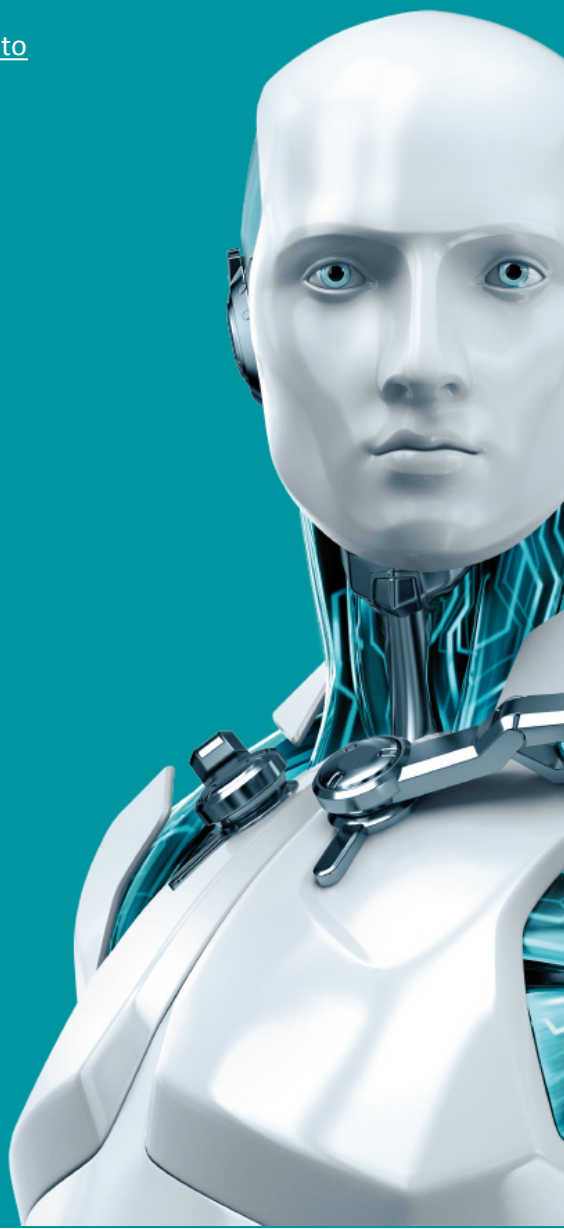
INTERNET SECURITY

GUÍA DEL USUARIO

(diseñada para la versión 12.0 o posterior del producto)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / Home Server 2011

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



ENJOY SAFER TECHNOLOGY™

Atención al cliente internacional: www.eset.com/support

REV. 14/09/2018

Contenido

1. ESET Internet Security

ESET Internet Security representa un nuevo enfoque de la seguridad informática realmente integrada. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que podrían poner en peligro su ordenador.

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

Características y ventajas

Interfaz de usuario rediseñada	La interfaz de usuario de esta versión se ha rediseñado y simplificado considerablemente en función de los resultados de las pruebas de usabilidad. Todos los textos y notificaciones de la GUI se han revisado cuidadosamente y la interfaz facilita actualmente asistencia para idiomas con escritura de derecha a izquierda, como hebreo y árabe. **Se integra Ayuda en línea** en ESET Internet Security y ofrece contenido de asistencia actualizado dinámicamente.
Antivirus y antiespía	Detecta y desinfecta de forma proactiva más virus, gusanos, troyanos y rootkits, conocidos o no. La **Heurística avanzada** detecta incluso el código malicioso nunca visto hasta el momento, protegiéndole de amenazas desconocidas y neutralizándolas antes de que causen daños. **La protección del tráfico de Internet** y el **Antiphishing** funcionan supervisando la comunicación entre navegadores web y servidores remotos (incluido SSL). **La protección del cliente de correo electrónico** proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3(S) e IMAP(S).
Actualizaciones periódicas	La mejor manera de disfrutar del máximo nivel de seguridad en el ordenador es actualizar el motor de detección (anteriormente conocida como la "base de firmas de virus") y los módulos del programa de forma periódica.
ESET LiveGrid® (Reputación basada en la nube)	Puede comprobar la reputación de los procesos en ejecución y los archivos directamente desde ESET Internet Security.
Control del dispositivo	Analiza automáticamente todas las unidades flash USB, tarjetas de memoria y CD/DVD. Bloquea los medios extraíbles en función del tipo de medio, el fabricante, el tamaño y otros atributos.
Funcionalidad HIPS	Puede personalizar el comportamiento del sistema de forma mucho más precisa, especificar reglas para el registro del sistema, activar procesos y programas y ajustar su configuración de seguridad.
Modo de juego	Pospone todas las ventanas emergentes, las actualizaciones y otras actividades que utilizan gran cantidad de recursos para reservarlos para los juegos y otras actividades de pantalla completa.

Para que las características de ESET Internet Security funcionen debe haber una licencia activa. Se recomienda que renueve la licencia de ESET Internet Security unas semanas antes de que expire.

1.1 Novedades de esta versión?

La nueva versión de ESET Internet Security incorpora las siguientes mejoras:

- **Registro en un clic**: puede crear registros avanzados con un clic.
- **Análisis de la interfaz de firmware extensible unificada (UEFI)**: agrega niveles superiores de protección contra malware al detectar y eliminar amenazas que pueden iniciarse antes de que arranque el sistema operativo. Si desea obtener más información, haga clic aquí.
- **Alto rendimiento y baja repercusión en el sistema**: esta versión está diseñada para lograr un uso eficiente de los recursos del sistema, con lo que podrá disfrutar del rendimiento de su ordenador, al tiempo que se defiende de los nuevos tipos de amenazas.
- **Configuración avanzada reorganizada**: los ajustes de ESET LiveGrid® se han cambiado a la sección Motor de detección, el registro avanzado antispam se ha cambiado a la sección Diagnóstico, etc.
- **Compatibilidad mejorada con lectores de pantalla**: ESET Internet Security es compatible con los lectores de pantalla más populares (JAWS, NVDA, Narrator).
- **Arrastrar y colocar para analizar archivos**: puede analizar un archivo o una carpeta con solo moverlos a la zona marcada.
- **Recomendar el producto ESET a un amigo**: ESET Internet Security ahora ofrece bonificaciones por recomendación, así que puede compartir su experiencia con el producto ESET con sus familiares o amigos.
- ESET Internet Security ahora se instala en un formato compacto para acelerar la instalación. Una vez instalado y activado el producto, empiezan a descargarse los módulos.
- ESET Internet Security le avisa cuando se conecta a una red inalámbrica no protegida o a una red con un nivel de protección débil.

Para ver información detallada sobre las nuevas características de ESET Internet Security, lea el siguiente artículo de la base de conocimientos de ESET:
Novedades de esta versión de los productos domésticos de ESET

1.2 ¿Qué producto tengo?

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

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

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

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

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Antivirus	✔	✔	✔
Antiespía	✔	✔	✔
Bloqueador de exploits	✔	✔	✔
Protección contra ataques basados en scripts	✔	✔	✔
Antiphishing	✔	✔	✔

Protección del tráfico de Internet	✔	✔	✔
HIPS (incluida la **Protección contra ransomware**)	✔	✔	✔
Antispam		✔	✔
Cortafuegos		✔	✔
Protección de la red doméstica		✔	✔
Protección de cámara web		✔	✔
Protección contra los ataques de red		✔	✔
Protección contra botnets		✔	✔
Protección de pago y banca		✔	✔
Control parental		✔	✔
Antirrobo		✔	✔
ESET Password Manager			✔
ESET Secure Data			✔

NOTA
Puede que algunos de los productos anteriores no estén disponibles para su idioma o zona geográfica.

1.3 Requisitos del sistema

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

Procesadores compatibles

Intel® o AMD x86/x64

Sistemas operativos compatibles

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® Home Server 2011 de 64 bits

NOTA
ESET Anti-Theft no es compatible con Microsoft Windows Home Server.

1.4 Prevención

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

Actualización regular

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

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

Descarga de parches de seguridad

Los autores de software malintencionado con frecuencia explotan varias vulnerabilidades del sistema para aumentar la eficacia de la propagación de códigos malintencionados. Por ello, las empresas de software vigilan de cerca las nuevas vulnerabilidades en las aplicaciones y publican actualizaciones de seguridad para eliminar amenazas potenciales periódicamente. Es importante descargar estas actualizaciones de seguridad a medida que se publican. Microsoft Windows y los navegadores web como Internet Explorer son dos ejemplos de programas que publican de forma periódica actualizaciones de seguridad.

Copia de seguridad de los datos importantes

Normalmente, a los autores de código malicioso no les importan las necesidades de los usuarios y, con frecuencia, la actividad de los programas malintencionados provoca un funcionamiento incorrecto del sistema operativo y la pérdida de datos importantes. Es importante realizar copias de seguridad periódicas de sus datos importantes y confidenciales en una fuente externa, como un DVD o un disco duro externo. Estas precauciones facilitan y aceleran la recuperación de los datos en caso de fallo del sistema.

Análisis regular del ordenador en busca de virus

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

Seguimiento de las reglas de seguridad básicas

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

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

2. Instalación

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

- El Live installer se puede descargar del sitio web de ESET. Este paquete de instalación es universal para todos los idiomas (elija el idioma que desee). Live installer es un pequeño archivo, los archivos adicionales que necesite para instalar ESET Internet Security se descargarán automáticamente.

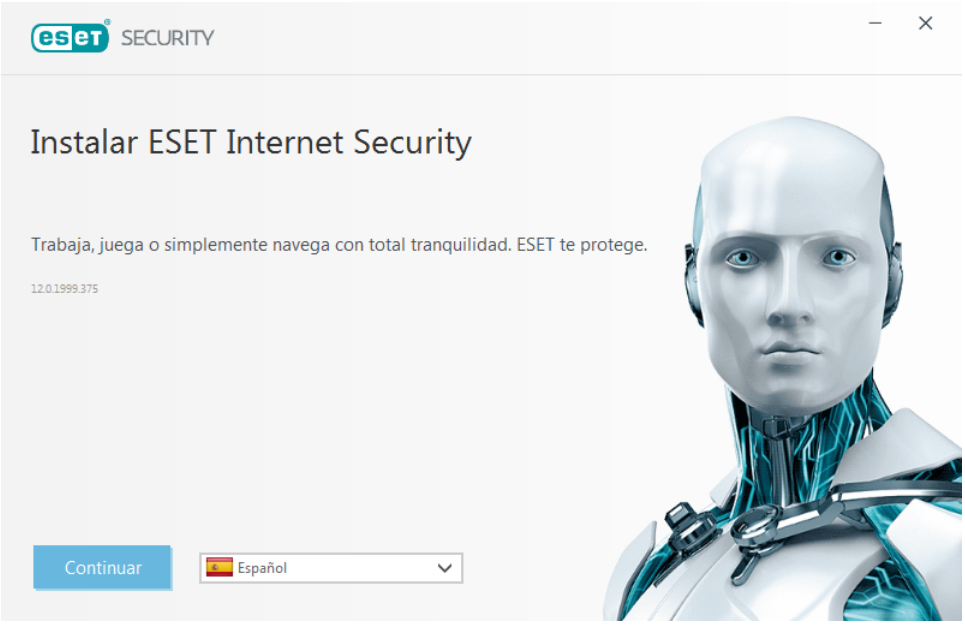
- Instalación sin conexión: este tipo de instalación se utiliza cuando se instala el producto desde un CD o DVD. Utiliza un archivo *.exe* de mayor tamaño que Live installer y que no necesita una conexión a Internet ni archivos adicionales para completar la instalación.

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

2.1 Live installer

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

IMPORTANTE
Para este tipo de instalación debe estar conectado a Internet.



Seleccione el idioma que desee en el menú desplegable y haga clic en **Continuar**. Los archivos de instalación tardarán unos momentos en descargarse.

Cuando haya aceptado el **Acuerdo de licencia para el usuario final** se le pedirá que configure **ESET LiveGrid®** y **detección de aplicaciones potencialmente indeseables**. ESET LiveGrid® ayuda a garantizar que se informe a ESET de forma continua e inmediata sobre las nuevas amenazas a fin de proteger a nuestros clientes. El sistema permite el envío de nuevas amenazas al laboratorio de investigación de ESET, donde se analizan, procesan y agregan a la base de firmas de virus.

La opción **Activar el sistema de respuesta ESET LiveGrid® (recomendado)** está seleccionada de forma predeterminada, lo que activará esta característica.

El paso siguiente del proceso de instalación consiste en configurar la detección de aplicaciones potencialmente indeseables. Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden influir negativamente en el comportamiento del sistema operativo. Consulte el capítulo Aplicaciones potencialmente indeseables para ver más detalles.

Haga clic en **Instalar** para iniciar el proceso de instalación. Esta operación puede tardar un rato. Haga clic en **Finalizar** para completar la configuración del producto y comenzar el proceso de activación.

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

NOTA
Si dispone de una licencia que le permite instalar otras versiones de un producto, podrá seleccionar el producto que desee según sus preferencias. Para obtener más información sobre las características de cada producto, haga clic aquí.

2.2 Instalación sin conexión

Una vez iniciada la instalación sin conexión (.exe), el asistente de instalación le proporcionará instrucciones para realizar la configuración.

Seleccione el idioma que desee en el menú desplegable y haga clic en **Instalar**.

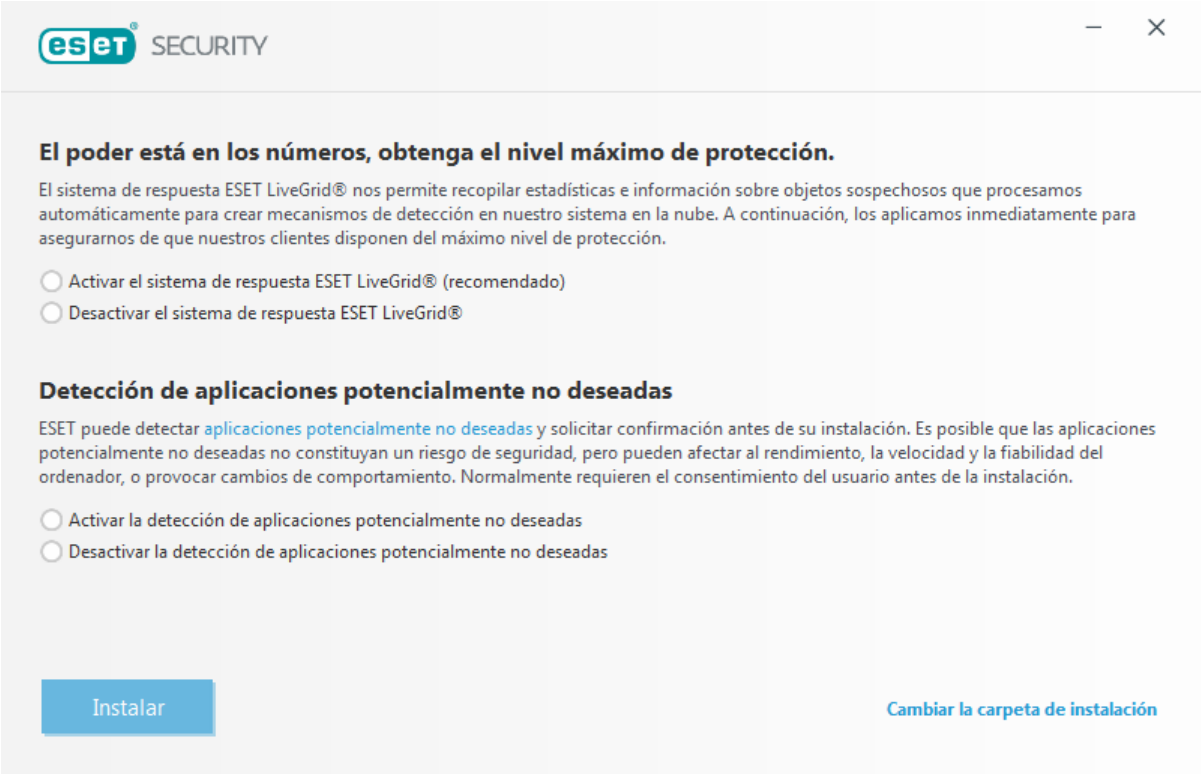
Tras aceptar el **Acuerdo de licencia para el usuario final** se le pedirá que **introduzca una clave de licencia** o **utilice el administrador de licencias**.

Si aún no tiene una licencia, seleccione **Prueba gratuita** para probar el producto ESET durante un periodo de tiempo limitado, o seleccione **Adquirir licencia**. También puede seleccionar **Omitir activación** para continuar con la instalación sin activar el producto; se le pedirá la clave de licencia más adelante.

2.2.1 Introduzca una clave de licencia

En el Asistente de instalación, seleccione el producto que desee instalar según su clave de licencia y visualice el nombre del producto durante la instalación. Para ver una lista de los productos con los que puede activarse la licencia, haga clic en **Cambiar producto**. Para obtener más información sobre las características de cada producto, haga clic aquí.

Haga clic en **Continuar** y seleccione la configuración que desee para **ESET LiveGrid®** y **Detección de aplicaciones potencialmente indeseables**. **ESET LiveGrid®** ayuda a garantizar que se informe a ESET de forma continua e inmediata sobre las nuevas amenazas a fin de proteger a nuestros clientes. El sistema permite el envío de nuevas amenazas al laboratorio de investigación de ESET, donde se analizan, procesan y agregan a la base de firmas de virus. Las **aplicaciones potencialmente indeseables** no tienen por qué ser maliciosas, pero pueden influir negativamente en el comportamiento del sistema operativo. Consulte el capítulo Aplicaciones potencialmente indeseables para ver más detalles.



Haga clic en **Instalar** para iniciar el proceso de instalación. Esta operación puede tardar un rato. Haga clic en **Finalizar** para completar la configuración del producto y comenzar el proceso de activación.

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

NOTA
Si tiene una licencia que permite seleccionar entre varios productos, puede instalar el que desee. Para obtener más información sobre las características de cada producto, haga clic aquí.

Si desea más instrucciones sobre los pasos de la instalación, **ESET LiveGrid®** y **Detección de aplicaciones potencialmente indeseables**, siga las instrucciones de la sección mencionada "Live installer".

2.2.2 Usar Administrador de licencias

Tras seleccionar **Usar Administrador de licencias** se le pedirán las credenciales de my.eset.com en una ventana nueva. Introduzca sus credenciales de my.eset.com y haga clic en **Iniciar sesión** para usar una licencia en el Administrador de licencias. Elija una licencia para la activación, haga clic en **Continuar** y se activará su instancia de ESET Internet Security.

NOTA
Si aún no tiene una cuenta de my.eset.com, haga clic en el botón **Crear cuenta** para registrarse.

NOTA
Si ha olvidado la contraseña, haga clic en **He olvidado mi contraseña** y siga los pasos indicados en la página web a la que se le redirigirá.

El Administrador de licencias de ESET le ayuda a gestionar las licencias de ESET. De una forma sencilla podrá renovar, ampliar o prorrogar la licencia y ver detalles importantes sobre la misma. Introduzca la clave de licencia. A continuación verá el producto, el dispositivo asociado, el número de puestos disponibles y la fecha de caducidad. Puede desactivar o renombrar los dispositivos que quiera. Al hacer clic en **Renovar** se le redirigirá a la tienda en línea, en la que puede confirmar la compra y comprar la renovación.

Si desea ampliar la licencia (por ejemplo de ESET NOD32 Antivirus a ESET Smart Security Premium) o desea instalar el producto de seguridad de ESET en otro dispositivo, se le redirigirá a una tienda en línea para que realice la compra.

En el Administrador de licencias de ESET también puede agregar diferentes licencias, descargar productos en sus dispositivos.

2.2.3 Cómo cambiar la carpeta de instalación

Después de seleccionar **Cambiar la carpeta de instalación**, se le pedirá que seleccione una ubicación para la instalación. De forma predeterminada, el programa se instala en el directorio siguiente:

C:\Archivos de programa\ESET\ESET Internet Security

Haga clic en **Examinar** para cambiar esta ubicación (no recomendado).

Para completar los siguientes pasos de la instalación, **ESET LiveGrid®** y **Detección de aplicaciones potencialmente indeseables**, siga las instrucciones de la sección del instalador en directo (consulte "Live installer").

Haga clic en **Continuar** y, a continuación, en **Instalar** para finalizar la instalación.

2.3 Problemas de instalación comunes

Si ocurren problemas durante la instalación, consulte nuestra lista de errores de instalación comunes y resoluciones para encontrar una solución para su problema.

2.4 Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto.

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

- Si ha adquirido una versión en caja física del producto, active su producto con una **clave de licencia**. Normalmente, la clave de licencia se encuentra en el interior o en la parte posterior del paquete del producto. Para una correcta activación, la clave de licencia se debe introducir tal como se proporciona. Clave de licencia: se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX y sirve para identificar al propietario de la licencia y activar la licencia.
- Tras seleccionar **Usar Administrador de licencias** se le pedirán las credenciales de my.eset.com en una ventana nueva.
- Si desea evaluar ESET Internet Security antes de adquirir el producto, seleccione la opción **Prueba gratuita**. Introduzca su dirección de correo electrónico y el país para activar ESET Internet Security durante un período de tiempo limitado. Recibirá la licencia de prueba por correo electrónico. Las licencias de prueba solo se pueden activar una vez por cliente.
- Si no tiene una licencia y quiere adquirir una, haga clic en Comprar licencia. Será redirigido al sitio web del distribuidor local de ESET.

2.5 Introducción de la clave de licencia

Las actualizaciones automáticas son importantes para su seguridad. ESET Internet Security solo recibirá las actualizaciones cuando se active con la **Clave de licencia**.

Si no introduce la clave de licencia tras la instalación del producto, este no se activará. Puede cambiar la licencia en la ventana principal del programa. Para ello, haga clic en **Ayuda y soporte técnico** > **Activar licencia**, e introduzca los datos de licencia que se le proporcionaron con el producto de seguridad de ESET en la ventana Activación del producto.

Cuando introduzca su **clave de licencia**, es importante que la escriba exactamente tal y como está escrita:

- La clave de licencia es una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.

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

2.6 Recomendar el producto ESET a un amigo

Esta versión de ESET Internet Security ahora ofrece bonificaciones por recomendación, así que puede compartir su experiencia con el producto ESET con sus familiares o amigos y enviar recomendaciones incluso desde un producto activado con una licencia de prueba. Por cada recomendación correcta que genere la activación de un producto, tanto usted como su amigo recibirán un mes más de protección total.

Puede enviar recomendaciones desde su ESET Internet Security instalado. Los productos que puede recomendar varían en función del producto desde el que envía la recomendación; vea la tabla mostrada a continuación.

Su producto instalado	Producto que puede recomendar
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Recomendación de un producto

Para enviar un vínculo de recomendación, haga clic en **Recomendar a su amigo** en el menú principal de ESET Internet Security. Haga clic en **Recomendar mediante vínculo**. Su producto generará un vínculo de recomendación que se mostrará en una ventana nueva. Copie el vínculo y envíeselo a sus familiares y amigos. Hay varias formas de compartir su vínculo de recomendación: directamente desde su producto ESET, a través de **Google+**, enviándolo a sus contactos de **Gmail** o publicándolo en **Facebook**.

Cuando su amigo hace clic en el vínculo de recomendación que le ha enviado, se le redirigirá a una página web en la que puede descargar el producto (si es un usuario nuevo) o ampliar su licencia de prueba durante un mes más. Usted recibirá una notificación por cada vínculo de recomendación que se active correctamente, y su licencia se ampliará automáticamente un mes más. Puede consultar el número de vínculos de referencia activados correctamente en la ventana **Recomendar a su amigo** de su producto ESET.

