIONA USAR DICHO ALMACENAMIENTO, SITIOS WEB, PORTAL WEB, SERVIDOR O SERVICIO DE TERCEROS, EL PROVEEDOR NO ES RESPONSABLE POR LA CALIDAD, SEGURIDAD O DISPONIBILIDAD DE DICHO SERVICIO DE TERCEROS Y EN NINGÚN CASO SERÁ EL PROVEEDOR RESPONSABLE ANTE USTED POR CUALQUIER INCUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES O LEGALES POR PARTE DEL TERCERO NI POR DAÑOS, PÉRDIDA DE GANANCIAS, DAÑOS ECONÓMICOS O NO ECONÓMICOS O CUALQUIER OTRO TIPO DE PÉRDIDA DURANTE EL USO DE ESTE SOFTWARE. EL PROVEEDOR NO ES RESPONSABLE DEL CONTENIDO DE LOS DATOS ADQUIRIDOS, USADOS, CIFRADOS, ALMACENADOS, SINCRONIZADOS O ENVIADOS MEDIANTE EL SOFTWARE DE PASSWORD MANAGER O EN EL ALMACENAMIENTO. USTED RECONOCE QUE EL PROVEEDOR NO TIENE ACCESO AL CONTENIDO DE LOS DATOS ALMACENADOS Y NO PUEDE CONTROLARLOS O ELIMINAR EL CONTENIDO LEGALMENTE DAÑINO.

El proveedor posee todos los derechos de mejoras, actualizaciones y arreglos relacionados con el software de Password MANAGER ("Mejoras"), incluso en el caso de que dichas mejoras hayan sido creadas a partir de comentarios, ideas o sugerencias enviados por usted en cualquier formato. Usted no tendrá derecho a compensación, incluidas regalías relacionadas con dichas Mejoras.

LAS ENTIDADES O LICENCIADORES DEL PROVEEDOR NO SERÁN RESPONSABLES ANTE USTED POR RECLAMOS Y RESPONSABILIDADES DE CUALQUIER TIPO QUE SURJAN O ESTÉN DE ALGUNA MANERA RELACIONADAS AL USO DEL SOFTWARE DE PASSWORD MANAGER POR PARTE SUYA O DE TERCEROS, AL USO O NO USO DE FIRMAS O PROVEEDORES DE CORRETAJE O A LA VENTA O COMPRA DE CUALQUIER SEGURIDAD, INDEPENDIENTEMENTE DE QUE DICHOS RECLAMOS Y RESPONSABILIDADES SE BASEN EN UNA TEORÍA LEGAL O EQUITATIVA.

LAS ENTIDADES O LICENCIADORES DEL PROVEEDOR NO SON RESPONSABLES ANTE USTED POR CUALQUIER DAÑO DIRECTO, ACCIDENTAL, ESPECIAL, INDIRECTO O CONSECUENTE DERIVADO O RELACIONADO A CUALQUIER SOFTWARE DE TERCEROS, CUALQUIER DATO AL QUE SE ACCEDE A TRAVÉS DEL SOFTWARE DE PASSWORD MANAGER, SU USO O IMPOSIBILIDAD DE USO O ACCESO AL SOFTWARE DE PASSWORD MANAGER O A CUALQUIER DATO PROVISTO A TRAVÉS DEL SOFTWARE DE PASSWORD MANAGER, INDEPENDIENTEMENTE DE QUE DICHOS RECLAMOS POR DAÑOS SE GENEREN BAJO UNA TEORÍA DE LEY O EQUIDAD. LOS DAÑOS EXCLUIDOS POR ESTA CLÁUSULA INCLUYEN, POR EJEMPLO, AQUELLOS DE PÉRDIDAS DE GANANCIAS COMERCIALES, LESIÓN A PERSONAS O DAÑOS MATERIALES, INTERRUPCIÓN DE NEGOCIOS, PÉRDIDA DE INFORMACIÓN COMERCIAL O PERSONAL. ALGUNAS JURISDICCIONES NO PERMITEN LA LIMITACIÓN DE DAÑOS ACCIDENTALES O CONSECUENTES, POR LO QUE ESTA RESTRICCIÓN PODRÍA NO APLICARSE A USTED. EN DICHO CASO, EL GRADO DE

RESPONSABILIDAD DEL PROVEEDOR SERÁ EL MÍNIMO PERMITIDO POR LA LEY EN VIGOR.

LA INFORMACIÓN PROVISTA A TRAVÉS DEL SOFTWARE DE PASSWORD MANAGER, INCLUIDAS COTIZACIONES DE ACCIONES, ANÁLISIS, INFORMACIÓN DE MERCADO, NOTICIAS Y DATOS ECONÓMICOS PUEDE ESTAR RETRASADA, SER IMPRECISA O CONTENER ERRORES U OMISIONES, Y LAS ENTIDADES Y LICENCIADORES DEL PROVEEDOR NO SERÁN RESPONSABLES RESPECTO A LA MISMA. EL PROVEEDOR PUEDE CAMBIAR O DISCONTINUAR CUALQUIER ASPECTO O FUNCIÓN DEL SOFTWARE DE PASSWORD MANAGER O EL USO DE TODAS O ALGUNAS DE LAS FUNCIONES O LA TECNOLOGÍA DEL SOFTWARE DE PASSWORD MANAGER EN CUALQUIER MOMENTO SIN PREVIO AVISO.

SI LAS DISPOSICIONES DE ESTE ARTÍCULO SON NULAS POR CUALQUIER MOTIVO O SI EL PROVEEDOR ES CONSIDERADO RESPONSABLE POR PÉRDIDAS, DAÑOS, ETC. EN EL MARCO DE LAS LEYES VIGENTES, LAS PARTES ACUERDAN QUE LA RESPONSABILIDAD DEL PROVEEDOR ANTE USTED SE LIMITARÁ AL MONTO TOTAL DE DERECHOS DE LICENCIA QUE HA PAGADO.

USTED ACUERDA INDEMNIZAR, DEFENDER Y EXONERAR AL PROVEEDOR Y A SUS EMPLEADOS, SUBSIDIARIAS, AFILIADOS, REPOSICIONAMIENTO DE MARCA Y DEMÁS SOCIOS CONTRA TODO RECLAMO, RESPONSABILIDAD, DAÑO, PÉRDIDA, COSTO, GASTO Y TARIFA DE TERCEROS (INCLUIDOS LOS PROPIETARIOS DEL DISPOSITIVO O LAS PARTES CUYOS DERECHOS FUERON AFECTADOS POR LOS DATOS USADOS EN EL SOFTWARE DE PASSWORD MANAGER O EN EL ALMACENAMIENTO) QUE DICHAS PARTES PUDIERAN INCURRIR COMO RESULTADO DE SU USO DEL SOFTWARE DE PASSWORD MANAGER.

3. Datos en el software de Password Manager. A menos que usted lo seleccione de manera explícita, todos los datos ingresados por usted que sean guardados en una base de datos del software de Password Manager se almacenan en un formato cifrado en su equipo u otro dispositivo de almacenamiento que haya definido. Usted comprende que en el caso de eliminación de cualquier base de datos u otros archivos del software de Password Manager o la eliminación de estos, todos los datos contenidos en los mismos se perderán irreversiblemente y usted comprende y acepta el riesgo de dicha pérdida. El hecho de que sus datos personales estén almacenados en un formato cifrado en el equipo no significa que la información no pueda ser robada o usada de forma errónea por alguien que descubra la Contraseña maestra u obtenga acceso al dispositivo de activación definido por el usuario para abrir la base de datos. Usted es responsable de mantener la seguridad de todos los métodos de acceso.