2.7 Actualización a una versión más reciente

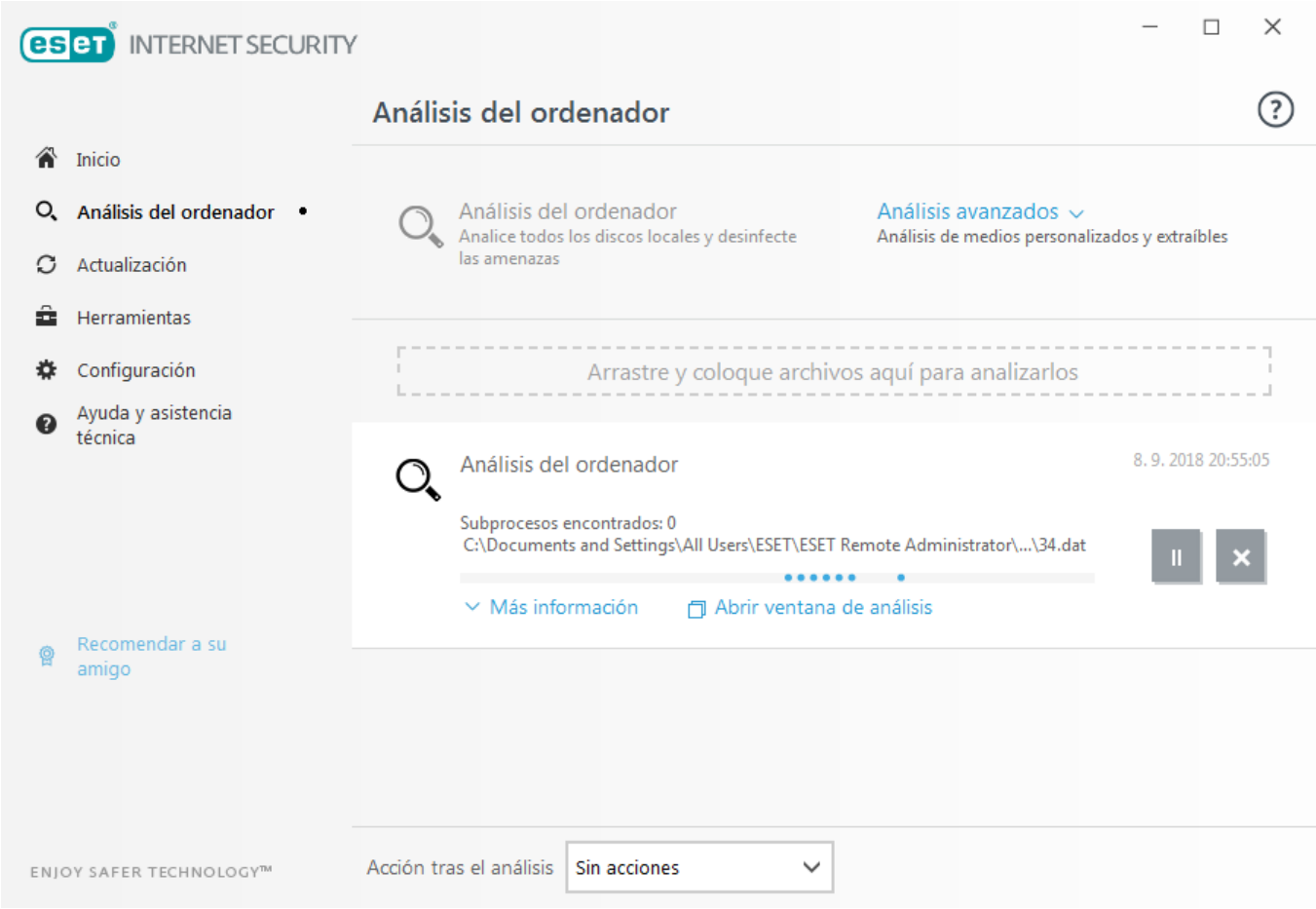
Las versiones nuevas de ESET Internet Security implementan mejoras o solucionan problemas que no se pueden arreglar con las actualizaciones automáticas de los módulos de programa. La actualización a una versión más reciente se puede realizar de varias maneras:

1. Actualización automática mediante una actualización del programa.
   Las actualizaciones del programa se distribuyen a todos los usuarios y pueden afectar a determinadas configuraciones del sistema, de modo que se envían tras un largo periodo de pruebas que garantizan su funcionalidad en todas las configuraciones posibles del sistema. Si necesita instalar una versión más reciente en cuanto se publica, utilice uno de los métodos que se indican a continuación.
2. Actualización manual, haciendo clic en **Buscar actualizaciones** en la sección **Actualizar**.
3. Actualización manual mediante la descarga e instalación de una versión más reciente sobre la instalación existente.

2.8 Analizar primero tras la instalación

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

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



3. Guía para principiantes

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

3.1 Ventana principal del programa

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

A continuación, se muestra una descripción de las opciones del menú principal:

Inicio: proporciona información sobre el estado de protección de ESET Internet Security.

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

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

Herramientas: proporciona acceso a Archivos de registro, Estadísticas de protección, Observar actividad, Procesos en ejecución, Conexiones de red, Planificador de tareas, ESET SysInspector y ESET SysRescue.

Configuración: seleccione esta opción para definir el nivel de seguridad para Ordenador, Internet, Protección de la red y Herramientas de seguridad.

Ayuda y soporte: proporciona acceso a los archivos de ayuda, la Base de conocimiento de ESET y el sitio web de ESET, así como vínculos para enviar una solicitud de soporte técnico.

La pantalla **Inicio** contiene información importante sobre el nivel de protección actual del ordenador. En la ventana de estado se muestran las características más habituales de ESET Internet Security. Aquí también se muestra información sobre la actualización más reciente y la fecha de expiración del programa.

El icono verde y el estado **Máxima protección** verde indican que se garantiza la máxima protección.

¿Qué hacer si el programa no funciona correctamente?

Si un módulo de protección activa funciona correctamente, su icono de estado de la protección será verde. Un signo de exclamación rojo o un icono de notificación naranja indican que no se garantiza el nivel de protección máximo. En **Inicio** se mostrará información adicional acerca del estado de protección de cada módulo, así como soluciones sugeridas para restaurar la protección completa. Para cambiar el estado de módulos individuales, haga clic en **Configuración** y seleccione el módulo que desee.

El icono rojo y el estado La protección máxima no está asegurada indican problemas críticos. Existen varios motivos para que se muestre este estado, por ejemplo:

- **Producto no activado**: puede activar ESET Internet Security desde **Inicio** haciendo clic en **Activar producto** o en **Comprar ahora**, debajo del Estado de la protección.
- **El Motor de detección no está actualizado**: este error aparecerá tras varios intentos sin éxito de actualizar la base de firmas de virus. Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.
- **La protección antivirus y antiespía está desactivada**: puede volver a activar la protección antivirus y antiespía haciendo clic en **Activar la protección antivirus y antiespía**.
- **Cortafuegos personal de ESET desactivado**: este problema también se indica mediante una notificación de seguridad junto al elemento **Red** del escritorio. Puede volver a activar la protección de red haciendo clic en **Activar cortafuegos**.
- **La licencia ha caducado**: esto se indica mediante un icono de estado de la protección. Una vez que expire la licencia, el programa no se puede actualizar. Siga las instrucciones de la ventana de alerta para renovar la licencia.

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

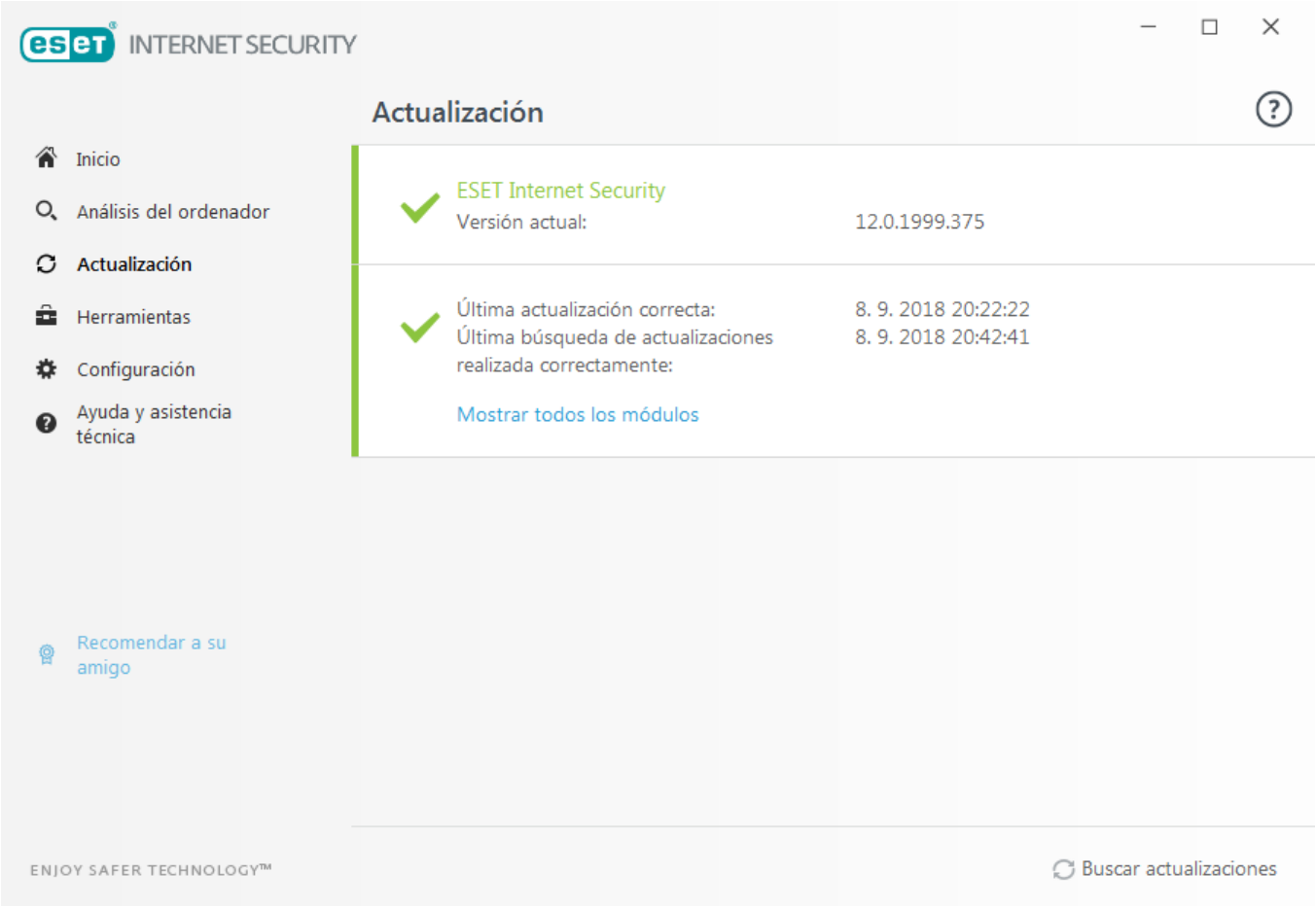
- **Modo de juego activo**: la activación del Modo de juego es un posible riesgo para la seguridad. Al activar esta característica se desactivan todas las ventanas emergentes y se detiene cualquier tarea planificada.
- **Su licencia caducará en breve**: esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación junto al reloj del sistema. Cuando expire la licencia, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.

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

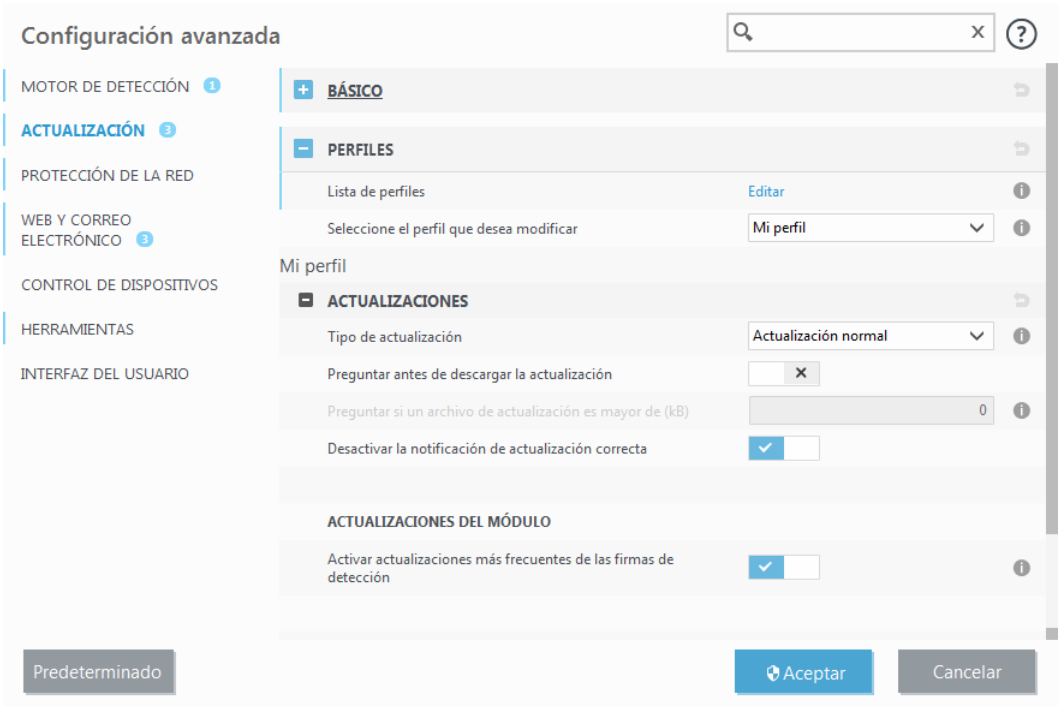
3.2 Actualizaciones

La actualización del motor de detección y los componentes del programa es una parte importante a la hora de proteger su sistema frente a código malicioso. Preste especial atención a su configuración y funcionamiento. En el menú principal, haga clic en **Actualizar** y, a continuación, en **Buscar actualizaciones** para comprobar si hay alguna actualización del motor de detección.

Si no ha introducido la clave de licencia durante la activación de ESET Internet Security, se le pedirá que lo haga ahora.



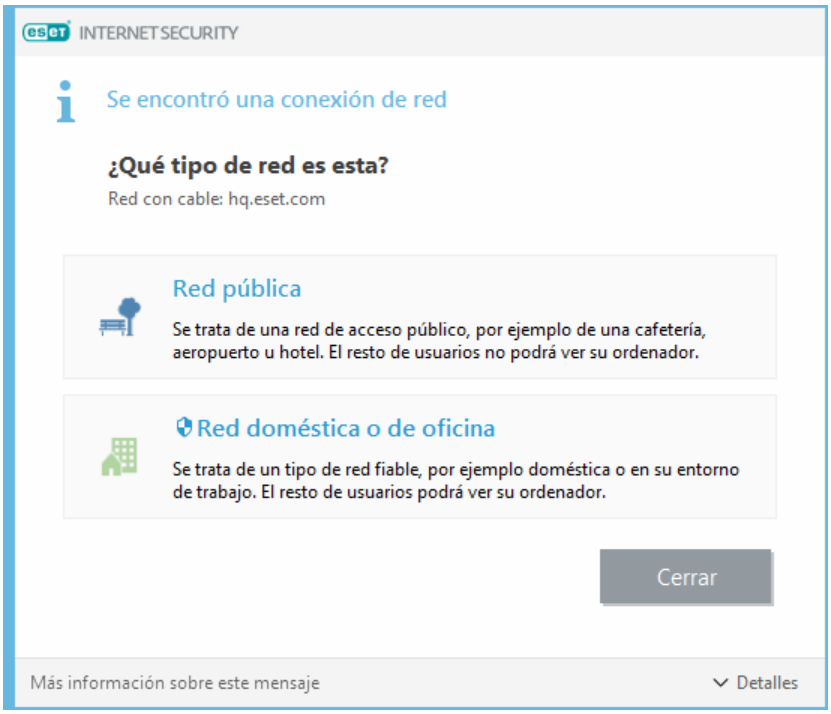
La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Configuración avanzada**, o pulse **F5** en el teclado) ofrece más opciones de actualización. Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor proxy y las conexiones de red local, haga clic en la ficha en cuestión de la ventana **Actualizar**.



3.3 Configuración de la zona de confianza

Es necesario configurar las zonas de confianza con el fin de proteger el ordenador en entornos de red. Puede permitir que otros usuarios accedan a su ordenador mediante la activación del uso compartido al configurar zonas de confianza. Haga clic en **Configuración** > **Protección de la red** > **Redes conectadas** y haga clic en el vínculo debajo de la red conectada. Se abrirá una ventana con opciones para elegir el modo de protección que aplicar al ordenador en la red.

La zona de confianza se detecta después de instalar ESET Internet Security y cada vez que el ordenador se conecta a una red nueva. Por lo tanto, no suele ser necesario definir zonas de confianza. De forma predeterminada, cuando se detecta una nueva zona, un cuadro de diálogo le pedirá que establezca el nivel de protección de dicha zona.



ADVERTENCIA
La configuración incorrecta de la zona de confianza puede exponer su ordenador a ciertos riesgos.

NOTA
De forma predeterminada, se concede acceso a las estaciones de trabajo de una zona de confianza para compartir archivos e impresoras, tener activada la comunicación RPC entrante y disfrutar del uso compartido de escritorio remoto.

Para obtener más información sobre esta característica, lea el siguiente artículo de la base de conocimiento de ESET: Detección de una nueva conexión de red en ESET Smart Security

3.4 Antirrobo

Para localizar su ordenador en caso de pérdida o robo, elija entre las siguientes opciones para registrar el ordenador en ESET Anti-Theft.

1. Tras una activación correcta, haga clic en **Activar Antirrobo** para activar las funciones de ESET Anti-Theft en el ordenador que acaba de registrar.
2. Si ve el mensaje **ESET Anti-Theft disponible** en el panel **Inicio** de ESET Internet Security, piense en activar esta característica en su ordenador. Haga clic en **Activar ESET Anti-Theft** para registrar su ordenador con ESET Anti-Theft.
3. Desde la ventana principal del programa, haga clic en **Configuración** > **Herramientas de seguridad.** Haga clic en junto a **ESET Anti-Theft** y siga las instrucciones de la ventana emergente.

NOTA
ESET Anti-Theft no es compatible con Microsoft Windows Home Server.

Para obtener más instrucciones sobre cómo enlazar el ordenador con ESET Anti-Theft, consulte Cómo agregar un dispositivo nuevo.

3.5 Herramientas de control parental

Si ya ha activado el control parental en ESET Internet Security, debe configurarlo para las cuentas de usuario que desee a fin de que funcione adecuadamente.

Si los controles parentales están activados, pero no se han configurado las cuentas de usuario, se mostrará **El control parental no está configurado** en el panel **Inicio** de la ventana principal del programa. Haga clic en **Configurar reglas** y consulte el capítulo Control parental si desea información sobre cómo crear restricciones específicas para proteger a sus hijos del material potencialmente ofensivo.

4. Trabajo con ESET Internet Security

Las opciones de configuración de ESET Internet Security le permiten ajustar los niveles de protección del ordenador y la red.

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

Protección del ordenador

Protección de Internet

Protección de la red

Herramientas de seguridad

Haga clic en un componente para ajustar la configuración avanzada del correspondiente módulo de protección.

La configuración de **protección del ordenador** le permite activar o desactivar los siguientes componentes:

- **Protección del sistema de archivos en tiempo real**: todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador.
- **HIPS**: el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.
- **Modo de juego**: activa o desactiva el Modo de juego. Cuando se active el modo de juego, recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal se volverá naranja.
- **Protección de cámara web**: controla los procesos y las aplicaciones que acceden a la cámara conectada al ordenador. Si desea obtener más información, haga clic aquí.

La configuración de **protección de Internet** le permite activar o desactivar los siguientes componentes:

- **Protección del acceso a la Web**: si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso.
- **Protección de clientes de correo electrónico**: supervisa comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Antispam**: analiza el correo electrónico no solicitado (spam).
- **Protección Antiphishing**: filtra los sitios web sospechosos de distribuir contenido destinado a manipular a los usuarios para que envíen información confidencial.

En la sección **Protección de la red** puede activar o desactivar el Cortafuegos, la Protección contra los ataques de red (IDS) y la Protección contra botnets.

La configuración de Herramientas de seguridad permite ajustar los siguientes módulos:

- Protección de pagos y banca online
- Control parental
- Antirrobo

El control parental le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo. Asimismo, los padres pueden prohibir el acceso a más de 40 categorías predefinidas y más de 140 subcategorías de sitios web.

Para volver a activar la protección de un componente de seguridad desactivado, haga clic en el control deslizante  para que muestre una marca de verificación verde  .

NOTA
Si desactiva la protección con este método, todos los módulos desactivados de la protección se activarán al reiniciar el ordenador.

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

4.1 Protección del ordenador

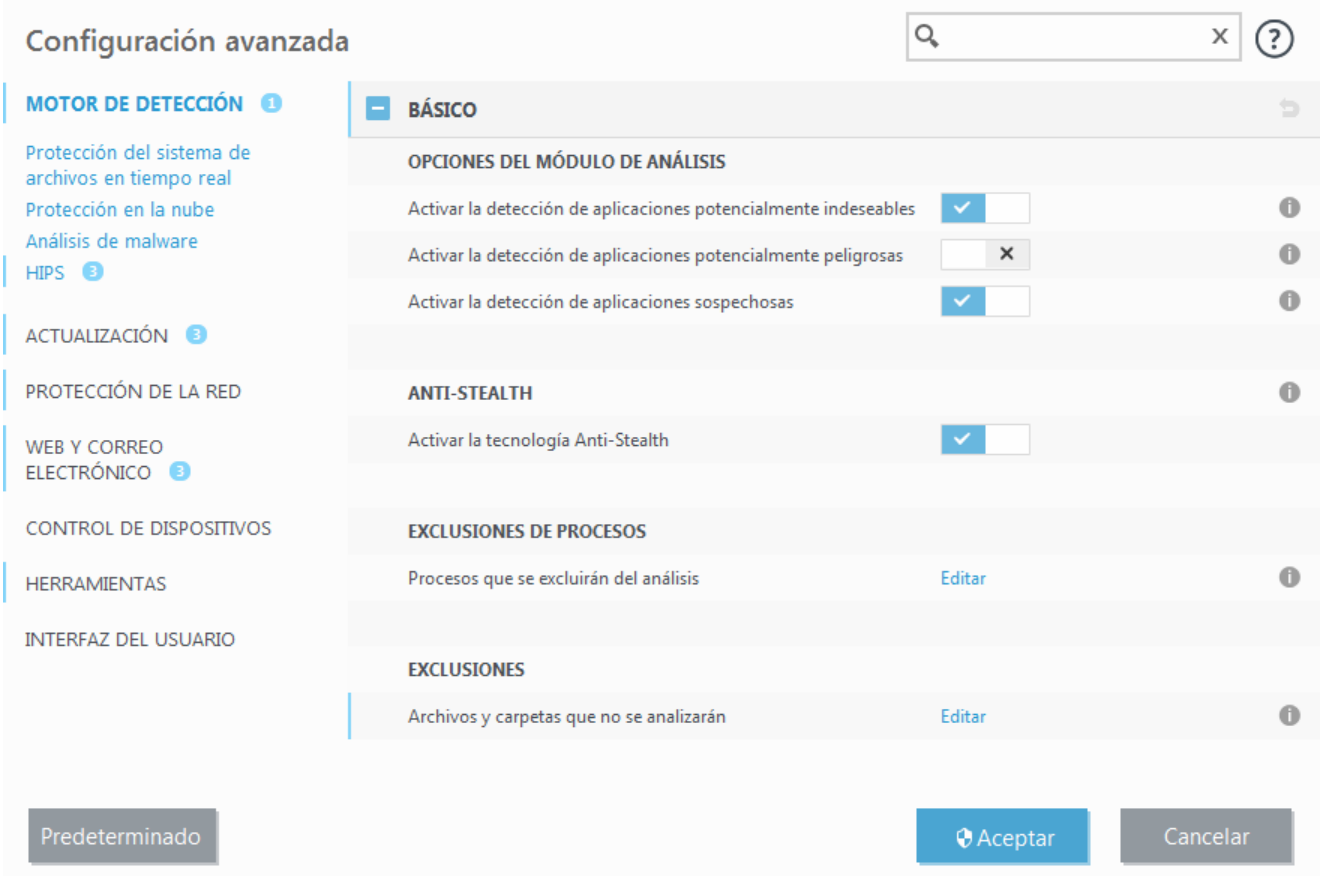
Haga clic en Protección del ordenador en la ventana Configuración para consultar una descripción general de todos los módulos de protección. Para desactivar temporalmente módulos individuales, haga clic en . Tenga en cuenta que esto puede disminuir el nivel de protección del ordenador. Haga clic en junto a un módulo de protección para acceder a la configuración avanzada para ese módulo.