4. Transmisión de datos personales al proveedor o al almacenamiento. Si elige hacerlo, y con el único propósito de garantizar una sincronización y copia de seguridad oportunas, el software de Password Manager transmite o envía datos personales desde la base de datos del software de Password Manager (principalmente contraseñas, información de inicio de sesión, Cuentas e Identidades) a través de Internet hacia el Almacenamiento. Los datos se transfieren exclusivamente en forma cifrada. El uso del software de Password Manager para completar formularios en línea con contraseñas, inicios de sesión u otros datos puede requerir el envío de información a través de Internet al sitio web que identifica. Esta transmisión de datos no se inicia en el software de Password Manager y, por lo tanto, el Proveedor no puede ser responsable por la seguridad de dichas interacciones con cualquier sitio web admitido por los diversos proveedores. Cualquier transacción a través de Internet, ya sea en conjunto o no con el software de Password Manager, se realiza bajo su propia discreción y riesgo y usted será el único responsable por los daños en su sistema informático o pérdidas de datos resultantes de la descarga y/o uso de cualquier material o servicio mencionado. Para minimizar el riesgo de pérdidas de datos valiosos, el Proveedor recomienda que los clientes realicen una copia de seguridad periódica de la base de datos y de los demás archivos importantes en unidades externas. El Proveedor no puede proveerle asistencia en la recuperación de datos perdidos o dañados. Si el Proveedor le proporciona servicios de copia de seguridad de los archivos de la base de datos del usuario en caso de daños o eliminaciones de los archivos en las PC del usuario, dicho servicio de copia de seguridad se provee sin garantías y no implica que el Proveedor tenga responsabilidad alguna ante usted.

Al utilizar el software de Password Manager, Usted acepta que el software puede contactar a los servidores del Proveedor en distintas oportunidades para verificar la información de la licencia, parches disponibles, paquetes

de servicio y otras actualizaciones que pueden mejorar, mantener, modificar o realzar la operación del software de Password Manager. El software puede enviar información general del sistema relacionada con la funcionalidad del software de Password Manager en conformidad con la Polìtica de Privacidad.

5. Información e instrucciones de desinstalación. Toda la información que desee retener de la base de datos se debe exportar antes de desinstalar el software de Password Manager.

Las disposiciones adicionales del software Password Manager solo se podrán aplicar a los usuarios finales de ESET Smart Security Premium.

ESET LiveGuard. Se aplican disposiciones adicionales a ESET LiveGuard como se muestra a continuación:

El Software incluye una función de análisis adicional de los archivos enviados por el Usuario final. El Proveedor solo podrá usar los archivos enviados por el Usuario final y los resultados del análisis de acuerdo con la Política de Privacidad y la normativa legal relevante.

Las disposiciones adicionales de ESET LiveGuard solo se podrán aplicar 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 reviste especial importancia para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita en el Registro comercial del Tribunal de Distrito de Bratislava I, Sección Sro, Registro N.º 3586/B, Número de registro de empresa: 31333532 como controlador de datos (“ESET” o “Nosotros”). Queremos cumplir con el requisito de transparencia de acuerdo con el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”). A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”), en carácter de interesados, acerca de los siguientes temas relativos a la protección de los datos personales:

- Fundamento jurídico para el procesamiento de datos personales.
- Intercambio y confidencialidad de los datos.
- Seguridad de los datos.
- Sus derechos como interesado.
- Procesamiento de sus datos personales.
- Información de contacto.

Fundamento jurídico para el procesamiento de datos personales

Existen solo unas pocas bases legales para el procesamiento de datos que usamos de acuerdo con el marco legislativo aplicable en relación con la protección de datos personales. En ESET, el procesamiento de datos personales es necesario principalmente a fin de cumplir con el Acuerdo de Licencia de Usuario Final (“EULA”) con el Usuario final [Art. 6 (1) (b) del Reglamento General de Protección de Datos (RGPD)], que rige la prestación de productos o servicios de ESET, a menos que se indique algo distinto explícitamente, p. ej.:

- El fundamento jurídico del interés legítimo, conforme al Art. 6 (1) (f) del RGPD, que nos permite procesar los

datos sobre cómo nuestros clientes usan nuestros Servicios y su satisfacción a fin de ofrecerles a nuestros usuarios el máximo nivel posible en protección, soporte y experiencia. Incluso la legislación aplicable reconoce el marketing como un interés legítimo. Por lo tanto, solemos confiar en este concepto cuando se trata de la comunicación de marketing con nuestros clientes.

- El consentimiento, conforme al Art. 6 (1) (a) del RGPD, que podemos solicitarle a Usted en situaciones específicas en las que consideramos que este fundamento jurídico es el más adecuado o si lo exige la ley.

- El cumplimiento de una obligación legal, conforme al Art. 6 (1) (c) del RGPD, por ejemplo, una que estipula los requisitos para la comunicación electrónica o la retención de documentos de facturación o cobranza.

Intercambio y confidencialidad de los datos

No compartimos sus datos con terceros. Sin embargo, ESET es una compañía que opera globalmente a través de entidades afiliadas o socios como parte de nuestra red de venta, servicio y soporte. La información sobre licencias, facturación y soporte técnico que procesa ESET puede ser transferida desde las entidades afiliadas o los socios o hacia ellos a fin de ejecutar el EULA, por ejemplo, para la prestación de servicios o soporte.

ESET prefiere procesar sus datos en la Unión Europea (UE). Sin embargo, según su ubicación (el uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transmitir sus datos a un país ubicado fuera de la UE. Por ejemplo, usamos servicios de terceros en conexión con la informática en la nube. En estos casos, seleccionamos cuidadosamente a nuestros proveedores de servicios y garantizamos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por regla general, pactamos las cláusulas contractuales estándar de la UE, si es necesario, con normas contractuales complementarias.

En el caso de algunos países fuera de la UE, como Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos equivalente. Debido a este nivel de protección de datos equivalente, la transferencia de datos hacia estos países no requiere ninguna autorización ni acuerdo especial.

Seguridad de los datos

ESET implementa medidas técnicas y de organización para asegurar un nivel de seguridad apropiado ante riesgos potenciales. Hacemos todo lo posible para garantizar una continua confidencialidad, integridad, disponibilidad y resistencia de los sistemas operativos y servicios. Sin embargo, si ocurre una filtración de datos que genera un riesgo para sus derechos y libertades, estamos preparados para notificar a la autoridad supervisora pertinente, como también a los Usuarios finales afectados que actúen en carácter de interesados.

Derechos de la persona registrada

Los derechos de los Usuarios finales son importantes. Queremos informarle que cada Usuario final (de cualquier país, dentro y fuera de la Unión Europea) tiene los siguientes derechos, que ESET garantiza. Para ejercer los derechos de los interesados, puede comunicarse con nosotros a través del formulario de soporte o por correo electrónico a la siguiente dirección: dpo@eset.sk. A fin de poder identificarlo, le solicitamos la siguiente información: Nombre, dirección de correo electrónico y, de estar disponible, clave de licencia o número de cliente y empresa de afiliación. No debe enviarnos ningún otro dato personal, como la fecha de nacimiento. Queremos señalar que, para poder procesar su solicitud, así como con fines de identificación, procesaremos sus datos personales.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento resulta aplicable únicamente cuando nuestro procesamiento requiera su consentimiento. Si procesamos sus datos personales en razón de su

consentimiento, tiene derecho a retirarlo en cualquier momento sin expresión de causa. Solo podrá retirar su consentimiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad.

Derecho a oponerse. El derecho a oponerse al procesamiento resulta aplicable únicamente cuando nuestro procesamiento esté basado en el interés legítimo de ESET o un tercero. Si procesamos sus datos personales en pos de un interés legítimo, Usted, como interesado, tiene derecho a oponerse, en cualquier momento, al interés legítimo que designemos y al procesamiento de sus datos personales. Solo podrá oponerse al procesamiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad. Si procesamos sus datos personales con fines de marketing directo, no es necesario que exprese una causa. Esto también se aplica a la elaboración de perfiles, ya que se relaciona con el marketing directo. En todos los demás casos, le solicitamos que nos informe, de forma breve, sus quejas en contra del interés legítimo de ESET para el procesamiento de sus datos personales.