Haga clic en > **Modificar exclusiones**, situado junto a **Protección del sistema de archivos en tiempo real**, para abrir la ventana de configuración Exclusión, que permite excluir archivos y carpetas del análisis.

Pausar la protección antivirus y antiespía: desactiva todos los módulos de protección antivirus y antiespía. Cuando desactive la protección, se abrirá una ventana en la que puede determinar cuánto tiempo permanecerá desactivada mediante el menú desplegable **Intervalo de tiempo**. Haga clic en **Aplicar** para confirmar.

4.1.1 Motor de detección

La protección antivirus protege contra ataques maliciosos al sistema mediante el control de las comunicaciones por Internet, el correo electrónico y los archivos. Si se detecta una amenaza con código malicioso, el módulo antivirus puede bloquearlo para después desinfectarlo, eliminarlo o ponerlo en cuarentena.



Las **Opciones de análisis** para todos los módulos de protección (p. ej. protección del sistema de archivos en tiempo real, protección del tráfico de Internet, etc.) le permiten activar o desactivar la detección de lo siguiente:

- Las **aplicaciones potencialmente indeseables** (PUA) no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
- Por **aplicaciones potencialmente peligrosas** se entienden programas de software comercial legítimo que tienen el potencial de usarse con fines maliciosos. Entre los ejemplos de este tipo de programas encontramos herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Esta opción está desactivada de manera predeterminada.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
- Entre las **aplicaciones sospechosas** se incluyen programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia explotan estos tipos de protectores para evitar ser detectados.

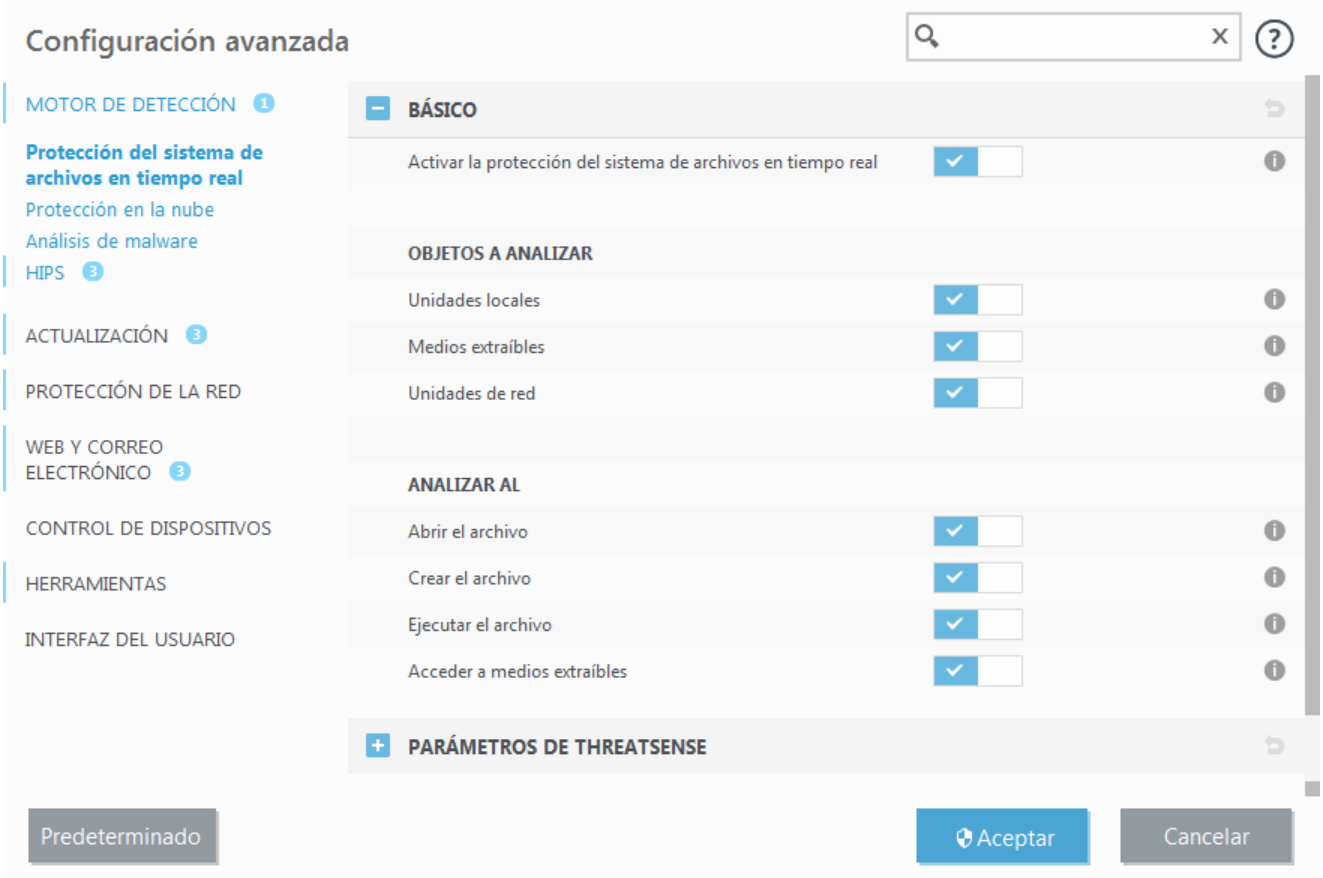
La **tecnología AntiStealth** es un sofisticado sistema de detección de programas peligrosos como rootkits, que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.

Las **exclusiones** le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Puede que haya situaciones en las que necesite excluir un objeto, como durante el análisis de entradas de una base de datos grande que ralentice el ordenador o software que entre en conflicto con el análisis. Para excluir un objeto del análisis, consulte Exclusiones.

Activar análisis avanzado mediante AMSI: herramienta Interfaz de análisis contra el código malicioso de Microsoft que permite que los desarrolladores de aplicaciones creen nuevas defensas contra el código malicioso (solo para Windows 10).

4.1.1.1 Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con el antivirus en el sistema. Todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. La protección del sistema de archivos en tiempo real se inicia al arrancar el sistema.



La protección del sistema de archivos en tiempo real comienza de forma predeterminada cuando se inicia el sistema y proporciona un análisis ininterrumpido. En casos especiales (por ejemplo, si hay un conflicto con otro análisis en tiempo real), puede desactivar la protección en tiempo real anulando la selección de **Activar la protección del sistema de archivos en tiempo real**, en la sección **Configuración avanzada** de **Protección del sistema de archivos en tiempo real** > **Básico**.

Objetos a analizar

De forma predeterminada, se buscan posibles amenazas en todos los tipos de objetos:

Unidades locales: controla todas las unidades de disco duro del sistema.
Medios extraíbles: controla los discos CD y DVD, el almacenamiento USB, los dispositivos Bluetooth, etc.
Unidades de red: analiza todas las unidades asignadas.

Recomendamos que esta configuración predeterminada se modifique solo en casos específicos como, por ejemplo, cuando el control de ciertos objetos ralentiza significativamente las transferencias de datos.

Analizar al ...

De forma predeterminada, todos los archivos se analizan cuando se abren, crean o ejecutan. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador:

- **Abrir el archivo**: activa o desactiva el análisis al abrir archivos.
- **Crear el archivo**: activa o desactiva el análisis durante la creación de archivos.
- **Ejecutar el archivo**: activa o desactiva el análisis cuando se ejecutan archivos.
- **Acceso a medios extraíbles**: activa o desactiva el análisis activado por el acceso a determinados medios extraíbles con espacio de almacenamiento.

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y se activa con varios sucesos del sistema como, por ejemplo, cuando se accede a un archivo. Si se utilizan métodos de detección con la tecnología ThreatSense (tal como se describe en la sección Configuración de parámetros del motor ThreatSense), la protección del sistema de archivos en tiempo real se puede configurar para que trate de forma diferente los archivos recién creados y los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se analizan de nuevo inmediatamente tras cada actualización del motor de detección. Este comportamiento se controla con la opción **Optimización inteligente**. Si la opción **Optimización inteligente** está desactivada, se analizan todos los archivos cada vez que se accede a ellos. Para modificar esta configuración, pulse **F5** para abrir **Configuración avanzada** y despliegue **Motor de detección** > **Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetros de ThreatSense** > **Otros** y seleccione o anule la selección de **Activar optimización inteligente**.

4.1.1.1.1 Parámetros adicionales de ThreatSense

Parámetros adicionales de ThreatSense para archivos nuevos y modificados

La probabilidad de infección en archivos modificados o recién creados es superior que en los archivos existentes. Por eso el programa comprueba estos archivos con parámetros de análisis adicionales. ESET Internet Security utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización del motor de detección en combinación con métodos de análisis basados en firmas. Además de los archivos nuevos, el análisis se realiza también en **archivos de autoextracción** (.sfx) y **empaquetadores en tiempo real** (archivos ejecutables comprimidos internamente). Los archivos se analizan, de forma predeterminada, hasta el 10.º nivel de anidamiento; además, se analizan independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, anule la selección de la opción **Configuración por defecto para archivos comprimidos**.

Parámetros adicionales de ThreatSense para los archivos ejecutados

Heurística avanzada para los archivos ejecutados: de forma predeterminada, se utiliza la Heurística avanzada al ejecutar archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET LiveGrid® con el fin de mitigar su repercusión en el rendimiento del sistema.

Heurística avanzada al ejecutar archivos desde las unidades extraíbles: la heurística avanzada emula el código en un entorno virtual y evalúa su comportamiento antes de permitir la ejecución del código desde soportes extraíbles.

4.1.1.1.2 Niveles de desinfección

La protección en tiempo real tiene tres niveles de desinfección (para acceder a la configuración de niveles de desinfección, haga clic en **Configuración de los parámetros del motor ThreatSense** en la sección **Protección del sistema de archivos en tiempo real** y, a continuación, en **Desinfección**).

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción. Este nivel es adecuado para usuarios avanzados que conocen los pasos necesarios en caso de amenaza.

Desinfección normal: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (según el tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección estricta: el programa desinfecta o elimina todos los archivos infectados. Las únicas excepciones son los

archivos del sistema. Si no es posible desinfectarlos, se insta al usuario a que seleccione una acción indicada en una ventana de alerta.

ADVERTENCIA
Si un archivo comprimido contiene archivos infectados, se puede tratar de dos maneras: en el modo estándar (Desinfección normal), se elimina el archivo comprimido completo si este está compuesto únicamente por código malicioso; y en el modo **Desinfección exhaustiva**, el archivo se elimina si contiene al menos una porción de código malicioso, independientemente del estado de los demás archivos.

4.1.1.1.3 Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más importante para mantener un sistema seguro, por lo que debe tener cuidado cuando modifique los parámetros correspondientes. Es aconsejable que los modifique únicamente en casos concretos.

Una vez que se ha instalado ESET Internet Security, se optimiza toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en junto a las diferentes fichas de la ventana (**Configuración avanzada** > **Motor de detección** > **Protección del sistema de archivos en tiempo real**).

4.1.1.1.4 Análisis de protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, utilice el archivo de prueba de eicar.com., un archivo inofensivo detectable por todos los programas antivirus. El archivo fue creado por la compañía EICAR (European Institute for Computer Antivirus Research, Instituto europeo para la investigación de antivirus de ordenador) para probar la funcionalidad de los programas antivirus. Este archivo se puede descargar en http://www.eicar.org/download/eicar.com.

NOTA
Antes de realizar un análisis de protección en tiempo real, es necesario desactivar el cortafuegos. Si está activado, detectará el archivo y no dejará que los archivos de prueba se descarguen.

4.1.1.1.5 Qué debo hacer si la protección en tiempo real no funciona

En este capítulo, describimos los problemas que pueden surgir cuando se utiliza la protección en tiempo real y cómo resolverlos.

Protección en tiempo real desactivada

Si un usuario desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para volver a activar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del ordenador** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no se activa al iniciar el sistema, probablemente se deba a que la opción **Activar la protección del sistema de archivos en tiempo real** está desactivada. Para garantizar que esta opción esté activada, vaya a **Configuración avanzada** (**F5**) y haga clic en **Motor de detección** > **Protección del sistema de archivos en tiempo real**.

Si la protección en tiempo real no detecta ni desinfecta amenazas

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si dos programas antivirus están instalados simultáneamente, pueden entrar en conflicto entre sí. Recomendamos que desinstale del sistema cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y la opción **Activar la protección del sistema de archivos en tiempo real** está activada), es posible que se deba a conflictos con otros programas. Para obtener ayuda para resolver este problema, póngase en contacto con el Servicio de atención al cliente de ESET.

4.1.1.2 Análisis del ordenador

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

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

Análisis del ordenador

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

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

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

Análisis personalizado

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

Análisis de medios extraíbles

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

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

Repetir el último análisis

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

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

NOTA
Le recomendamos que ejecute un análisis del ordenador una vez al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas** > **Más herramientas** > **Planificador de tareas**. ¿Cómo programar un análisis del ordenador semanal?

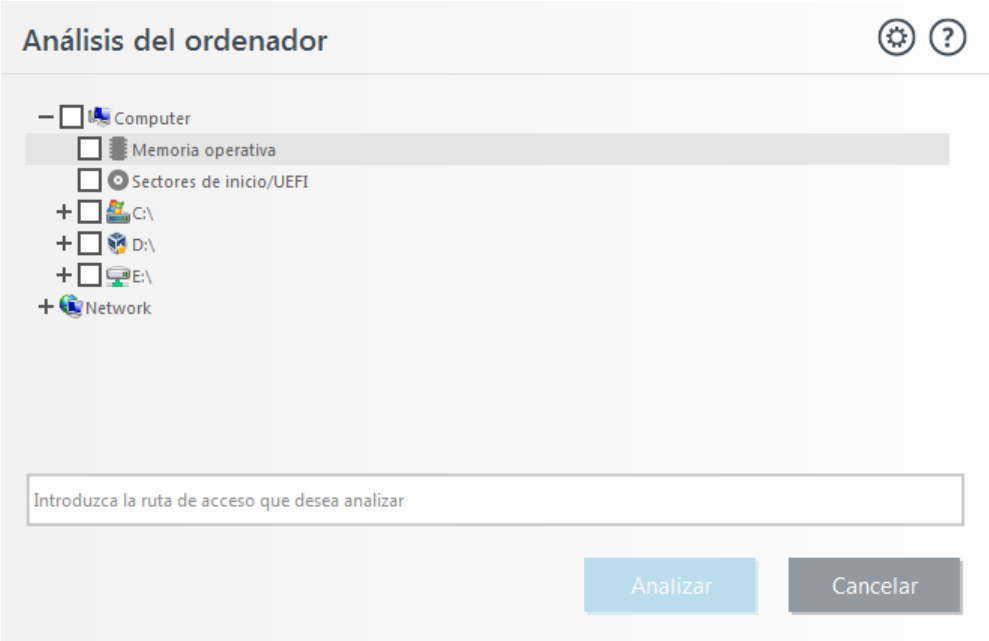
4.1.1.2.1 Iniciador del análisis personalizado

Puede utilizar el Análisis personalizado para analizar determinadas partes de un disco, en lugar del disco al completo. Para ello, haga clic en **Análisis avanzados** > **Análisis personalizado** y elija una opción en el menú desplegable **Objetos de análisis** o seleccione objetos específicos en la estructura de carpetas (árbol).

En el menú desplegable **Objetos de análisis**, puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos especificados por el perfil de análisis seleccionado.
- **Unidades extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Sin selección**: cancela todas las selecciones.

Para acceder rápidamente a un objeto de análisis o agregar directamente carpetas o archivos, introdúzcalos en el campo en blanco disponible debajo de la lista de carpetas. Si no se ha seleccionado ningún objeto en la estructura de árbol y el menú **Objetos de análisis** está definido en **Sin selección**, no podrá hacerlo.



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

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

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

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

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

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

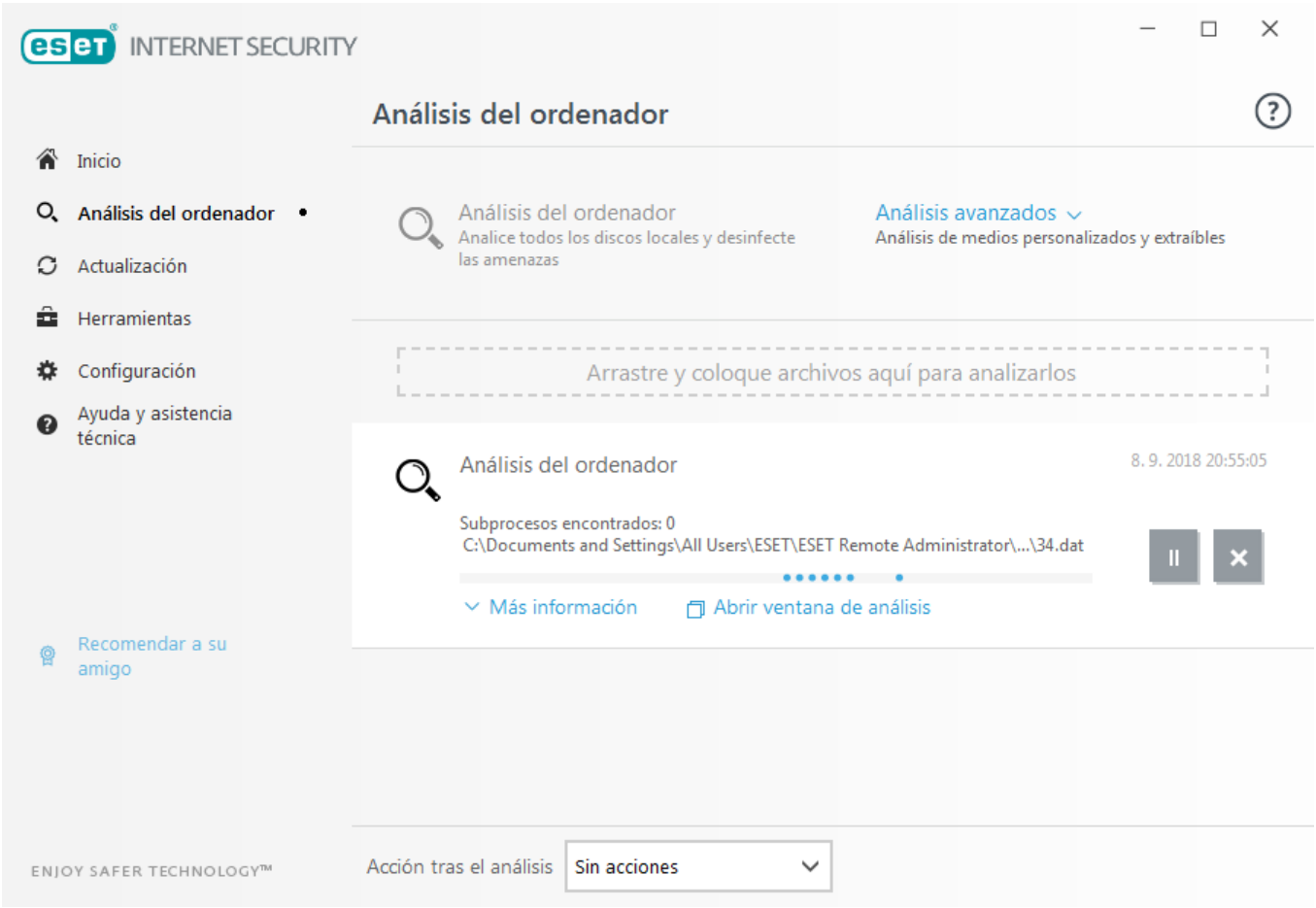
4.1.1.2.2 Progreso del análisis

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

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

Progreso del análisis: la barra de progreso muestra el estado de objetos ya analizados en comparación con el porcentaje de objetos pendientes. El estado de progreso del análisis se calcula a partir del número total de objetos incluidos en el análisis.
Destino: el nombre y la ubicación del objeto que se está analizando.
Amenazas encontradas: muestra el número total de objetos analizados, las amenazas encontradas y las desinfectadas durante un análisis.
Pausa: pone el análisis en pausa.
Reanudar: esta opción está visible cuando el progreso del análisis está en pausa. Haga clic en **Continuar** para proseguir con el análisis.
Detener: termina el análisis.
Desplazarse por el registro de exploración: si esta opción está activada, el registro de análisis se desplaza automáticamente a medida que se añaden entradas nuevas, de modo que se visualizan las entradas más recientes.

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



Acción tras el análisis: activa un apagado, reinicio o suspensión programados al finalizar el análisis del ordenador. Cuando finalice el análisis, se abrirá un cuadro de diálogo de confirmación de apagado con un tiempo de espera de 60 segundos.

4.1.1.2.3 Perfiles de análisis

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

Para crear un perfil nuevo, abra la ventana Configuración avanzada (F5) y haga clic en **Motor de detección** > **Análisis de malware** > **Análisis a petición** > **Lista de perfiles**. En la ventana **Administrador de perfiles** encontrará el menú desplegable **Perfil seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección Configuración de parámetros del motor ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

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

4.1.1.2.4 Registro de análisis del ordenador

El registro de análisis del ordenador contiene información general sobre el análisis, como la siguiente:

- Hora de finalización
- Tiempo total de análisis
- Número de amenazas detectadas
- Número de objetos analizados
- Discos, carpetas y archivos analizados
- Fecha y hora del análisis
- Versión del motor de detección

4.1.1.3 Análisis en estado inactivo

Activar análisis de estado inactivo: esta opción realizará un análisis completo del ordenador cuando este no se esté utilizando.

De forma predeterminada, el análisis de estado inactivo no se ejecutará si el ordenador (portátil) está funcionando con batería. Puede anular este ajuste con la función **Ejecutar aunque el ordenador esté funcionando con la batería**.

Active la opción **Activar el registro de sucesos** para guardar un informe del análisis del ordenador en la sección Archivos de registro (en la ventana principal del programa, haga clic en **Herramientas** > **Más herramientas** > **Archivos de registro** y seleccione **Análisis del ordenador** en el menú desplegable **Registro**).

La **detección de estado inactivo** se ejecutará cuando el ordenador se encuentre en uno de los estados siguientes:

- Pantalla apagada o con protector de pantalla
- Bloqueo de equipo
- Cierre de sesión de usuario

Haga clic en Parámetros de ThreatSense para modificar los parámetros de análisis (por ejemplo, los métodos de detección) del análisis en estado inactivo.

4.1.1.4 Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o durante actualizaciones del motor de detección. Este análisis depende de las tareas y la configuración del Planificador de tareas.

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos en el inicio del sistema** del Planificador de tareas. Para modificar su configuración, desplácese hasta **Herramientas** > **Planificador de tareas**, haga clic en **Verificación de la ejecución de archivos en el inicio** y, a continuación, haga clic en **Modificar**. En el último paso, aparece la ventana Verificación de la ejecución de archivos en el inicio (consulte el siguiente capítulo para obtener más detalles).

Para obtener instrucciones detalladas acerca de la creación y gestión de tareas del Planificador de tareas, consulte Creación de tareas nuevas.

4.1.1.4.1 Verificación de la ejecución de archivos en el inicio

Al crear una tarea programada de comprobación de archivos en el inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Archivos comúnmente utilizados** especifica la profundidad de análisis de los archivos ejecutados al iniciar el sistema basado en un sofisticado algoritmo secreto. Los archivos se organizan en orden descendente de acuerdo con los siguientes criterios:

- **Todos los archivos registrados** (se analiza el mayor número de archivos)
- **Archivos usados pocas veces**
- **Archivos usados ocasionalmente**
- **Archivos usados frecuentemente**
- **Solo los archivos usados con más frecuencia** (se analiza el menor número de archivos)

También se incluyen dos grupos específicos:

- **Los archivos se ejecutan antes de que se conecte el usuario**: contiene archivos de ubicaciones a las que se puede tener acceso sin que el usuario haya iniciado sesión (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, notificación del registro de Windows, entradas del Planificador de tareas de Windows, archivos dll conocidos, etc.).
- **Archivos en ejecución después del registro del usuario**: contiene archivos de ubicaciones a las que solo se puede tener acceso cuando el usuario se ha registrado (incluye archivos que solo ejecuta un usuario específico, generalmente los archivos de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se analizan son fijas para cada grupo de los anteriores.

Prioridad del análisis: el nivel de prioridad empleado para determinar cuándo se iniciará un análisis:

- **Cuando el procesador esté desocupado**: la tarea se ejecutará solo cuando el sistema esté inactivo.
- **Muy bajo**: cuando la carga del sistema es la más baja posible.
- **Bajo**: con poca carga del sistema.
- **Normal**: con carga media del sistema.

4.1.1.5 Exclusiones

Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. No obstante, puede que haya situaciones en las que necesite excluir un objeto, como por ejemplo entradas de una base de datos grande que ralenticen el ordenador durante el análisis o software que entre en conflicto con el análisis.

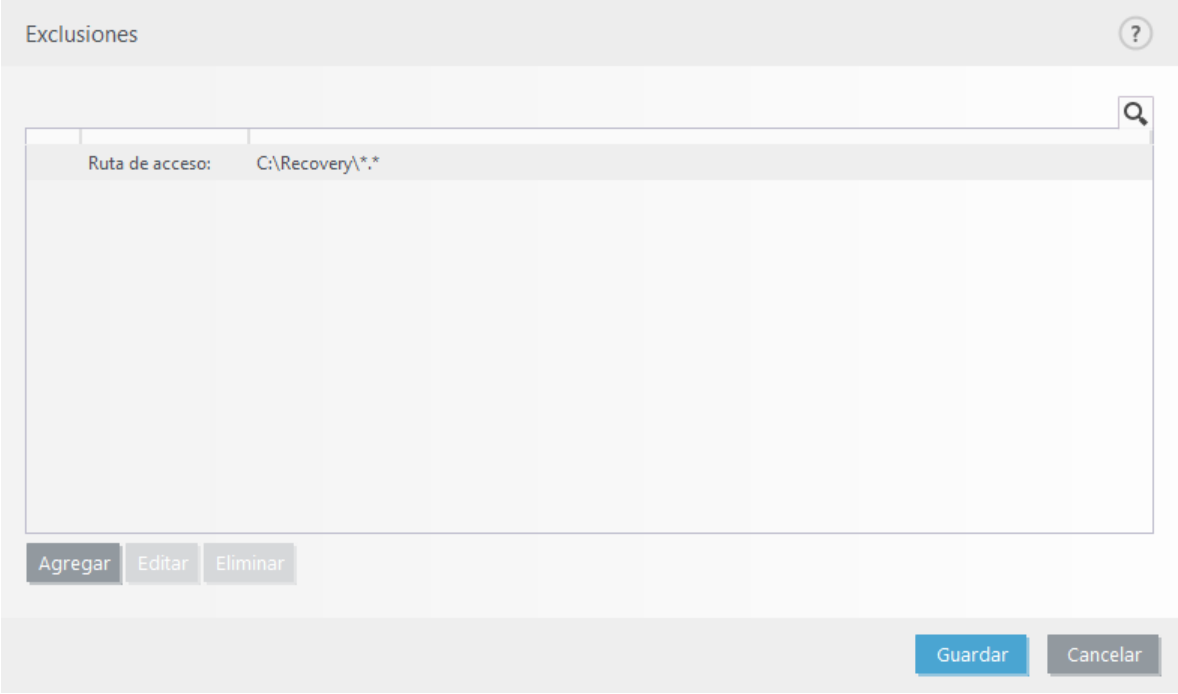
Para excluir un objeto del análisis:

1. Haga clic en **Agregar**.
2. Escriba la ruta de un objeto o selecciónelo en la estructura de árbol.

Puede utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (?) representa un carácter único variable, y el asterisco (*) una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos de una carpeta, escriba la ruta de acceso a la carpeta y utilice la máscara "*.*".
- Para excluir una unidad entera incluidos archivos y subcarpetas, utilice la máscara "D:*".
- Si desea excluir únicamente los archivos .doc, utilice la máscara "*.doc".
- Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato: "D????.exe". Los símbolos de interrogación sustituyen a los caracteres que faltan (desconocidos).



NOTA
El módulo de protección del sistema de archivos en tiempo real o de análisis del ordenador no detectará las amenazas que haya contenidas en un archivo si este cumple los criterios de exclusión del análisis.

Columnas

Ruta: ruta de los archivos y carpetas excluidos.

Amenaza: si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha amenaza. Si este archivo se infecta más adelante con otro código malicioso, el módulo antivirus lo detectará. Este tipo de exclusión únicamente se puede utilizar para determinados tipos de amenazas, y se puede crear bien en la ventana de alerta de amenaza que informa de la amenaza (haga clic en **Mostrar opciones avanzadas** y, a continuación, seleccione **Excluir de la detección**) o haciendo clic en **Herramientas** > **Más herramientas** > **Cuarentena** y, a continuación, haciendo clic en el archivo en cuarentena y seleccionando **Restaurar y excluir de la detección** en el menú contextual.

Elementos de control

Agregar: excluye los objetos de la detección.

Modificar: le permite modificar las entradas seleccionadas.

Quitar: elimina las entradas seleccionadas.

4.1.1.6 Parámetros de ThreatSense

ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina eficazmente los programas peligrosos (rootkits).

Las opciones de configuración del motor ThreatSense permiten al usuario especificar distintos parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar.
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **Parámetros de ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte más abajo). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis en estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección de clientes de correo electrónico
- Protección del acceso a la Web
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, con estos métodos solo se analizan los archivos recién creados). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

Memoria operativa: busca amenazas que ataquen a la memoria operativa del sistema.

Sectores de inicio: analiza los sectores de inicio para detectar virus en el registro de inicio principal.

Archivos de correo electrónico: el programa admite las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos comprimidos: el programa admite las siguientes extensiones: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.

Archivos comprimidos autoextraíbles: los archivos comprimidos de autoextracción (SFX) son archivos comprimidos que pueden extraerse por sí solos.

Empaquetadores de tiempo de ejecución: después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis permite reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

Heurística: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que la base de firmas de virus anterior no cubría. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.

Heurística avanzada/Firmas de ADN: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

Aplicaciones potencialmente indeseables: el grayware (o aplicaciones potencialmente indeseables [PUA]) es una amplia categoría de software no inequívocamente malintencionado, al contrario de lo que sucede 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. Consulte el capítulo Aplicaciones potencialmente indeseables para obtener más detalles.

Aplicaciones potencialmente peligrosas: Aplicaciones potencialmente peligrosas es la clasificación utilizada para programas comerciales legítimos, como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran todas las teclas que pulsa un usuario). Esta opción está desactivada de manera predeterminada.

Las opciones de desinfección determinan el comportamiento del análisis durante la desinfección de archivos infectados. Hay 3 niveles de desinfección.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

Otro

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

Analizar secuencias de datos alternativas (ADS): las secuencias de datos alternativos utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Realizar análisis en segundo plano con baja prioridad: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos: si se selecciona esta opción, el archivo de registro mostrará todos los archivos analizados, incluso los que no están infectados. Por ejemplo, si se detecta una amenaza en un archivo comprimido, en el registro se incluirán también los archivos sin infectar del archivo comprimido.

Activar la optimización inteligente: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.

Preservar el último acceso con su fecha y hora: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Tamaño máximo del objeto: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: *ilimitado*.

Tiempo máximo de análisis para el objeto (seg.): define el tiempo máximo asignado para analizar un objeto. Si se especifica un valor definido por el usuario, el módulo antivirus detendrá el análisis de un objeto cuando se haya agotado el tiempo, independientemente de si el análisis ha finalizado o no. Valor predeterminado: *ilimitado*.

Configuración del análisis de archivos comprimidos

Nivel de anidamiento de archivos: especifica el nivel máximo de análisis de archivos. Valor predeterminado: *10*.

Tamaño máx. de archivo en el archivo comprimido: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. Valor predeterminado: *ilimitado*.

NOTA
No se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

4.1.1.6.1 Desinfección

Las opciones de desinfección determinan el comportamiento del análisis durante la desinfección de archivos infectados. Hay 3 niveles de desinfección.

4.1.1.6.2 Extensiones de archivo excluidas del análisis

Una extensión es la parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

De forma predeterminada, se analizan todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis.

A veces es necesario excluir archivos del análisis si, por ejemplo, el análisis de determinados tipos de archivo impide la correcta ejecución del programa que utiliza determinadas extensiones. Por ejemplo, podría ser recomendable excluir las extensiones de archivo `.edb`, `.eml` y `.tmp` al utilizar servidores de Microsoft Exchange.

Con los botones **Agregar** y **Quitar**, puede activar o prohibir el análisis de extensiones de archivo específicas. Para añadir una extensión nueva a la lista, haga clic en **Agregar**, escriba la extensión en el campo en blanco (por ejemplo, `tmp`) y haga clic en **Aceptar**. Seleccione **Introduzca múltiples valores** para añadir varias extensiones de archivos delimitadas por líneas, comas o punto y coma. Si está activada la selección múltiple, las extensiones se mostrarán en la lista. Seleccione una extensión en la lista y haga clic en **Quitar** para eliminarla de la lista. Si desea modificar una extensión seleccionada, haga clic en **Modificar**.

Se pueden usar los símbolos especiales ? (signo de interrogación). El signo de interrogación representa cualquier símbolo.

NOTA

Para ver la extensión concreta (en caso de tener alguna) de un archivo en un sistema operativo Windows, tiene que desmarcar la opción **Ocultar extensiones de tipos de archivo conocidos** en **Panel de control** > **Opciones de carpeta** > **Ver** (ficha) y aplicar este cambio.

4.1.1.7 Detección de una amenaza

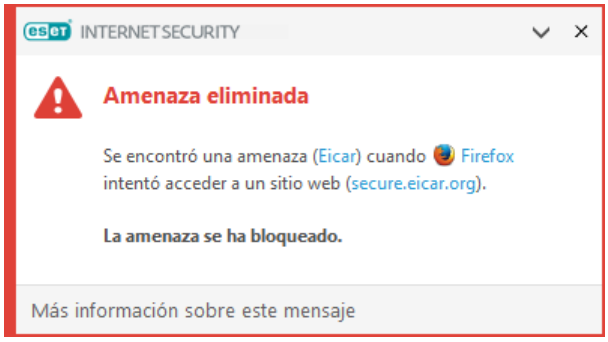
Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Comportamiento estándar

Como ejemplo general de cómo ESET Internet Security gestiona las amenazas, estas se pueden detectar mediante:

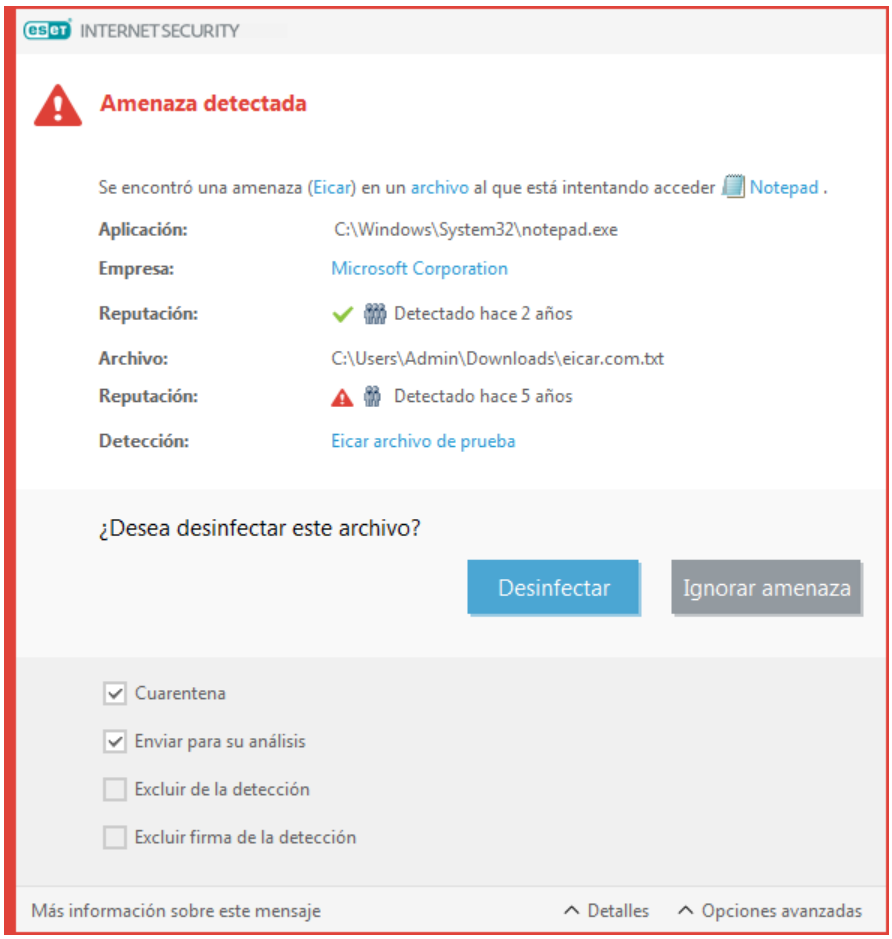
- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección de clientes de correo electrónico
- Análisis de estado inactivo

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



Desinfección y eliminación

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



Aplique esta opción si un archivo ha sido infectado por un virus que le ha añadido código malicioso. Si este es el caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.

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

Múltiples amenazas

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

Eliminar amenazas en archivos comprimidos

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

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

- Abra ESET Internet Security y haga clic en Análisis del ordenador.
- Haga clic en **Análisis del ordenador** (para obtener más información, consulte Análisis del ordenador).
- Una vez que haya finalizado el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

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

4.1.1.8 Protección de documentos

La característica de protección de documentos analiza los documentos de Microsoft Office antes de que se abran y los archivos descargados automáticamente con Internet Explorer como, por ejemplo, elementos de Microsoft ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección en tiempo real del sistema de archivos, y se puede desactivar para mejorar el rendimiento en sistemas que no gestionan a un volumen elevado de documentos de Microsoft Office.

Para activar la protección de documentos, abra la ventana **Configuración avanzada** (pulsando F5) > **Motor de detección** > **Análisis de malware** > **Protección de documentos** y haga clic en el conmutador **Integrar en el sistema**.

NOTA
Esta función se activa mediante aplicaciones que utilizan la Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y superior, o Microsoft Internet Explorer 5.0 y superior).

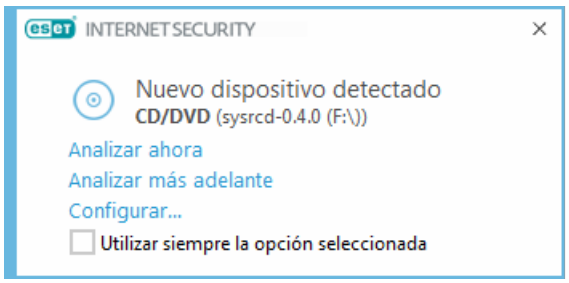
4.1.2 Medios extraíbles

ESET Internet Security permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática. Este módulo le permite analizar un medio insertado. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Acción que debe efectuarse cuando se insertan medios extraíbles: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el ordenador (CD, DVD o USB). Si selecciona **Mostrar las opciones de análisis**, se mostrará una ventana en la que puede seleccionar la acción deseada:

- **No analizar**: no se realizará ninguna acción y se cerrará la ventana **Nuevo dispositivo detectado**.
- **Análisis automático del dispositivo**: se realizará un análisis del ordenador a petición del medio extraíble insertado.
- **Mostrar las opciones de análisis**: abre la sección de configuración de medios extraíbles.

Cuando se inserta un medio extraíble aparece la siguiente ventana:



Analizar ahora: activa el análisis del medio extraíble.

Analizar más adelante: el análisis del medio extraíble se pospone.

Configuración: abre la configuración avanzada.

Utilizar siempre la opción seleccionada: cuando se seleccione esta opción, se realizará la misma acción la próxima vez que se introduzca un medio extraíble.

Además, ESET Internet Security presenta funciones de control de dispositivos, lo que le permite definir reglas para el uso de dispositivos externos en un ordenador dado. Encontrará más detalles sobre el control de dispositivos en la sección Control de dispositivos.

4.1.3 Control de dispositivos

Control de dispositivos

ESET Internet Security permite controlar los dispositivos automáticamente (CD, DVD, USB, etc.). Este módulo le permite bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (unidad de disco duro, disco USB extraíble)
- CD/DVD
- Impresora USB
- Almacenamiento FireWire
- Dispositivo Bluetooth
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- Puerto LPT/COM
- Dispositivo portátil
- Micrófono
- Todos los tipos de dispositivos

Las opciones de configuración del control del dispositivo se pueden modificar en **Configuración avanzada** (F5) > **Control del dispositivo**.

Al activar el conmutador situado junto a **Integrar en el sistema** se activa la característica de Control del dispositivo en ESET Internet Security; deberá reiniciar el ordenador para que se aplique este cambio. Una vez que Control del dispositivo esté activado, se activarán las **Reglas**, lo que le permitirá abrir la ventana Editor de reglas.

NOTA
Puede crear varios grupos de dispositivos a los que se aplicarán reglas distintas. También puede crear solo un grupo de dispositivos al que se aplicará la regla con la acción **Lectura/Escritura** o **Solo lectura**. Esto garantiza el bloqueo de dispositivos no reconocidos por el control de dispositivos pero conectados al ordenador.

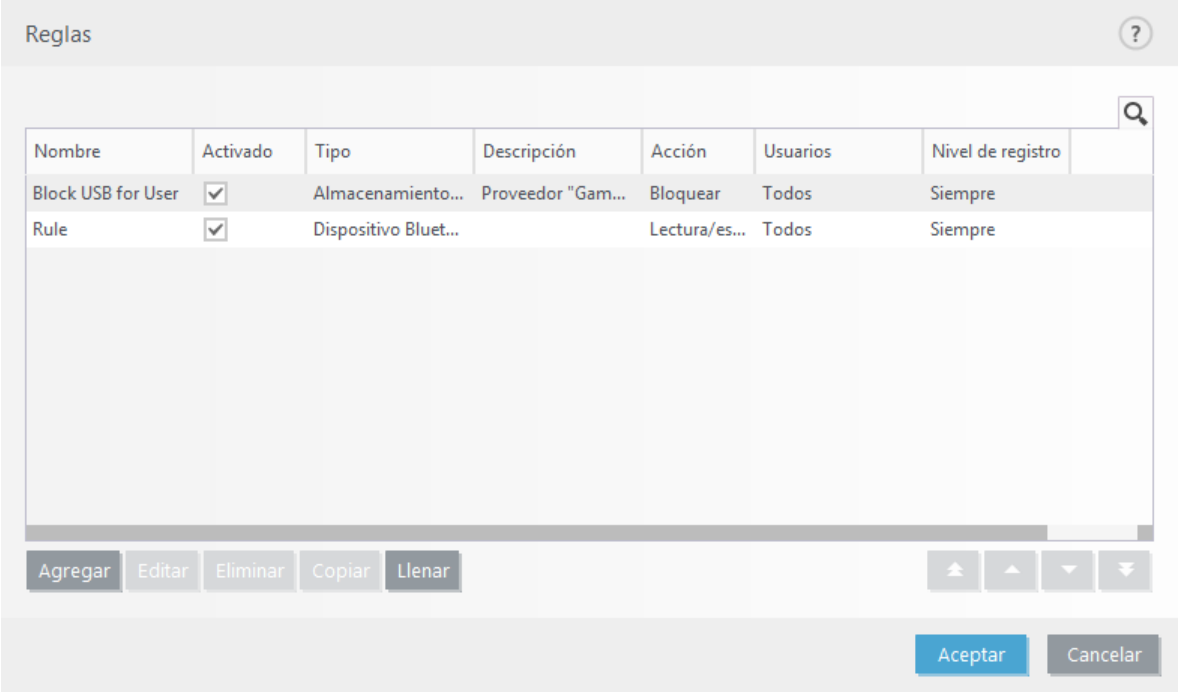
Si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación y se prohíbe el acceso a dicho dispositivo.

Protección de cámara web

Activar el conmutador situado junto a **Integrar en el sistema** activa la función Protección de cámara web en ESET Internet Security. Una vez que la Protección de la cámara web esté activada, se activarán las **Reglas**, lo que le permitirá abrir la ventana Editor de reglas.

4.1.3.1 Editor de reglas de control del dispositivo

La ventana **Editor de reglas de control de dispositivos** muestra las reglas existentes para dispositivos externos que los usuarios conectan al ordenador y permite controlarlos de forma precisa.



Determinados dispositivos se pueden permitir o bloquear por usuario o por grupo de usuarios y según parámetros adicionales del dispositivo que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Haga clic en **Copiar** para crear una nueva regla con opciones predefinidas utilizadas para otra regla seleccionada. Las cadenas XML que se muestran al hacer clic en una regla se pueden copiar en el portapapeles para ayudar a administradores de sistemas a exportar o importar datos y utilizarlos; por ejemplo, en ESET Remote Administrator.

Al mantener pulsado CTRL y hacer clic, puede seleccionar varias reglas y aplicar acciones, como eliminarlas o moverlas hacia arriba o hacia abajo en la lista, a todas las reglas seleccionadas. La casilla de verificación **Activado** desactiva o activa una regla; puede ser útil si no desea eliminar una regla de forma permanente, por si decide utilizarla en el futuro.

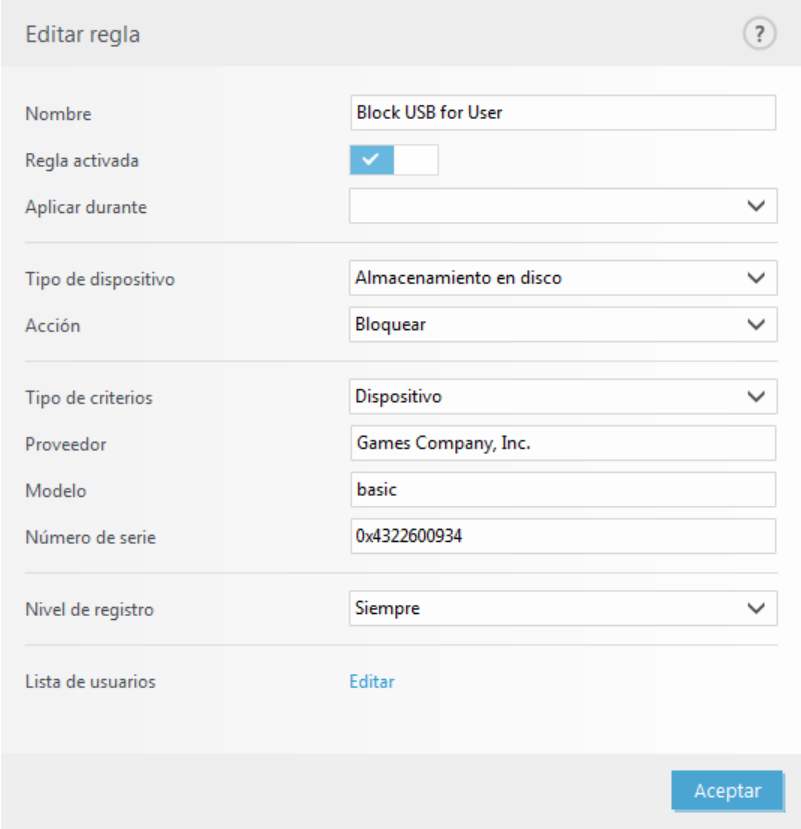
El control se efectúa mediante reglas que se clasifican en el orden que determina su prioridad, situándose al principio las reglas con la prioridad más alta.

Las entradas de registro se pueden ver desde la ventana principal de ESET Internet Security en **Herramientas** > **Más herramientas** > Archivos de registro.

El Registro de control de dispositivos anota todas las ocasiones en las que se activa el Control de dispositivos.

4.1.3.2 Adición de reglas de control de dispositivos

Una regla de control de dispositivos define la acción que se realizará al conectar al ordenador un dispositivo que cumple los criterios de la regla.



Introduzca una descripción de la regla en el campo **Nombre** para mejorar la identificación. Haga clic en el conmutador situado junto a **Regla activada** para activar o desactivar esta regla, lo cual puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (Almacenamiento en disco, Dispositivo portátil, Bluetooth, FireWire…). La información sobre el tipo de dispositivo se recopila del sistema operativo y se puede ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Los lectores de tarjetas inteligentes abarcan todos los lectores que tienen incrustado un circuito integrado, como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras. Como estos dispositivos solo proporcionan información sobre sus acciones y no sobre los usuarios, solo pueden bloquearse a nivel global.

Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/Escritura**: se permitirá el acceso completo al dispositivo.
- **Bloquear**: se bloqueará el acceso al dispositivo.
- **Solo lectura**: solo se permitirá el acceso de lectura al dispositivo.
- **Advertir**: cada vez que se conecte un dispositivo se informará al usuario de si está permitido o bloqueado, y se creará una entrada de registro. Los dispositivos no se recuerdan, se seguirá mostrando una notificación en las siguientes conexiones del mismo dispositivo.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. Si se trata de un dispositivo de tipo almacenamiento, las cuatro acciones estarán disponibles. En el caso de los dispositivos que no son de almacenamiento solo hay tres disponibles (por ejemplo, **Solo lectura** no está disponible

para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

Tipo de criterios – Seleccione **Grupo de dispositivos** o **Dispositivo**.

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas y adaptarlas a dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas:

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

NOTA
Si estos parámetros están sin definir, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).

NOTA
Si desea ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo, conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo en el Registro de control de dispositivos.

Nivel de registro

ESET Internet Security guarda todos los sucesos importantes en un archivo de registro que se puede ver directamente en el menú principal. Haga clic en **Herramientas** > **Archivos de registro** y, a continuación, seleccione **Control de dispositivos** en el menú desplegable **Registro**.

- **Siempre**: registra todos los sucesos.
- **Diagnóstico**: registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta.
- **Ninguno**: no se registra nada.

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios agregándolos a la **Lista de usuarios**:

- **Agregar**: abre el cuadro de diálogo **Tipos de objeto: Usuarios o grupos**, que le permite seleccionar los usuarios que desee.
- **Quitar**: elimina del filtro al usuario seleccionado.

NOTA
Los dispositivos se pueden filtrar mediante reglas de usuario (por ejemplo, los dispositivos de imagen no proporcionan información sobre los usuarios, sino únicamente sobre las acciones).

4.1.3.3 Editor de reglas de protección de cámara web

En esta ventana se muestran las reglas existentes y se pueden controlar las aplicaciones y los procesos que acceden a la cámara web del ordenador en función de la acción que haya tomado.

Están disponibles las siguientes acciones:

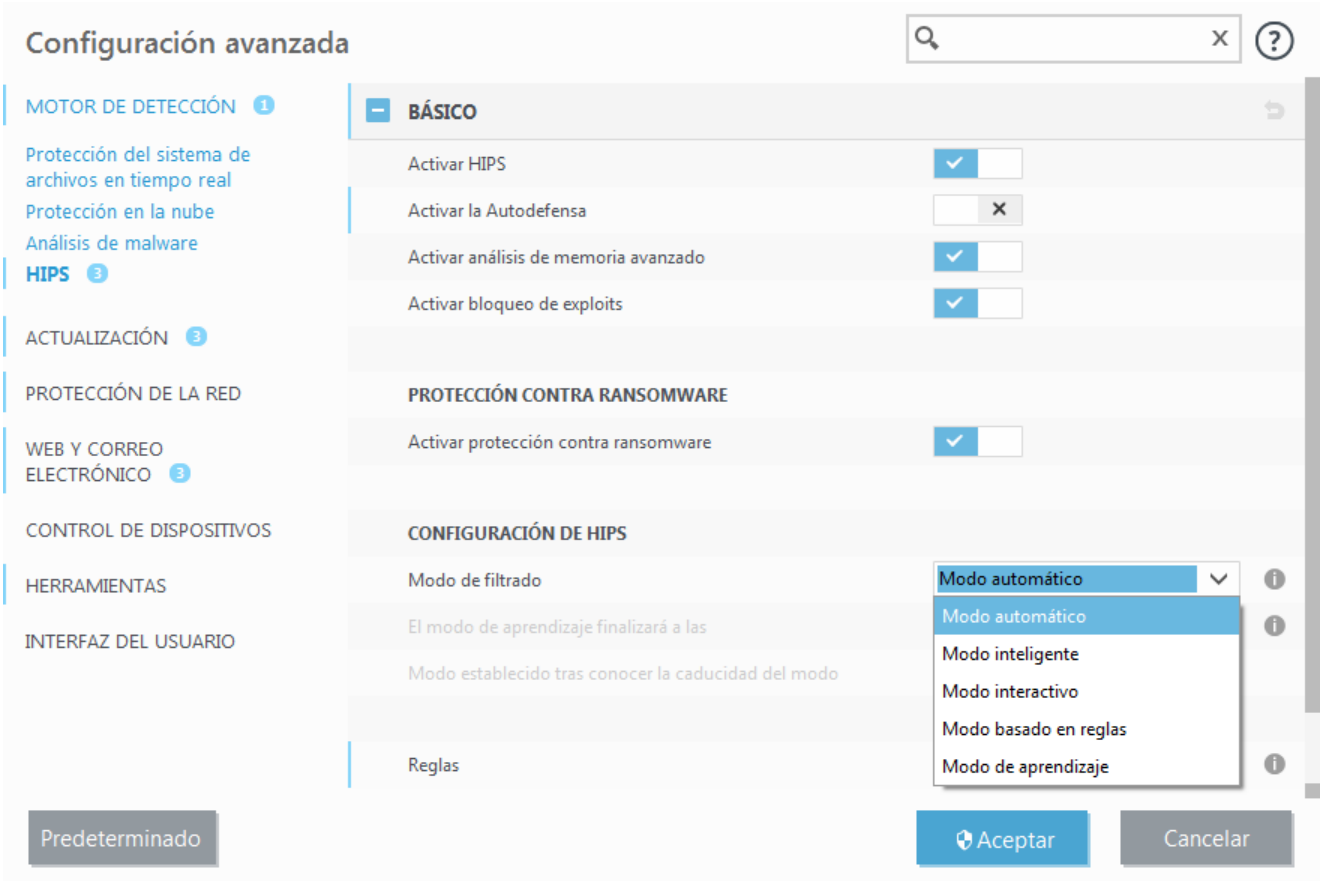
- **Bloquear acceso**
- **Preguntar**
- **Permitir acceso**

4.1.4 Sistema de prevención de intrusiones del host (HIPS)

ADVERTENCIA
Solo debe modificar la configuración de HIPS si es un usuario experimentado. Una configuración incorrecta de los parámetros de HIPS puede provocar inestabilidad en el sistema.

El **Sistema de prevención de intrusiones del host** (HIPS) protege el sistema frente a código malicioso o cualquier actividad no deseada que intente menoscabar la seguridad del ordenador. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos; solo supervisa los procesos que se ejecutan dentro del sistema operativo.

Los ajustes del HIPS se pueden encontrar en **Configuración avanzada** (F5) > **Motor de detección** > **HIPS** > **Básico**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal de ESET Internet Security, dentro de **Configuración** > **Protección del ordenador**.



ESET Internet Security utiliza la tecnología de **Autodefensa** integrada como parte del HIPS para impedir que el software malicioso dañe o desactive la protección antivirus y antiespía. La autodefensa evita la manipulación de procesos, claves de registro y archivos cruciales del sistema y de ESET.

Activar servicio protegido: activa la protección del kernel (Windows 8.1, 10).

Análisis avanzado de memoria: trabaja conjuntamente con el Bloqueador de exploits para aumentar la protección frente a código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

El **Bloqueador de exploits** se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de Internet, los lectores de archivos pdf, los clientes de correo electrónico y los componentes de MS Office. El bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

Protección contra ransomware es otra capa de protección que funciona como parte de la función HIPS. Para que la protección contra ransomware funcione, debe tener activado el sistema de reputación LiveGrid®. Puede obtener

más información sobre este tipo de protección aquí.

El filtrado se puede realizar en cualquiera de los cuatro modos:

Modo automático: las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema.

Modo inteligente: solo se informará al usuario de los sucesos muy sospechosos.

Modo interactivo: el usuario debe confirmar las operaciones.

Modo basado en reglas: las operaciones están bloqueadas.

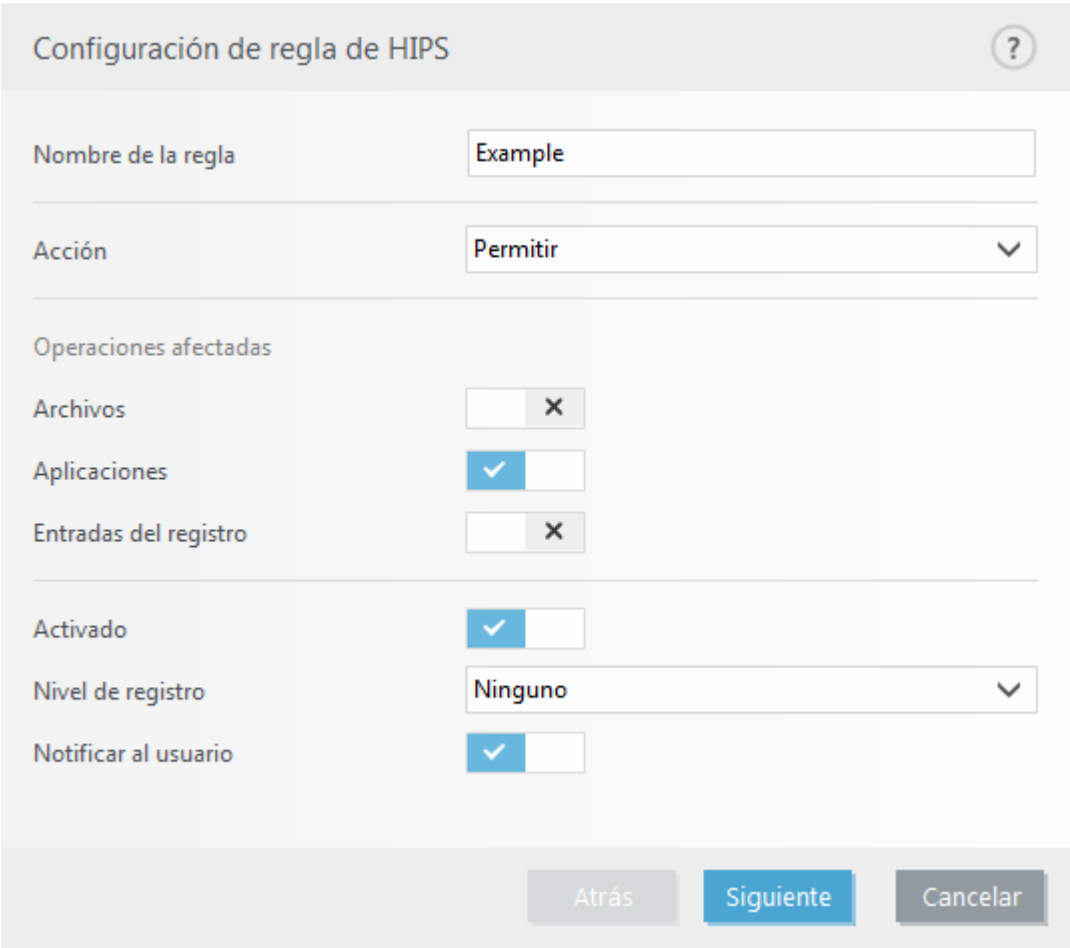
Modo de aprendizaje: las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de reglas, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el Modo de aprendizaje en el menú desplegable del modo de filtrado de HIPS, el ajuste **El modo de aprendizaje finalizará a las** estará disponible. Seleccione el periodo de tiempo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada se le pedirá que modifique las reglas creadas por el HIPS mientras estaba en modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje.

Modo establecido tras conocer la caducidad del modo: seleccione el modo de filtrado que se utilizará cuando caduque el modo de aprendizaje.

El sistema HIPS supervisa los sucesos del sistema operativo y reacciona de acuerdo con reglas similares a las que utiliza el cortafuegos. Haga clic en **Modificar** junto a Reglas para abrir la ventana de gestión de reglas de HIPS. En la ventana de reglas de HIPS puede seleccionar, agregar, modificar o eliminar reglas.

En el ejemplo siguiente, veremos cómo restringir el comportamiento no deseado de las aplicaciones:

1. Asigne un nombre a la regla y seleccione **Bloquear** en el menú desplegable **Acción**.
2. Active el conmutador **Advertir al usuario** para mostrar una notificación siempre que se aplique una regla.
3. Seleccione al menos una operación a la que se aplicará la regla. En la ventana **Aplicaciones de origen**, seleccione **Todas las aplicaciones** en el menú desplegable para aplicar la nueva regla a todas aquellas aplicaciones que intenten realizar cualquiera de las operaciones de aplicación seleccionadas en las aplicaciones especificadas.
4. Seleccione **Modificar el estado de otra aplicación** (todas las operaciones se describen en la ayuda del producto, a la que puede acceder pulsando la tecla F1).
5. Seleccione **Aplicaciones específicas** en el menú desplegable y pulse **Agregar** para añadir las aplicaciones que desee proteger.
6. Haga clic en **Finalizar** para guardar la nueva regla.



4.1.4.1 Configuración avanzada

Las opciones siguientes son útiles para depurar y analizar el comportamiento de una aplicación:

Controladores con carga siempre autorizada: los controladores seleccionados pueden cargarse siempre sea cual sea el modo de filtrado configurado, a menos que la regla del usuario los bloquee de forma explícita.

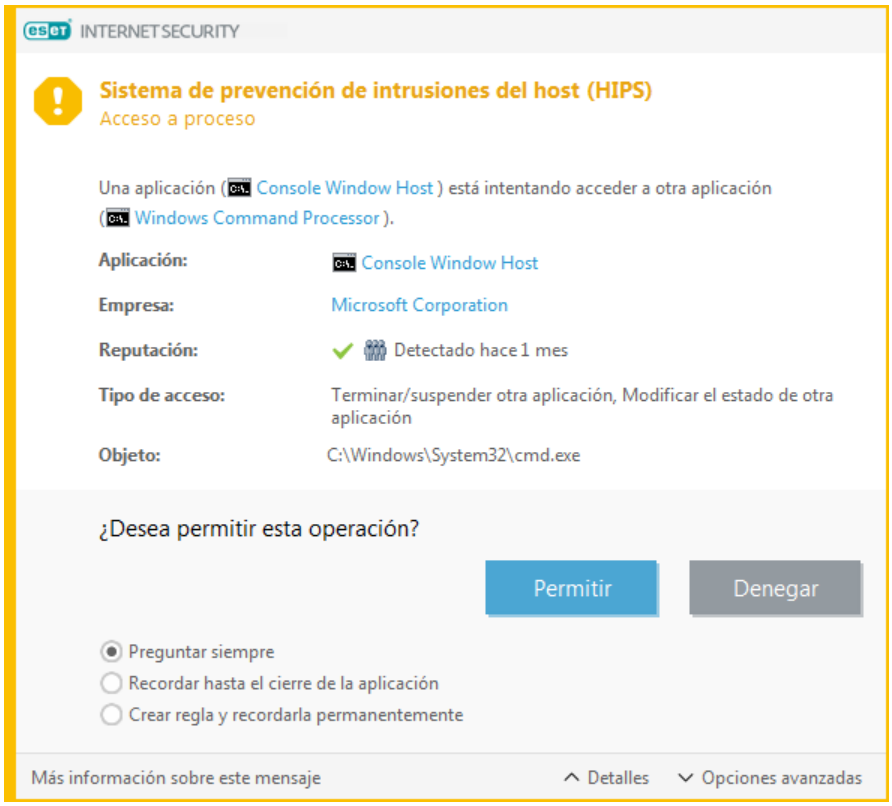
Registrar todas las operaciones bloqueadas: todas las operaciones bloqueadas se anotarán en el registro de HIPS.

Notificar cuando se produzcan cambios en las aplicaciones de inicio: muestra una notificación en el escritorio cada vez que se agrega o se elimina una aplicación del inicio del sistema.

Consulte nuestro artículo de la base de conocimiento para ver una versión actualizada de esta página de ayuda.

4.1.4.2 Ventana interactiva de HIPS

Si la acción predeterminada para una regla es **Preguntar**, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla. Puede seleccionar entre **Bloquear** y **Permitir** la operación. Si no selecciona una opción en el tiempo indicado, se aplican las reglas para seleccionar la nueva acción.

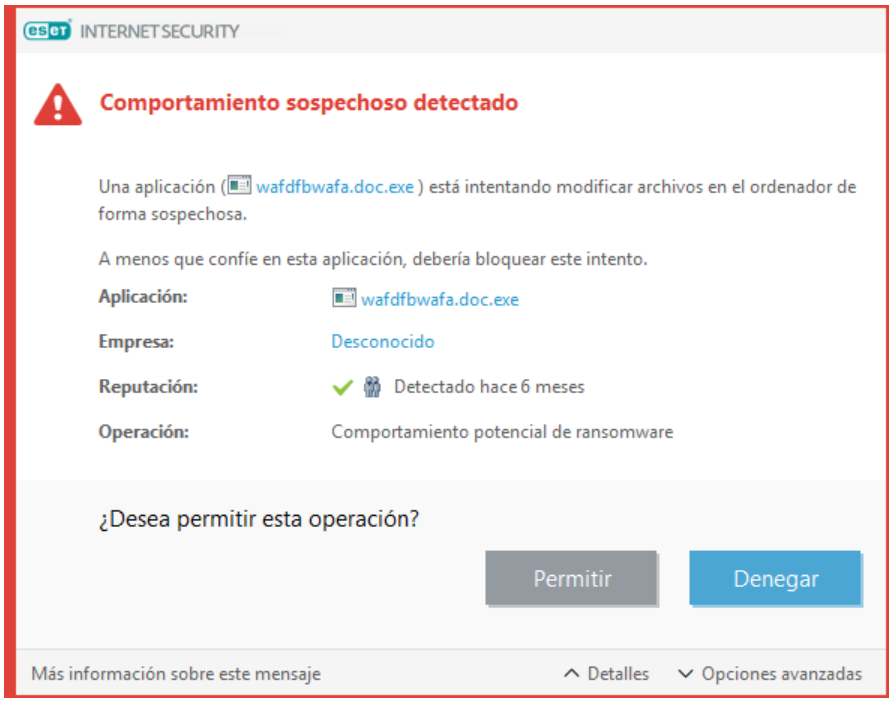


El cuadro de diálogo permite crear reglas de acuerdo con cualquier nueva acción que detecte HIPS y definir las condiciones en las que se permite o se rechaza dicha acción. Los parámetros exactos se pueden consultar haciendo clic en **Detalles**. Las reglas creadas con este método se tratan igual que las creadas manualmente, por lo que una regla creada desde un cuadro de diálogo puede ser menos específica que la regla que activó dicho cuadro de diálogo. Esto significa que, después de crear esta regla, la misma operación puede activar la misma ventana.

Recordar hasta el cierre de la aplicación provoca que se use la acción (**Permitir/Bloquear**) hasta que se cambien las reglas o el modo de filtrado, se actualice el módulo HIPS o se reinicie el sistema. Después de cualquiera de estas tres acciones, las reglas temporales se eliminarán.

4.1.4.3 Se ha detectado un comportamiento potencial de ransomware

Esta ventana interactiva aparecerá cuando se detecte un comportamiento potencial de ransomware. Puede seleccionar entre **Bloquear** y **Permitir** la operación.



El cuadro de diálogo le permite **enviar el archivo para su análisis** o **excluirlo de la detección**. Haga clic en **Detalles** para ver parámetros de detección concretos.

IMPORTANTE
Para que la protección contra ransomware funcione correctamente, ESET Live Grid debe estar activado.

4.1.5 Modo de juego

El modo jugador es una característica para usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. También se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Al activar esta característica se desactivan todas las ventanas emergentes y la actividad del planificador de tareas se detiene por completo. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Si desea activar o desactivar el modo jugador, lo puede hacer en la ventana principal del programa al hacer clic en **Configuración** > **Protección del ordenador** haciendo clic en o en junto a **Modo jugador**. Activar el modo de juego constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección disponible en la barra de tareas se volverá naranja y mostrará un signo de alerta. Esta alerta también se puede ver en la ventana principal del programa donde verá el mensaje **Modo de juego activo** en naranja.

Active la opción **Activar el modo de juego automáticamente al ejecutar aplicaciones en pantalla completa** en **Configuración avanzada** (F5) > **Herramientas** > **Modo de juego** para que el Modo de juego se active cuando inicie una aplicación a pantalla completa y se detenga cuando cierre dicha aplicación.

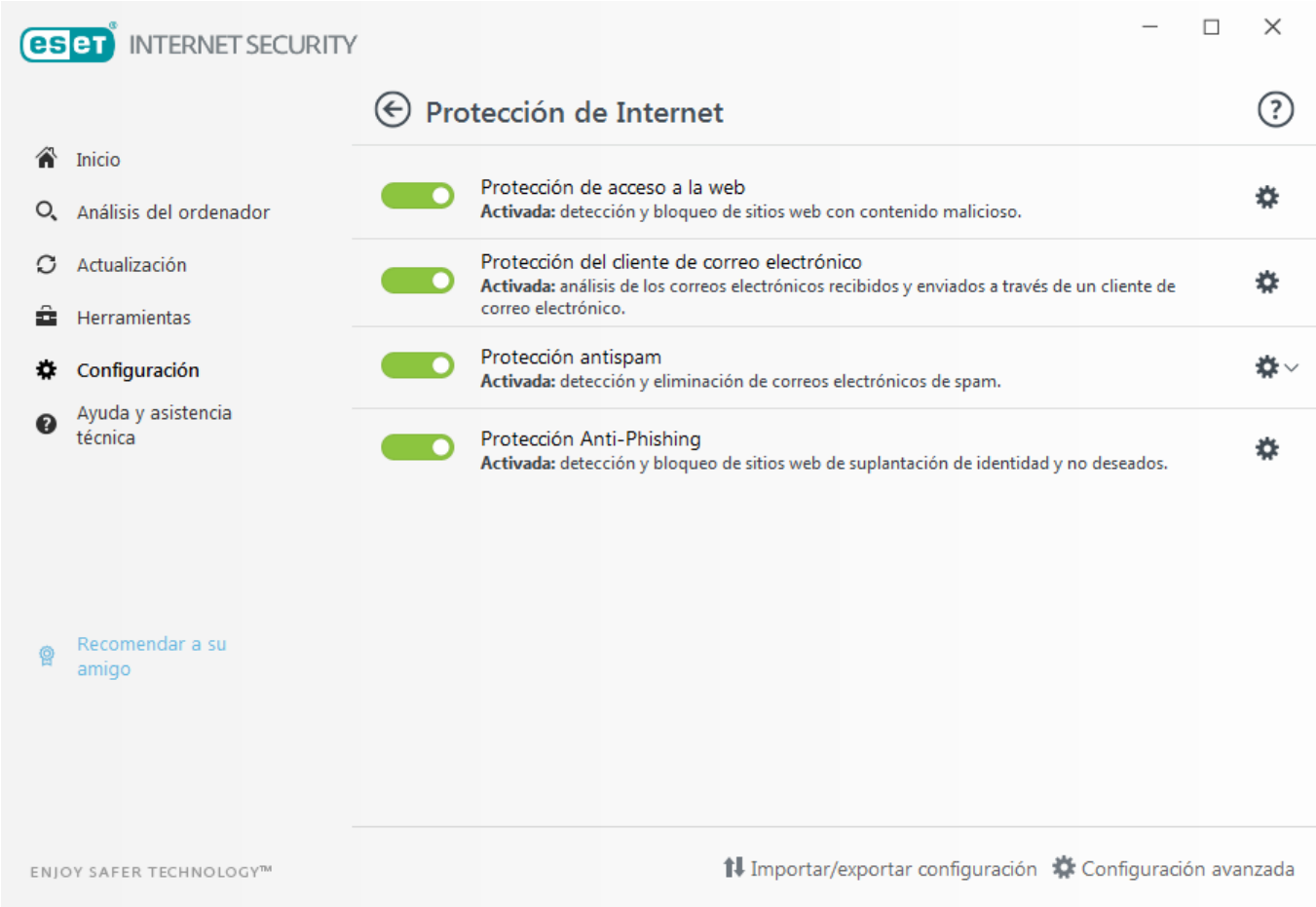
Active la opción **Desactivar el modo de juego automáticamente después de** para definir la cantidad de tiempo tras el cual el Modo de juego se desactivará automáticamente.

NOTA
Si el cortafuegos está en modo interactivo y el modo de juego está activado, podría tener problemas para conectarse a Internet. Esto puede ser un problema si el juego necesita conexión a Internet. Por lo general, se le solicita que confirme dicha acción (si no se ha definido ninguna regla o excepción de comunicación), pero en el modo de juego la intervención del usuario está desactivada. Para permitir la comunicación, defina una regla de comunicación para cualquier aplicación que pueda encontrar este problema, o utilice un Modo de filtrado en el

cortafuegos. Recuerde que si el modo jugador está activado y accede a una página web o aplicación que presente un riesgo de seguridad potencial, esta podría bloquearse sin ninguna explicación o alerta, ya que la intervención del usuario está desactivada.

4.2 Protección de Internet

Puede consultar la configuración web y del correo electrónico en el panel **Configuración** haciendo clic en **Protección de Internet**. Desde aquí puede acceder a configuraciones más detalladas del programa.



La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. Por eso, es fundamental prestar la debida atención a la **protección del tráfico de Internet**.

Haga clic en ⚙ para abrir opciones de protección de web/correo electrónico/antiphishing/antispam en la configuración avanzada.

La protección del cliente de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el programa de complemento para su cliente de correo electrónico, ESET Internet Security ofrece control de todas las comunicaciones realizadas a y desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP).

La **Protección antispam** filtra los mensajes de correo electrónico no solicitados.

Al hacer clic en la rueda dentada ⚙ disponible junto a **Protección Antispam**, se muestran las siguientes opciones:

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

Lista blanca/Lista negra/Lista de excepciones del usuario: abre un cuadro de diálogo en el que puede agregar, modificar o eliminar direcciones de correo electrónico que se consideran seguras o peligrosas. El correo

electrónico procedente de estas direcciones se tratará como correo no deseado o no se analizará de acuerdo con las reglas aquí definidas. Haga clic en **Lista de excepciones del usuario** para agregar, modificar o eliminar direcciones de correo electrónico que se puedan falsificar y utilizar para el envío de correo no deseado. Los mensajes de correo electrónico cuyo remitente se encuentre en la lista de excepciones no se analizarán en busca de correo no deseado.

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

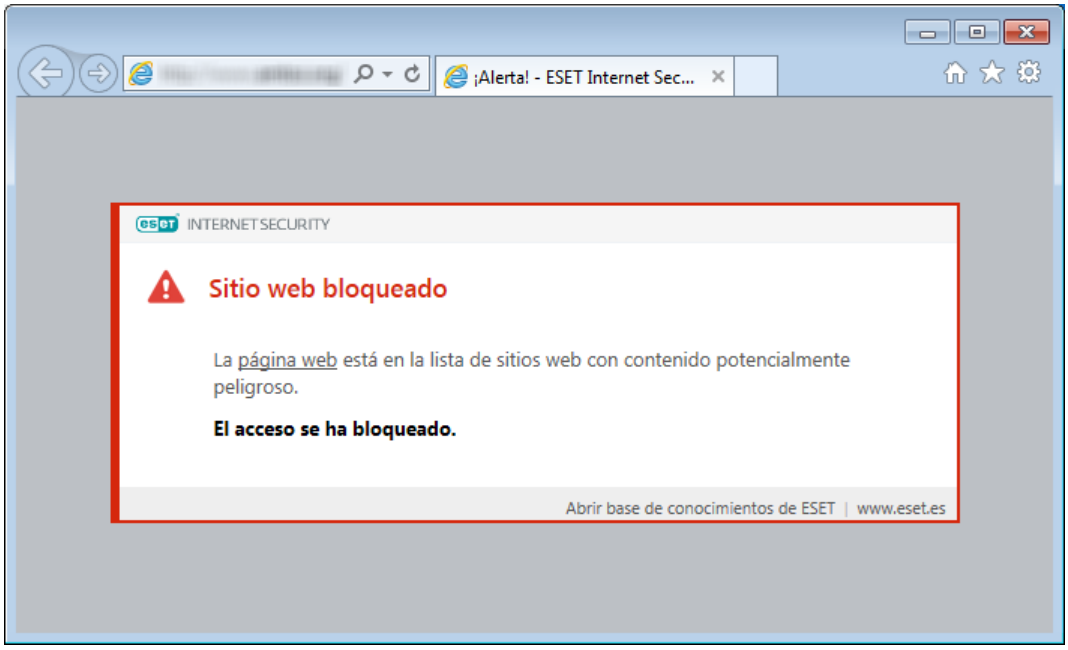
Puede desactivar temporalmente el módulo de protección de web/correo electrónico/anti-phishing/antispam haciendo clic en  .

4.2.1 Protección del acceso a Internet

La conectividad de Internet es una característica estándar de cualquier ordenador personal. Lamentablemente, también se ha convertido en el principal medio de transferencia de código malicioso. La protección del tráfico de Internet funciona supervisando la comunicación entre navegadores web y servidores remotos, y cumple con las reglas HTTP (Protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se sabe que contienen código malicioso se bloquea antes de descargar contenido. El motor de análisis ThreatSense analiza todas las demás páginas web cuando se cargan y bloquean en caso de detección de contenido malicioso. La protección del tráfico de Internet ofrece dos niveles de protección: bloqueo por lista negra y bloqueo por contenido.

Le recomendamos encarecidamente que active la opción de protección del tráfico de Internet. Se puede acceder a esta opción desde la ventana principal de ESET Internet Security accediendo a **Configuración** > **Protección de Internet** > **Protección del tráfico de Internet**.



Las opciones siguientes están disponibles en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet**:

- **Protocolos web**: le permite configurar la supervisión de estos protocolos estándar que utilizan la mayoría de los navegadores de Internet.
- **Gestión de direcciones URL**: aquí puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis.
- **Parámetros de ThreatSense**: la configuración avanzada del análisis de virus le permite configurar opciones como los tipos de objetos que desea analizar (mensajes de correo electrónico, archivos comprimidos, etc.), los métodos de detección para la protección del tráfico de Internet, etc.

4.2.1.1 Básico

Activar la protección del tráfico de Internet: cuando esta opción está desactivada no se ejecuta la protección del tráfico de Internet ni la protección Antiphishing.

Activar análisis avanzado de los scripts del navegador: cuando esta opción está activada el análisis antivirus comprueba todos los programas JavaScript que ejecuten los navegadores de Internet.

NOTA
Le recomendamos encarecidamente que mantenga activada la opción Protección del acceso a la Web.

4.2.1.2 Protocolos web

De forma predeterminada, ESET Internet Security está configurado para supervisar el protocolo HTTP que utilizan la mayoría de los navegadores de Internet.

Configuración del análisis de HTTP

En Windows Vista y versiones posteriores, el tráfico HTTP se supervisa siempre en todos los puertos y para todas las aplicaciones. En Windows XP se puede modificar la opción **Puertos utilizados por el protocolo HTTP** en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet** > **Protocolos web**. El tráfico HTTP se supervisa en los puertos especificados para todas las aplicaciones, y en todos los puertos de las aplicaciones marcadas como Clientes de correo electrónico y web.

Configuración del análisis de HTTPS

ESET Internet Security admite también la comprobación del protocolo HTTPS. La comunicación HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Internet Security comprueba la comunicación mediante los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos utilizados por el protocolo HTTPS**, independientemente de la versión del sistema operativo.

La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, vaya a SSL/TLS en la sección Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y active la opción **Activar el filtrado del protocolo SSL/TLS**.

4.2.1.3 Gestión de direcciones URL

En esta sección puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis.

No podrá acceder a los sitios web de **Lista de direcciones bloqueadas**, a menos que también se incluyan en **Lista de direcciones permitidas**. Cuando acceda a sitios web que se encuentran en **Lista de direcciones excluidas de la verificación**, no se buscará código malicioso en ellos.

Debe seleccionar **Activar el filtrado del protocolo SSL/TLS** si desea filtrar las direcciones HTTPS, además de las páginas web HTTP. Si no lo hace, solo se agregarán los dominios de los sitios HTTPS que haya visitado, pero no la URL completa.

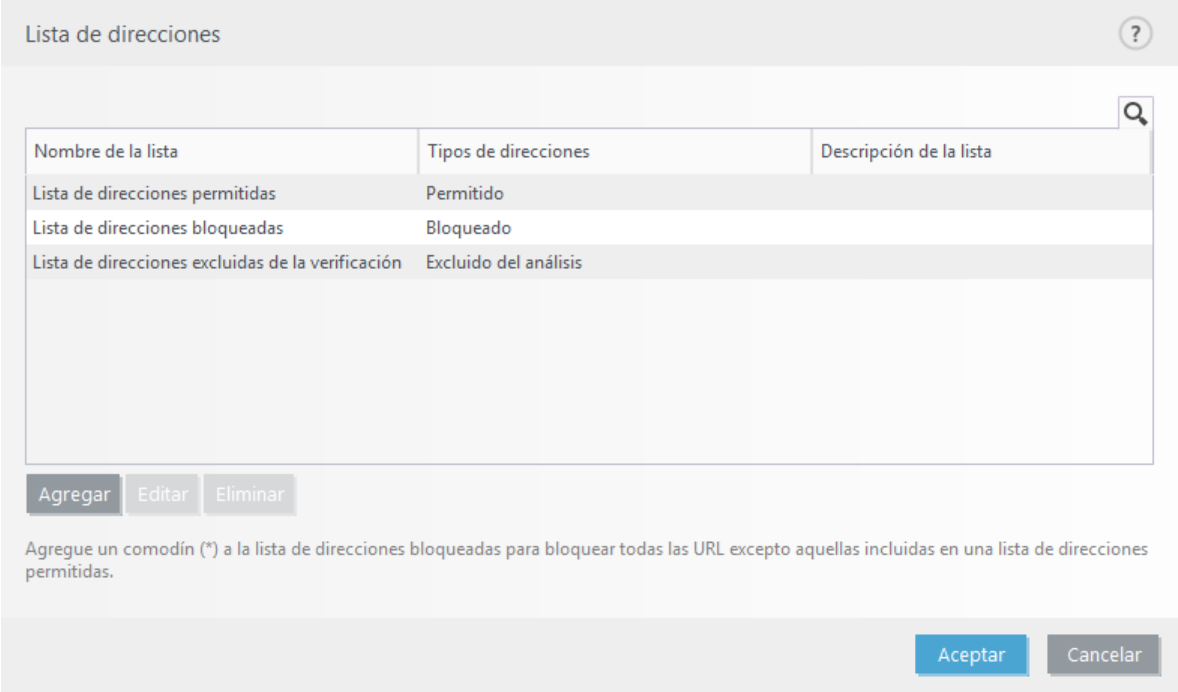
Si añade una dirección URL a la **Lista de direcciones excluidas del filtrado**, esta dirección se excluirá del análisis. También puede permitir o bloquear determinadas direcciones añadiéndolas a la **Lista de direcciones permitidas** o **Lista de direcciones bloqueadas**.

Si desea bloquear todas las direcciones HTTP menos las incluidas en la **Lista de direcciones permitidas** activa, agregue el símbolo * a la **Lista de direcciones bloqueadas** activa.

No se pueden utilizar los símbolos especiales * (asterisco) y ? (signo de interrogación) en listas. El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista. Consulte Agregar dirección HTTP/máscara de dominio para obtener información sobre cómo detectar un dominio completo

con todos sus subdominios de forma segura. Para activar una lista, seleccione **Lista activa**. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione **Notificar al aplicar**.

NOTA
La gestión de direcciones URL también permite bloquear o permitir la apertura de tipos de archivos específicos durante la navegación en Internet. Por ejemplo, si no desea que se abran archivos ejecutables, seleccione la lista en la que desee bloquear estos archivos del menú desplegable y, a continuación, introduzca la máscara "**.exe".



Elementos de control

Agregar: crea una lista nueva que se suma a las predefinidas. Esta opción puede ser útil si se desea dividir varios grupos de direcciones de forma lógica. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que otra contiene su propia lista negra. Esto facilita la actualización de la lista externa sin que la suya se vea afectada.

Modificar: modifica las listas existentes. Utilice esta opción para agregar o quitar direcciones.

Eliminar: elimina las listas existentes. Esta opción solo está disponible en listas creadas con **Agregar**, no en las listas predeterminadas.

4.2.2 Protección del cliente de correo electrónico

4.2.2.1 Clientes de correo electrónico

La integración de ESET Internet Security 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, la integración se puede activar en ESET Internet Security. Cuando se integra en el cliente de correo electrónico, la barra de herramientas de ESET Internet Security se inserta directamente en el cliente de correo electrónico (la barra de herramientas de las versiones más recientes de Windows Live Mail no se inserta), aumentando así la eficacia de la protección del correo electrónico. Las opciones de integración están disponibles en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección de clientes de correo electrónico** > **Clientes de correo electrónico**.

Integración con el cliente de correo electrónico

Actualmente se admiten los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el

análisis de virus. Para ver una lista de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la base de conocimientos de ESET.

Aunque la integración no esté activada, la comunicación por correo electrónico sigue estando protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP).

Active **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si el sistema se ralentiza al trabajar con MS Outlook. Esto puede suceder cuando recupera correo electrónico de Kerio Outlook Connector Store.

Correo electrónico a analizar

Activar protección del correo electrónico mediante complementos del cliente: cuando la protección de clientes de correo electrónico mediante el cliente de correo electrónico se encuentra desactivada, la protección de clientes de correo electrónico por medio del filtrado de protocolos seguirá estando activa.
Correo electrónico recibido: activa el análisis de los mensajes recibidos.
Correo electrónico enviado: activa el análisis de los mensajes enviados.
Correo electrónico leído: activa el análisis de los mensajes leídos.

Acción para realizar en correos electrónicos infectados

Sin acción: si esta opción está activada, el programa identificará los archivos adjuntos infectados, pero dejará los mensajes sin realizar ninguna acción.
Eliminar correo electrónico: el programa informará al usuario sobre las amenazas y eliminará el mensaje.
Mover el correo electrónico a la carpeta de elementos eliminados: los mensajes infectados se moverán automáticamente a la carpeta Elementos eliminados.
Mover mensajes a la carpeta: los mensajes infectados se moverán automáticamente a la carpeta especificada.

Carpeta: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Repetir análisis después de actualizar: activa el nuevo análisis tras una actualización del motor de detección.

Aceptar los resultados de los análisis realizados por otros módulos: al seleccionar esta opción, el módulo de protección de correo electrónico acepta los resultados del análisis de otros módulos de protección (análisis de los protocolos POP3 e IMAP).

NOTA
Se recomienda activar "dejar" las opciones **Activar protección del correo electrónico mediante complementos del cliente** y **Activar la protección del correo electrónico mediante el filtrado de protocolos**. Estas opciones están disponibles en Configuración avanzada (F5) > Web y correo electrónico > Protección de clientes de correo electrónico > Protocolos de correo electrónico.

4.2.2.2 Protocolos de correo electrónico

Los protocolos IMAP y POP3 son los más utilizados para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. El Protocolo de acceso a mensajes de Internet (IMAP) es otro protocolo de Internet para la recuperación de mensajes de correo electrónico. IMAP presenta algunas ventajas sobre POP3; por ejemplo, permite la conexión simultánea de varios clientes al mismo buzón de correo y conserva la información de estado (si el mensaje se ha leído, contestado o eliminado). ESET Internet Security ofrece protección para estos protocolos independientemente del cliente de correo electrónico que se utilice, y sin necesidad de volver a configurar el cliente de correo electrónico.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema y, después, está activo en la memoria. El control del protocolo IMAP se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. De forma predeterminada se analizan todas las comunicaciones realizadas en el puerto 143, pero se pueden agregar otros puertos de comunicación si es necesario. Cuando haya varios números de puerto, deben delimitarse con una coma.

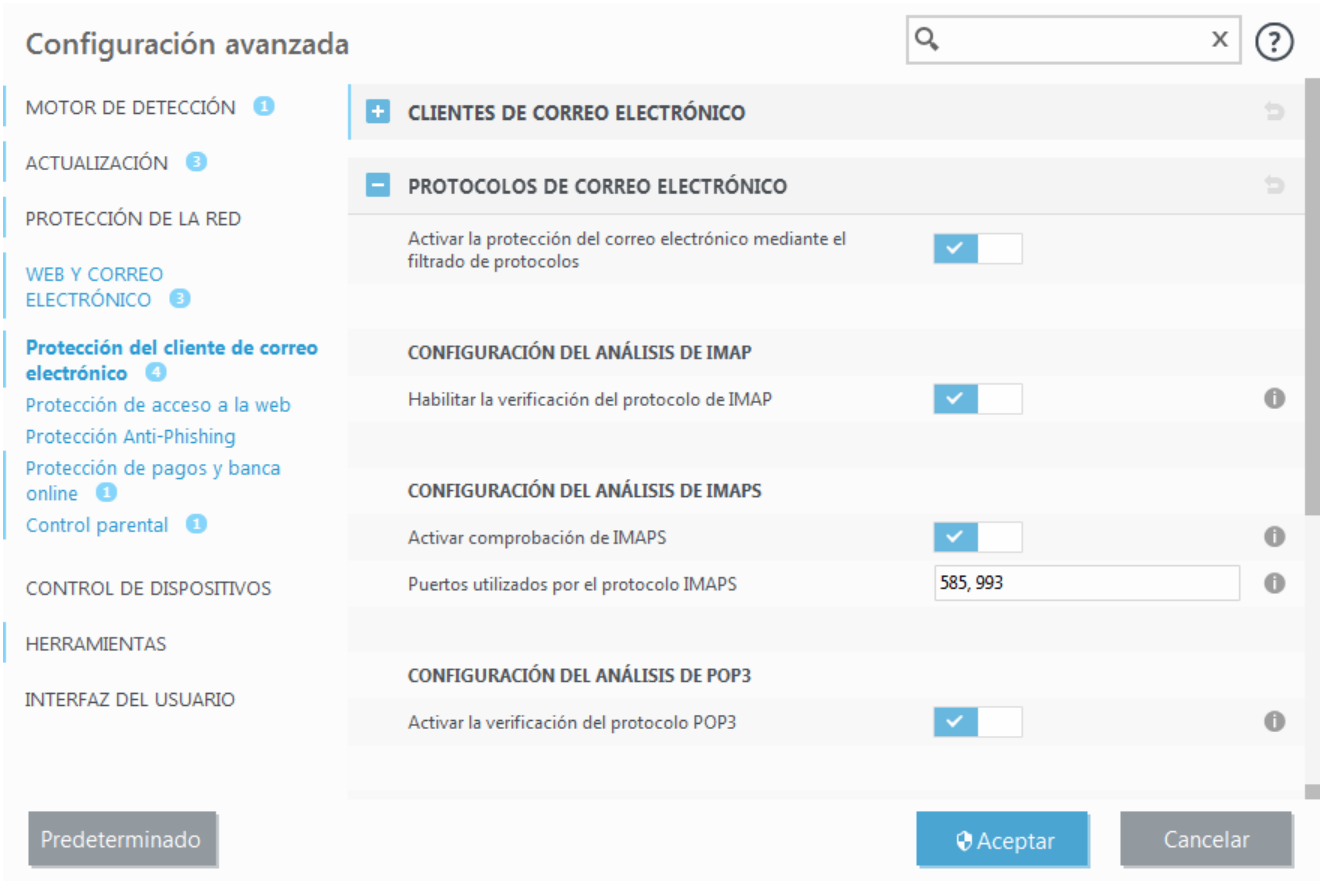
La verificación de los protocolos IMAP/IMAPS y POP3/POP3S se puede configurar en Configuración avanzada. Para acceder a esta configuración, despliegue **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Protocolos de correo electrónico**.

Activar la protección del correo electrónico mediante el filtrado de protocolos: permite la comprobación de los protocolos de correo electrónico.

En Windows Vista y versiones posteriores, los protocolos IMAP y POP3 se detectan automáticamente y se analizan en todos los puertos. En Windows XP solo se analizan para todas las aplicaciones los **Puertos usados por el protocolo IMAP/POP3**, y se analizan todos los puertos en busca de aplicaciones marcadas como Clientes de correo electrónico y web.

ESET Internet Security también admite el análisis de los protocolos IMAPS y POP3S, que utilizan un canal cifrado para transferir información entre el servidor y el cliente. ESET Internet Security comprueba la comunicación con los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en **Puertos usados por el protocolo IMAPS/POP3S**, independientemente de la versión del sistema operativo.

La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, vaya a SSL/TLS en la sección Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y active la opción **Activar el filtrado del protocolo SSL/TLS**.



4.2.2.3 Alertas y notificaciones

La protección de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET Internet Security ofrece control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP y HTTP). Al examinar los mensajes entrantes, el programa utiliza todos los métodos de análisis avanzados incluidos en el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con el motor de detección. El análisis de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

Las opciones de esta función están disponibles en **Configuración avanzada**, en **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Alertas y notificaciones**.

Después de analizar un mensaje de correo electrónico, se puede adjuntar al mensaje una notificación del análisis. Puede elegir entre las opciones **Notificar en los mensajes recibidos y leídos**, **Agregar una nota al asunto de los correos electrónicos infectados que fueron recibidos y leídos** o **Notificar en los mensajes enviados**. Tenga en cuenta

que en ocasiones puntuales es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o que hayan sido falsificados por código malicioso. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Están disponibles las opciones siguientes:

- **Nunca**: no se agregará ningún mensaje de etiqueta.
- **Solo al correo electrónico infectado**: únicamente se marcarán como analizados los mensajes que contengan software malicioso (opción predeterminada).
- **A todos los correos electrónicos analizados**: el programa agregará un mensaje a todo el correo analizado.

Agregar una nota al asunto de los correos electrónicos infectados enviados: desactive esta casilla de verificación si no desea que la protección de correo electrónico incluya una alerta de virus en el asunto de los mensajes infectados. Esta función permite el filtrado sencillo y por asunto de los mensajes infectados (si su programa de correo electrónico lo admite). Además, aumenta el nivel de credibilidad del destinatario. Si se detecta una amenaza, ofrece información valiosa sobre el nivel de amenaza de un correo electrónico o un remitente determinados.

Plantilla añadida al asunto del correo electrónico infectado: modifique esta plantilla si desea modificar el formato de prefijo del asunto de un mensaje infectado. Esta función sustituye el asunto del mensaje *"Hello"* con un valor de prefijo especificado *"[virus]"* por el formato siguiente: *"[virus] Hello"*. La variable *%VIRUSNAME%* hace referencia a la amenaza detectada.

4.2.2.4 Integración con clientes de correo electrónico

La integración de ESET Internet Security con clientes 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, la integración se puede activar en ESET Internet Security. Al activar la integración, la barra de herramientas de ESET Internet Security se inserta directamente en el cliente de correo electrónico, aumentando así la eficacia de la protección de correo electrónico. Las opciones de integración están disponibles en **Configuración** > **Configuración avanzada** > **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Clientes de correo electrónico**.

Actualmente, se admiten los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. Para ver una lista de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la base de conocimientos de ESET.

Seleccione la casilla de verificación situada junto a **Desactivar el análisis de cambios de contenido de la bandeja de entrada** si experimenta una ralentización del sistema cuando trabaja con su cliente de correo electrónico. Esto puede suceder cuando recupera correo electrónico de Kerio Outlook Connector Store.

Aunque la integración no esté activada, la comunicación por correo electrónico sigue estando protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP).

4.2.2.4.1 Configuración de la protección del cliente de correo electrónico

El módulo de protección cliente de correo electrónico admite los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus.

4.2.2.5 Filtro POP3, POP3S

El protocolo POP3 es el más utilizado para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. ESET Internet Security proporciona protección para este protocolo, independientemente del cliente de correo electrónico que se utilice.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema y, después, está activo en la memoria. Para que el módulo funcione correctamente, asegúrese de que está activado. La comprobación del protocolo POP3 se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. De forma predeterminada, se analizan todas las comunicaciones en el puerto 110, pero se pueden agregar otros puertos de comunicación si es necesario. Cuando haya varios números de puerto, deben delimitarse con una coma.

La comunicación cifrada se analizará de forma predeterminada. Para ver la configuración del análisis, vaya a SSL/TLS en la sección Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y active la opción **Activar el filtrado del protocolo SSL/TLS**.

En esta sección, puede configurar la comprobación de los protocolos POP3 y POP3S.

Activar la verificación del protocolo POP3: si esta opción está activada, se comprueba la presencia de software malicioso en todo el tráfico que pasa por POP3.

Puertos utilizados por el protocolo POP3: se trata de una lista de los puertos que utiliza el protocolo POP3 (de forma predeterminada, 110).

ESET Internet Security también admite la comprobación del protocolo POP3S. Este tipo de comunicación utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Internet Security comprueba la comunicación mediante los métodos de cifrado SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte).

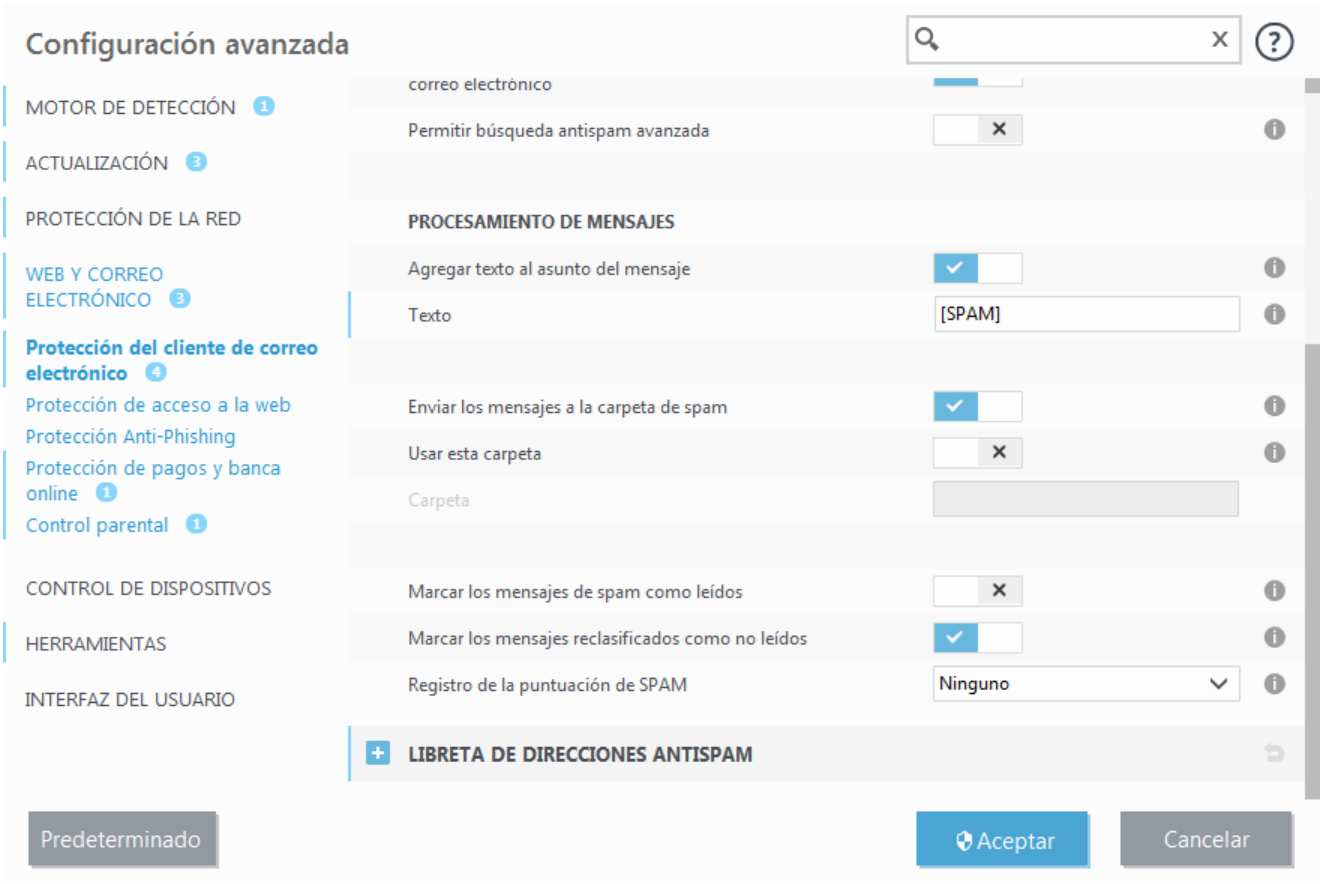
No utilizar la comprobación de POP3S: no se analizará la comunicación cifrada.

Utilizar la comprobación del protocolo POP3S para los puertos seleccionados: marque esta opción para activar el análisis POP3S solo de los puertos definidos en **Puertos utilizados por el protocolo POP3S**.

Puertos utilizados por el protocolo POP3S: consiste en una lista de puertos POP3S sujetos a análisis (de forma predeterminada, 995).

4.2.2.6 Protección Antispam

El correo electrónico no deseado (spam) es uno de los problemas más graves de la comunicación electrónica; representa hasta el 80 % de todas las comunicaciones por correo electrónico. La protección antispam sirve para protegerse frente a este problema. El módulo Antispam combina varios principios de seguridad del correo electrónico para ofrecer un filtrado superior para que su bandeja de entrada esté siempre desinfectada.



Un principio importante en la detección del correo no deseado es la capacidad de reconocer correo electrónico no solicitado a partir de listas de direcciones de confianza predefinidas (lista blanca) y de direcciones de correo no deseado (lista negra). Todas las direcciones de su lista de contactos se agregan automáticamente a la lista blanca, así como todas las demás direcciones que marque como seguras.

El principal método utilizado para detectar correo no deseado es el análisis de las propiedades de los mensajes de correo electrónico. Los mensajes recibidos se analizan con criterios básicos contra correo no deseado (definiciones de mensajes, heurística estadística, algoritmos reconocidos y otros métodos únicos) y el valor del índice resultante determina si un mensaje es deseado o no deseado.

Iniciar automáticamente la protección antispam del cliente de correo electrónico: si activa esta opción, la protección antispam se activará automáticamente al iniciar el sistema.

Permitir búsqueda antispam avanzada: se descargarán datos adicionales para correo no deseado periódicamente, lo cual mejorará las capacidades antispam y los resultados obtenidos.

La protección antispam de ESET Internet Security le permite definir varios parámetros para las listas de correo. Están disponibles las siguientes opciones:

Procesamiento de mensajes

Agregar texto al asunto del mensaje: le permite agregar un prefijo personalizado a la línea de asunto de los mensajes que se han clasificado como correo electrónico no deseado. La expresión predeterminada es "[SPAM]".

Enviar los mensajes a la carpeta de spam: si esta opción está activada, los mensajes no deseados se moverán a la carpeta predeterminada de correo basura, y los mensajes reclasificados como correo deseado se moverán a la bandeja de entrada. Cuando hace clic con el botón derecho del ratón en un mensaje de correo electrónico y selecciona ESET Internet Security en el menú contextual puede elegir entre las opciones aplicables.

Usar esta carpeta: esta opción mueve el correo no deseado a una carpeta definida por el usuario.

Marcar los mensajes de spam como leídos: active esta opción para marcar el correo no deseado como leído de forma automática. Esto le ayudará a centrar su atención en los mensajes "desinfectados".

Marcar los mensajes reclasificados como no leídos: se mostrarán como no leídos los mensajes que originalmente se clasificaron como correo no deseado, pero que después se marcaron como "desinfectados".

Registro del nivel de spam : el motor antispam de ESET Internet Security asigna un nivel de spam a cada uno de los mensajes analizados. El mensaje se anotará en el registro de antispam (**ESET Internet Security** > **Herramientas** > **Archivos de registro** > **Protección Antispam**).

- **Ninguno**: no se registrará el nivel obtenido en el análisis de correo no deseado.
- **Reclasificado y marcado como SPAM**: seleccione esta opción si desea registrar un nivel de spam a los mensajes marcados como correo no deseado.
- **Todos**: todos los mensajes se anotarán en el registro con un nivel de spam.

NOTA
Cuando hace clic en un mensaje de la carpeta de correo no deseado puede elegir **Reclasificar como correo deseado** y el mensaje se enviará a la bandeja de entrada. Si hace clic en un mensaje de la bandeja de entrada que considera como correo no deseado, seleccione **Reclasificar mensajes como correo no deseado** y el mensaje se enviará a la carpeta de correo no deseado. Puede seleccionar varios mensajes y efectuar la misma acción en todos ellos al mismo tiempo.

NOTA
ESET Internet Security admite la protección antispam para Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail.

4.2.3 Filtrado de protocolos

El motor de análisis ThreatSense, que integra a la perfección todas las técnicas avanzadas de análisis de código malicioso, proporciona la protección antivirus para los protocolos de aplicación. El filtrado de protocolos funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizados. Para editar la configuración cifrada (SSL/TLS), vaya a **Web y correo electrónico** > **SSL/TLS**.

Activar el filtrado del contenido de los protocolos de aplicación: se puede utilizar para desactivar el filtrado de protocolos. Tenga en cuenta que muchos componentes de ESET Internet Security (Protección del tráfico de Internet, Protección de protocolos de correo electrónico, Antiphishing, Control de acceso web) dependen de esto para funcionar.

Aplicaciones excluidas: le permite excluir determinadas aplicaciones del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Direcciones IP excluidas: le permite excluir determinadas direcciones remotas del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Clientes de correo electrónico y web: solo se utiliza en sistemas operativos Windows XP, y le permite seleccionar las aplicaciones para las que se filtra todo el tráfico con el filtrado de protocolos, independientemente de los puertos utilizados.

4.2.3.1 Clientes de correo electrónico y web

NOTA
La arquitectura Plataforma de filtrado de Windows (WFP) se empezó a aplicar en Windows Vista Service Pack 1 y Windows Server 2008, y se utiliza para comprobar la comunicación de red. La sección **Clientes de correo electrónico y web** no se encuentra disponible porque la tecnología WFP utiliza técnicas de supervisión especiales.

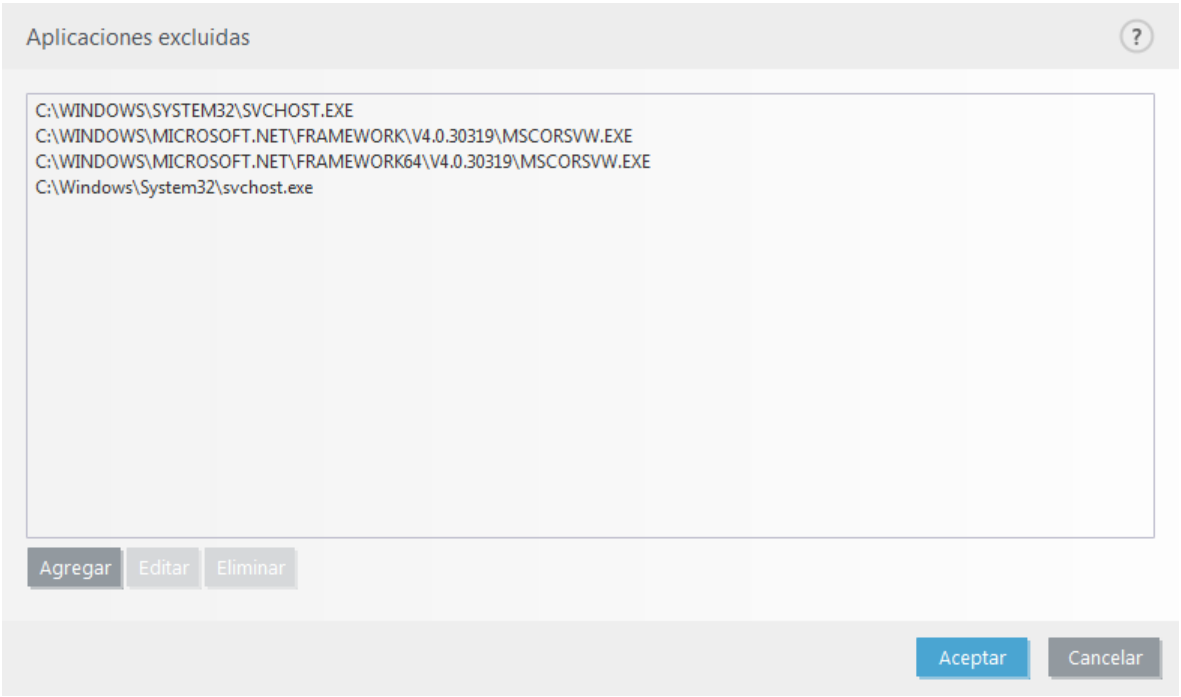
Dada la ingente cantidad de código malicioso que circula en Internet, la navegación segura es un aspecto crucial para la protección de los ordenadores. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET Internet Security se centra en la seguridad de los navegadores web. Cada aplicación que acceda a la red se puede marcar como un navegador de Internet. La casilla de verificación tiene dos estados:

- **Sin seleccionar**: la comunicación de las aplicaciones se filtra solamente para los puertos especificados.
- **Seleccionada**: la comunicación se filtra siempre (aunque se configure un puerto diferente).

4.2.3.2 Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones de red específicas, selecciónelas en la lista. No se comprobará la presencia de amenazas en la comunicación HTTP/POP3/IMAP de las aplicaciones seleccionadas. Se recomienda su uso únicamente en aplicaciones que no funcionen correctamente cuando se compruebe su comunicación.

Las aplicaciones y los servicios en ejecución estarán disponibles aquí de forma automática. Haga clic en **Agregar** para agregar manualmente una aplicación que no se muestre en la lista del filtrado de protocolos.

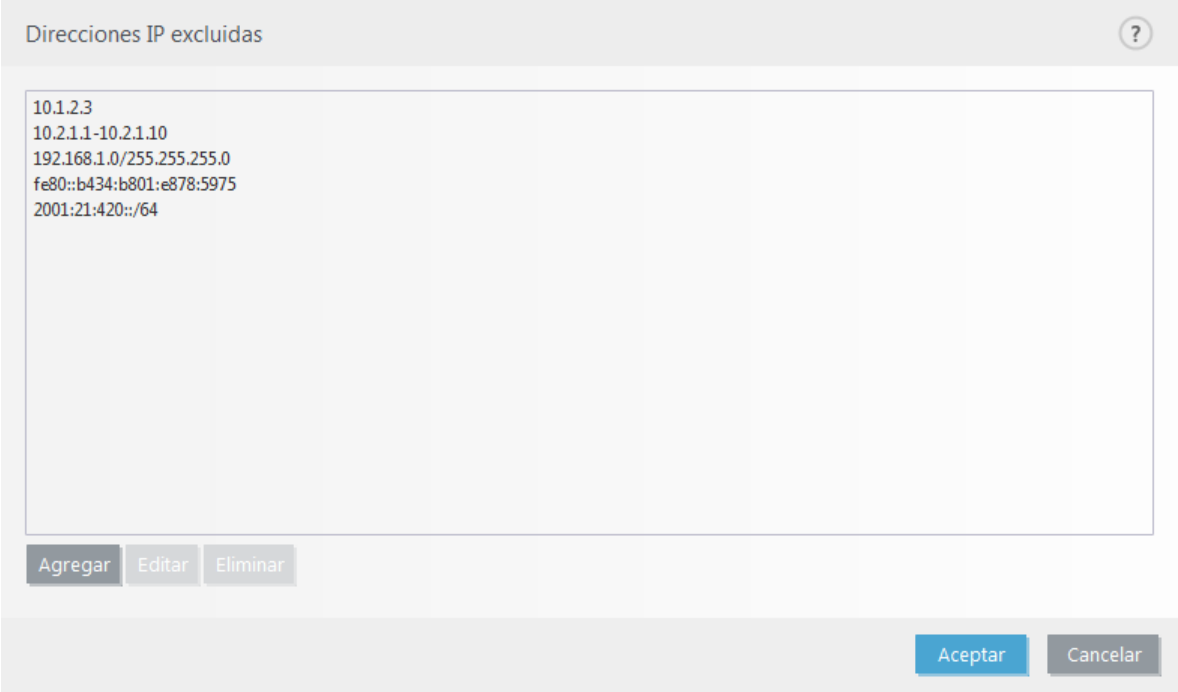


4.2.3.3 Direcciones IP excluidas

Las entradas de la lista se excluirán del filtrado de contenidos del protocolo. No se comprobará la presencia de amenazas en las comunicaciones HTTP/POP3/IMAP entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Haga clic en **Agregar** para excluir una dirección IP, un rango de direcciones o una subred de un punto remoto no mostrado en la lista de filtrado del protocolo.

Haga clic en **Quitar** para eliminar las entradas seleccionadas de la lista.



4.2.3.3.1 Agregar dirección IPv4

Esta opción le permite agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplica la regla. El protocolo de Internet versión 4 es el más antiguo, pero sigue siendo el más utilizado.

Dirección única: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla (por ejemplo, *192.168.0.10*).

Rango de direcciones: especifique las direcciones IP inicial y final para delimitar el intervalo de direcciones (de varios ordenadores) al que se aplicará la regla (por ejemplo, de *192.168.0.1* a *192.168.0.99*).

Subred: grupo de ordenadores definido por una dirección IP y una máscara.

Por ejemplo, *255.255.255.0* es la máscara de red del prefijo *192.168.1.0/24* (es decir, el intervalo de direcciones de *192.168.1.1* a *192.168.1.254*).

4.2.3.3.2 Agregar dirección IPv6

Esta opción le permite agregar una dirección IPv6 o una subred de un punto remoto al que se aplica la regla. Esta es la versión más reciente del protocolo de Internet, que sustituirá a la versión 4 anterior.

Dirección única: agrega la dirección IP de un ordenador individual al que debe aplicarse la regla (por ejemplo, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subred: grupo de ordenadores definido por una dirección IP y una máscara (por ejemplo: *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET Internet Security puede buscar amenazas en las comunicaciones que utilizan el protocolo SSL. Puede utilizar varios modos de análisis para examinar las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos del análisis de comunicaciones protegidas mediante el protocolo SSL.

Habilitar el filtrado del protocolo de SSL/TLS: si está desactivado el filtrado de protocolos, el programa no analizará las comunicaciones realizadas a través de SSL.

El **modo de filtrado del protocolo SSL/TLS** ofrece las opciones siguientes:

Modo automático: el modo predeterminado solo analizará las aplicaciones correspondientes, como navegadores de Internet y clientes de correo. Puede anular esta opción seleccionando las aplicaciones para las que se analizarán las comunicaciones.

Modo interactivo: si entra en un sitio nuevo protegido mediante SSL (con un certificado desconocido), se muestra un cuadro de diálogo con las acciones posibles. Este modo le permite crear una lista de aplicaciones o certificados SSL que se excluirán del análisis.

Modo de política: seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL, excepto las protegidas por certificados excluidos del análisis. Si se establece una comunicación nueva que utiliza un certificado firmado desconocido, no se le informará y la comunicación se filtrará automáticamente. Si accede a un servidor con un certificado que no sea de confianza pero que usted ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

Lista de aplicaciones con filtrado SSL: permite personalizar el comportamiento de ESET Internet Security para aplicaciones específicas.

Lista de certificados conocidos: permite personalizar el comportamiento de ESET Internet Security para certificados SSL específicos.

Excluir la comunicación con los dominios de confianza: cuando esta opción está activada, la comunicación con los dominios de confianza se excluye de la comprobación. La confianza en los dominios se determina mediante la lista blanca integrada.

Bloquear la comunicación cifrada utilizando el protocolo obsoleto SSL v2: la comunicación establecida con la versión anterior del protocolo SSL se bloqueará automáticamente.

Certificado raíz

Agregar el certificado raíz a los navegadores conocidos: para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). Cuando esté activada, ESET Internet Security agregará el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

Validez del certificado

Si el certificado no se puede verificar mediante el almacén de certificados TRCA: a veces no es posible verificar el certificado de un sitio web con el almacén de autoridades certificadoras de confianza (TRCA). Esto significa que el certificado ha sido firmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre representa un riesgo. La mayoría de las empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a sitios que tienen certificados sin verificar.

Si el certificado no es válido o está dañado: significa que el certificado ha caducado o que la firma no es correcta. En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**.

4.2.3.4.1 Certificados

Para que la comunicación SSL funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). **Añadir el certificado raíz a los navegadores conocidos** debe estar activada. Seleccione esta opción para agregar el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer). Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

En algunos casos, el certificado no se puede comprobar mediante el archivo de autoridades certificadoras de confianza (por ejemplo, VeriSign). Esto significa que el certificado ha sido autofirmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre representa un riesgo. La mayoría de empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. Se mostrará un cuadro de diálogo de selección que le permite marcar el certificado como de confianza o excluirlo. Si el certificado no se encuentra en la lista de TRCA, la ventana se mostrará en rojo, y si está en dicha lista, la ventana se mostrará en verde.

Bloquear las comunicaciones que utilicen el certificado se puede seleccionar para que se terminen todas las conexiones cifradas con el sitio que utilicen un certificado sin verificar.

Si el certificado no es válido o está dañado, significa que ha expirado o que la autofirma no es correcta. En este caso, se recomienda bloquear las comunicaciones que utilicen dicho certificado.

4.2.3.4.1.1 Tráfico de red cifrado

Si el ordenador está configurado para análisis del protocolo SSL, es posible que se abra un cuadro de diálogo solicitándole que seleccione una acción cuando haya un intento de establecer una comunicación cifrada (utilizando un certificado desconocido).

El cuadro de diálogo contiene la siguiente información:

- nombre de la aplicación que inició la comunicación
- nombre del certificado utilizado
- acción para realizar: si analizar la comunicación cifrada y si recordar la acción para la aplicación o el certificado

Si no se encuentra el certificado en el archivo de autoridades certificadoras de confianza (TRCA), se considerará que no es de confianza.

4.2.3.4.2 Lista de certificados conocidos

La **Lista de certificados conocidos** se puede utilizar para personalizar el comportamiento de ESET Internet Security para determinados certificados SSL, así como para recordar las acciones elegidas al seleccionar el **Modo interactivo** en el **Modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **SSL/TLS** > **Lista de certificados conocidos**.

La ventana **Lista de certificados conocidos** consta de estos elementos:

Columnas

Nombre: nombre del certificado.

Emisor del certificado: nombre del creador del certificado.

Sujeto del certificado: en este campo se identifica a la entidad asociada a la clave pública almacenada en el campo de clave pública del asunto.

Acceso: seleccione **Permitir** o **Bloquear** como **Acción del acceso** para permitir o bloquear la comunicación que protege este certificado, independientemente de su fiabilidad. Seleccione **Auto** para permitir los certificados de confianza y preguntar cuando uno no sea de confianza. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Analizar: seleccione **Analizar** o **Ignorar** como **Acción de análisis** para analizar o ignorar la comunicación que protege este certificado. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

Agregar: agrega un certificado nuevo y ajusta su configuración de opciones de análisis y acceso.

Modificar: seleccione el certificado que desea configurar y haga clic en **Modificar**.

Quitar: seleccione el certificado que desea eliminar y haga clic en **Quitar**.

Aceptar/Cancelar: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

4.2.3.4.3 Lista de aplicaciones con filtrado SSL/TLS

La **Lista de aplicaciones con filtrado SSL/TLS** se puede utilizar para personalizar el comportamiento de ESET Internet Security para determinadas aplicaciones, así como para recordar las acciones elegidas al seleccionar el **Modo interactivo** en el **Modo de filtrado de protocolos SSL/TLS**. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **SSL/TLS** > **Lista de aplicaciones con filtrado SSL/TLS**.

La ventana **Lista de aplicaciones con filtrado SSL/TLS** consta de estos elementos:

Columnas

Aplicación: nombre de la aplicación.

Acción de análisis: seleccione **Analizar** o **Ignorar** para analizar o ignorar la comunicación. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

Agregar: agregue la aplicación filtrada.

Modificar: seleccione el certificado que desea configurar y haga clic en **Modificar**.

Quitar: seleccione el certificado que desea eliminar y haga clic en **Quitar**.

Aceptar/Cancelar: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

4.2.4 Protección antiphishing

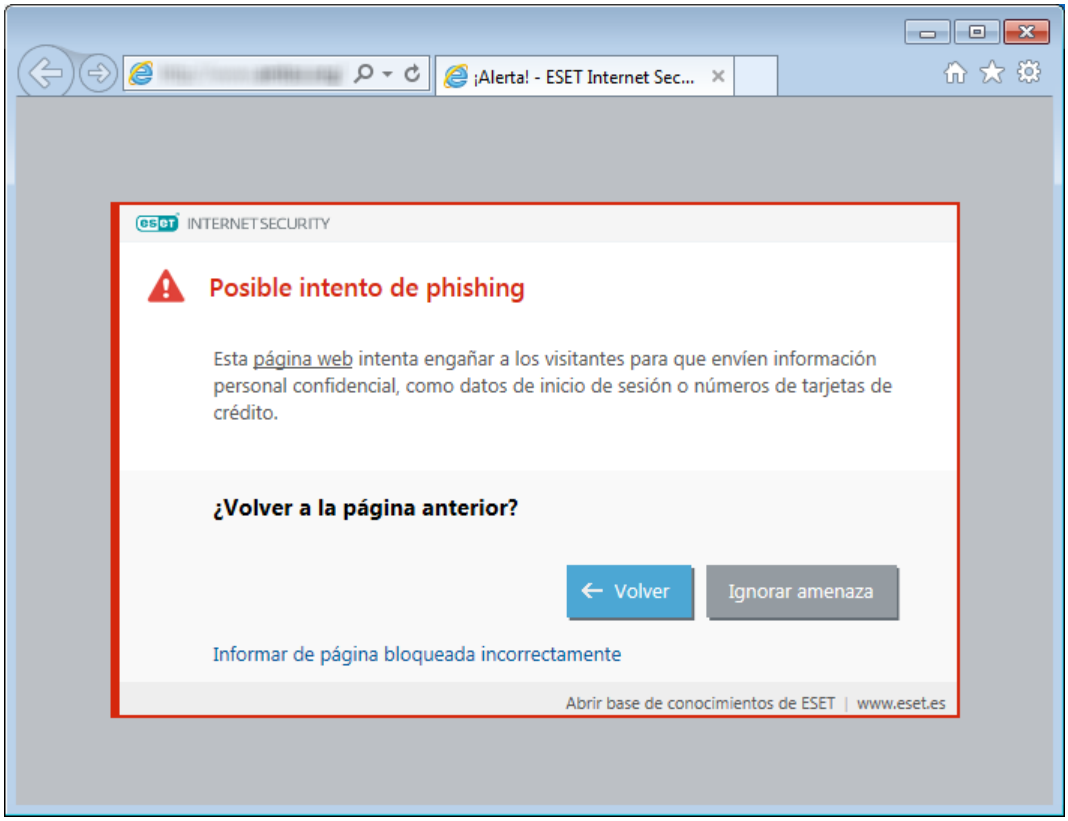
El término phishing, o suplantación de la identidad, define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo con frecuencia es acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre esta actividad en el glosario. ESET Internet Security incluye protección frente al phishing que bloquea páginas web conocidas por distribuir este tipo de contenido.

Recomendamos encarecidamente que active la protección Antiphishing en ESET Internet Security. Para ello, abra **Configuración avanzada** (F5) y acceda a **Web y correo electrónico** > **Protección antiphishing**.

Visite nuestro artículo de la base de conocimiento para obtener más información sobre la protección Antiphishing de ESET Internet Security.

Acceso a un sitio web de phishing

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



NOTA

Los posibles sitios de phishing que se han incluido en la lista blanca expirarán de forma predeterminada después de unas horas. Para permitir un sitio web permanentemente, use la herramienta Gestión de direcciones URL. En **Configuración avanzada** (F5), despliegue **Web y correo electrónico** > **Protección del tráfico de Internet** > **Gestión de direcciones URL**> **Lista de direcciones**, haga clic en **Modificar** y agregue a la lista el sitio web que desee modificar.

Cómo informar de sitios de phishing

El enlace Informar le permite informar de un sitio web de phishing o malicioso para que ESET lo analice.

NOTA

Antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:

- El sitio web no se detecta en absoluto.
- El sitio web se detecta como una amenaza, pero no lo es. En este caso, puede Informar de página bloqueada incorrectamente.

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

4.3 Protección de la red

El cortafuegos se encarga de controlar todo el tráfico de red entrante y saliente del sistema. Esta tarea se lleva a cabo permitiendo o denegando conexiones de red individuales en función de las reglas de filtrado. Proporciona protección frente a ataques procedentes de ordenadores remotos y activa el bloqueo de determinados dispositivos. También ofrece protección antivirus para los protocolos HTTP, POP3 e IMAP. Esta funcionalidad representa un elemento muy importante para la seguridad del ordenador. ESET Internet Security le informará cuando se conecte a una red inalámbrica no protegida o a una red con un nivel de protección débil.

Puede consultar la configuración del cortafuegos en el panel **Configuración** bajo **Protección de la red**. Aquí puede ajustar el modo de filtrado, las reglas y la configuración detallada; también puede acceder a opciones de configuración más detalladas haciendo clic en la rueda dentada > **Configurar...**, junto a **Cortafuegos**, o pulsando **F5** para acceder a Configuración avanzada.

Haga clic en la rueda dentada disponible junto a **Cortafuegos** para acceder a las opciones de configuración siguientes:

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

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

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

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

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

Protección contra los ataques de red (IDS) : analiza el contenido del tráfico de red y le protege contra posibles ataques de red. Se bloqueará el tráfico que se considere dañino.

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

Redes conectadas: muestra las redes a las que están conectados los adaptadores de red. Tras hacer clic en el nombre de red, se le solicitará que seleccione un tipo de protección (restrictiva o normal) para la red a la que está conectado a través de su adaptador de red. Este ajuste define el nivel de accesibilidad a su ordenador con respecto a otros ordenadores en la red.

Lista negra temporal de direcciones IP: muestra una lista de direcciones IP que se han detectado como fuente de los ataques y se han agregado a la lista negra para bloquear la conexión durante un período de tiempo concreto. Para obtener más información, haga clic en esta opción y pulse F1.

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

4.3.1 Cortafuegos

El cortafuegos se encarga de controlar todo el tráfico de red entrante y saliente del sistema. Esta tarea se lleva a cabo permitiendo o denegando conexiones de red individuales en función de las reglas de filtrado especificadas. Proporciona protección frente a ataques procedentes de ordenadores remotos y puede bloquear servicios potencialmente peligrosos. También ofrece protección antivirus para los protocolos HTTP, POP3 e IMAP.

Básico

Activar el cortafuegos: se recomienda mantener esta función activada para garantizar la seguridad del sistema. Cuando el cortafuegos está activado, el tráfico de la red se analiza en ambas direcciones.

Evaluar también las reglas del Firewall de Windows: en el modo automático, permitir también el tráfico entrante permitido por las reglas del Firewall de Windows, a menos que las reglas de ESET lo bloqueen explícitamente.

Modo de filtrado: el comportamiento del cortafuegos cambia en función del modo de filtrado. Los modos de filtrado influyen igualmente en el nivel de interacción del usuario. El cortafuegos de ESET Internet Security cuenta con los tres modos de filtrado siguientes:

Modo automático: este es el modo predeterminado; es aconsejable para usuarios que optan por un uso sencillo y cómodo del cortafuegos sin necesidad de definir reglas. Se pueden crear reglas personalizadas, definidas por el usuario, pero en este modo no es obligatorio. Este modo permite todo el tráfico saliente para un sistema en cuestión y bloquea casi todo el tráfico entrante, excepto determinado tráfico procedente de la zona de confianza, como se especifica en Sistema de detección de intrusos y opciones avanzadas/Servicios permitidos, y las respuestas a las comunicaciones salientes recientes.

Modo interactivo: le permite crear una configuración personalizada para el cortafuegos. Cuando se detecta una comunicación para la que no existen reglas, aparece un cuadro de diálogo que notifica la existencia de una conexión desconocida. El cuadro de diálogo ofrece la opción de permitir o denegar la comunicación; la decisión de permitirla o denegarla se puede recordar como una regla nueva para el cortafuegos. Si el usuario opta por crear una nueva regla, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla.

Modo basado en reglas: bloquea todas las conexiones que no se hayan definido en una regla específica que las permita. Este modo permite a los usuarios avanzados definir reglas que autoricen únicamente las conexiones especificadas y seguras. El cortafuegos bloqueará todas las demás conexiones no especificadas.

Modo de aprendizaje: crea y guarda reglas automáticamente. Este modo está recomendado para la configuración inicial del cortafuegos, pero no se debe mantener activado durante periodos de tiempo prolongados. No es necesaria la intervención del usuario, pues ESET Internet Security guarda las reglas según los parámetros predefinidos. El modo de aprendizaje solo debe utilizarse hasta que se hayan creado todas las reglas para las comunicaciones necesarias para evitar riesgos de seguridad.

Puede utilizar perfiles para personalizar el comportamiento del cortafuegos de ESET Internet Security especificando diferentes conjuntos de reglas para distintas situaciones.

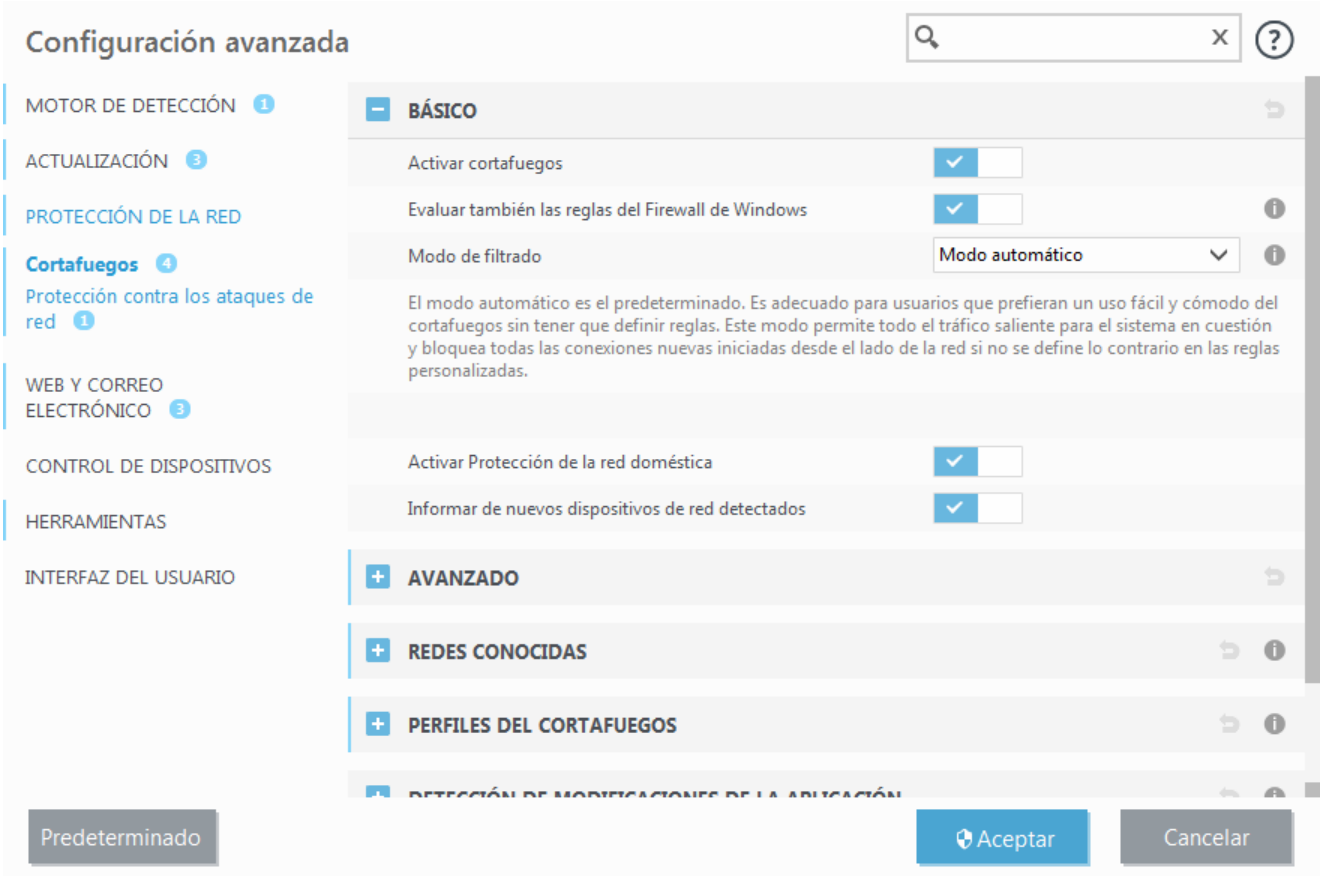
Activar Protección de la red doméstica: protege los ordenadores de las amenazas de red entrantes (Wi-Fi).

Informar de nuevos dispositivos de red detectados: le avisa cuando se detecta un dispositivo nuevo en la red.

Avanzado

Reglas: aquí puede agregar reglas y definir el método que utiliza el cortafuegos para gestionar el tráfico de red.

Zonas: aquí puede crear zonas que contienen una o varias direcciones IP.



NOTA

Puede crear una excepción de IDS cuando sufra un ataque de botnet en su ordenador. Las excepciones se pueden modificar en **Configuración avanzada** (F5) > **Protección de la red** > **Protección contra los ataques de red** > **Excepciones de IDS** haciendo clic en **Modificar**.

4.3.1.1 Configuración del modo de aprendizaje

En el modo de aprendizaje, se pueden crear y guardar reglas automáticamente para cada comunicación que se haya establecido en el sistema. No es necesaria la intervención del usuario, pues ESET Internet Security guarda las reglas según los parámetros predefinidos.

Este modo puede exponer su sistema a riesgos, por lo que solo se recomienda para la configuración inicial del cortafuegos.

Seleccione **Modo de aprendizaje** en el menú desplegable de **Configuración avanzada** (F5) > **Cortafuegos** > **Básico** > **Modo de filtrado** para activar **Opciones de modo de aprendizaje**. Esta sección contiene los elementos siguientes:

ADVERTENCIA

El cortafuegos no filtra la comunicación cuando el modo de aprendizaje está activado. Se permiten todas las comunicaciones de entrada y salida. En este modo el ordenador no cuenta con la protección completa del cortafuegos.

Tipo de comunicación: seleccione los parámetros de creación de reglas para cada tipo de comunicación. Hay cuatro tipos de comunicación:

- **Tráfico entrante de una zona de confianza**: un ordenador remoto de la zona de confianza que intenta comunicarse con una aplicación local de su ordenador sería un ejemplo de conexión entrante.

- **Tráfico saliente a una zona de confianza**: una aplicación local intenta establecer una conexión con otro ordenador dentro de la red local, o dentro de una red en la zona de confianza.

- **Tráfico de Internet entrante**: un ordenador remoto intenta comunicarse con una aplicación que se está ejecutando en el ordenador.

- **Tráfico de Internet saliente**: una aplicación local que intenta establecer una conexión con otro ordenador.

En todas las secciones puede definir los parámetros que desea agregar a las reglas de reciente creación:

Agregar puerto local: incluye el número de puerto local de la comunicación de red. Para las comunicaciones salientes, normalmente se generan números aleatorios. Por este motivo, le recomendamos que active esta opción solo para las comunicaciones entrantes.

Agregar aplicación: incluye el nombre de la aplicación local. Esta opción es útil para reglas futuras a nivel de aplicaciones (reglas que definen la comunicación para una aplicación entera). Por ejemplo, puede activar la comunicación solo para un navegador web o para un cliente de correo electrónico.

Agregar puerto remoto: incluye el número de puerto remoto de la comunicación de red. Por ejemplo, puede aceptar o denegar un servicio específico asociado con un número de puerto estándar (HTTP – 80, POP3 – 110, etc.).

Agregar dirección IP remota/zona de confianza: se puede utilizar una dirección IP remota o una zona como un parámetro para nuevas reglas que definan todas las conexiones de red entre el sistema local y dicha dirección remota o zona. Esta opción resulta útil a la hora de definir acciones para un ordenador concreto o un grupo de ordenadores en red.

Cantidad máxima de reglas distintas para una aplicación: si una aplicación se comunica a través de diferentes puertos con varias direcciones IP, etc., el cortafuegos en modo de aprendizaje crea un número adecuado de reglas para esta aplicación. Esta opción le permite limitar el número de reglas que se pueden crear para una sola aplicación.

4.3.1.2 Protección contra los ataques de red

Activar Protección contra los ataques de red (IDS) : analiza el contenido del tráfico de red y le protege contra posibles ataques de red. Se bloqueará todo el tráfico que se considere dañino.

Activar protección contra botnets: detecta y bloquea las comunicaciones asociadas con servidores de control y comando maliciosos reconociendo patrones habituales que indican que el ordenador está infectado y un bot intenta establecer comunicación.

Excepciones de IDS: le permite agregar excepciones de IDS y personalizar la respuesta ante actividades maliciosas.

4.3.2 Perfiles del cortafuegos

Los perfiles se pueden utilizar para controlar el comportamiento del cortafuegos de ESET Internet Security. Cuando cree o edite una regla para el cortafuegos, puede asignarla a un perfil específico o a todos los perfiles. Cuando hay un perfil activo en una interfaz de red, solo se aplican las reglas globales (que no tienen un perfil especificado) y las reglas que se han asignado a dicho perfil. Puede crear varios perfiles con reglas diferentes asignadas a adaptadores de red o a redes con el fin de modificar fácilmente el comportamiento del cortafuegos.

Haga clic en **Modificar** junto a la Lista de perfiles para abrir la ventana **Perfiles del cortafuegos** en la que puede modificar los perfiles.

Es posible configurar un adaptador de red para que utilice un perfil configurado para una red específica cuando esté conectado a dicha red. También puede asignar un perfil específico en **Configuración avanzada** (F5) > **Protección de la red** > **Cortafuegos** > **Redes conocidas** para utilizarlo cuando se encuentre en una red determinada. Seleccione una red de la lista de **Redes conocidas** y haga clic en **Modificar** para asignar un perfil del cortafuegos a la red especificada desde el menú desplegable **Perfiles de cortafuegos**. Si esa red no tiene ningún perfil asignado, se utilizará el perfil predeterminado del adaptador. Si el adaptador está configurado para que no utilice el perfil de la red, se utilizará su perfil predeterminado independientemente de la red a la que esté conectado. Si no hay ningún perfil