Tenga en cuenta que, en algunos casos, a pesar de que haya retirado su consentimiento, tenemos derecho a continuar procesando sus datos personales en función de algún otro fundamento jurídico, por ejemplo, para el cumplimiento de un contrato.

Derecho de acceso. En carácter de interesado, Usted tiene derecho a obtener información de los datos que almacene ESET sobre usted de forma gratuita, en cualquier momento.

Derecho a solicitar una rectificación. En caso de que procesemos de forma involuntaria datos personales incorrectos sobre Usted, tiene derecho a que se corrija esta información.

Derecho a solicitar el borrado de los datos y la restricción en el procesamiento. En carácter de interesado, Usted tiene derecho a solicitar el borrado de sus datos personales o una restricción en su procesamiento. Si procesamos sus datos personales, por ejemplo, con su consentimiento, Usted lo retira y no hay ningún otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. También eliminaremos sus datos personales en cuanto ya no sean necesarios para los fines indicados cuando finalice nuestro período de retención.

Si usamos sus datos personales únicamente con el fin de marketing directo y Usted ha retirado su consentimiento o se ha opuesto al interés legítimo subyacente de ESET, restringiremos el procesamiento de sus datos personales, lo que implicará que sus datos de contacto se incluyan en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales serán eliminados.

Tenga en cuenta que podemos tener la obligación de almacenar sus datos hasta que finalicen los períodos y las obligaciones de retención determinados por el legislador o las autoridades supervisoras. La legislación eslovaca también podría determinar períodos y obligaciones de retención. A partir de su finalización, los datos correspondientes se eliminarán de forma rutinaria.

Derecho a la portabilidad de datos. Nos complace proporcionarle a Usted, en carácter de interesado, los datos personales que procese ESET en formato xls.

Derecho a presentar una queja. Como interesado, Usted tiene el derecho de presentar una queja a una autoridad supervisora en cualquier momento. ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. La autoridad supervisora competente en materia de datos es la Oficina de Protección de Datos Personales de la República de Eslovaquia, con sede en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Procesamiento de sus datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del

EULA, pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos diversos servicios descritos en el EULA y la documentación. Para hacer que todo funcione, necesitamos recolectar la siguiente información:

Datos de facturación y licencia. ESET recopila y procesa el nombre, la dirección de correo electrónico, la clave de licencia y, si corresponde, la dirección, la empresa de afiliación y los datos de pago para facilitar la activación de la licencia, la entrega de la clave de licencia, los recordatorios sobre caducidad, las solicitudes de soporte, la verificación de la autenticidad de la licencia, la prestación de nuestro servicio y otras notificaciones, como mensajes de marketing acordes a la legislación aplicable o Su consentimiento. ESET tiene la obligación legal de conservar la información de facturación durante un plazo de 10 años, pero la información sobre licencias se anonimiza a más tardar 12 meses después de la caducidad de la licencia.

Actualización y otras estadísticas. La información procesada comprende información relacionada con el proceso de instalación y su equipo, lo que incluye 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. Esta información se procesa con el fin de prestar servicios de actualización y a efectos del mantenimiento, la seguridad y la mejora de nuestra infraestructura de backend.

Esta información se encuentra separada de la información de identificación necesaria para las licencias y la facturación, ya que no requiere la identificación del Usuario final. El período de retención es de hasta cuatro años.

Sistema de reputación de **ESET LiveGrid®.** Las funciones hash unidireccionales relativas a infiltraciones se procesan a efectos del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección contra malware comparando archivos analizados con una base de datos de elementos en listas blancas y negras en la nube. Durante este proceso, no se identifica al Usuario final.

Sistema de comentarios de **ESET LiveGrid®.** Muestras y metadatos sospechosos de la circulación, parte del sistema de realimentación de ESET LiveGrid®, que permite a ESET reaccionar de forma inmediata ante las necesidades de sus usuarios finales y responder a las amenazas más recientes. Nosotros dependemos de que Usted nos envíe:

- Infiltraciones como muestras potenciales de virus y otros programas malignos y sospechosos; objetos problemáticos o potencialmente no deseados o inseguros, como archivos ejecutables, mensajes de correo electrónico que haya clasificado, como correo no deseado o que nuestro producto haya marcado;

- Información relativa al uso de Internet, como dirección IP e información geográfica, paquetes IP, URL y marcos de Ethernet;

- Archivos de volcado de memoria y la información que contienen.

No necesitamos recopilar datos por fuera de este ámbito. Sin embargo, en algunas ocasiones no podemos evitarlo. Los datos recopilados accidentalmente pueden incluirse como malware y Nosotros no pretendemos que sean parte de nuestros sistemas o procesarlos para el cumplimiento de los objetivos detallados en la presente Política de privacidad.

Toda la información obtenida y procesada a través del sistema de comentarios de ESET LiveGrid® ha de utilizarse sin la identificación de Usuario final.

Evaluación de seguridad de los dispositivos conectados a la red. A fin de proporcionar la función de evaluación de seguridad, procesamos el nombre de la red local y la información acerca de los dispositivos en la red local, como presencia, tipo, nombre, dirección IP y dirección MAC en conexión con la información de licencia. La información también incluye tipo de seguridad inalámbrica y tipo de cifrado inalámbrico para los dispositivos del

enrutador. La información de licencia que identifique al Usuario final se anonimiza a más tardar 12 meses después de la caducidad de la licencia.

Soporte técnico. Se puede solicitar la información de contacto, la información de licencia y los datos incluidos en sus solicitudes de soporte para brindar asistencia. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, datos de licencia, detalles del producto y descripción de su caso de asistencia. Podemos solicitarle que proporcione datos adicionales para facilitar la prestación del servicio de soporte. Los datos procesados a los fines del soporte técnico se almacenan durante cuatro años.

Protección contra el uso indebido de datos. Si el Usuario final crea una Cuenta de ESET HOME en https://home.eset.com y activa esta función en caso de robo del equipo, se recopilará y procesará la siguiente información: datos sobre la ubicación, capturas de pantalla, datos sobre la configuración del equipo y datos grabados mediante la cámara del equipo. Los datos recopilados se almacenan en nuestros servidores o en los servidores de nuestros proveedores de servicios durante un período de retención de tres meses.

Password Manager. Si elige activar la función de Password Manager, la información relativa a sus datos de acceso se almacena de forma cifrada solo en su equipo o en otro 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. 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 desactive la función.

ESET LiveGuard. Si elige activar la función de ESET LiveGuard, se requiere el envío de muestras, como 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 a su equipo. Las muestras sospechosas se procesan como información recopilada por el sistema de comentarios de ESET LiveGrid®.

Programa de mejora de la experiencia del cliente. Si optó por activar Programa de mejora de la experiencia del cliente , se recopilará y usará la información de telemetría anónima relativa al uso de nuestros productos, en función de su consentimiento.

Tenga en cuenta que, si la persona que usa nuestros productos y servicios no es el Usuario final que ha adquirido el producto o el servicio y celebrado el EULA con Nosotros (por ejemplo, un empleado del Usuario final, un familiar o una persona autorizada por el Usuario final de otra forma a usar el producto o el servicio de acuerdo con el EULA), el procesamiento de los datos se lleva a cabo en pos del interés legítimo de ESET en virtud del Artículo 6 (1) (f) del RGPD, a fin de permitir que el usuario autorizado por el Usuario final use los productos y servicios prestados por Nosotros en virtud del EULA.

Información de contacto

Si desea ejercer su derecho como persona registrada o tiene una consulta o preocupación, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk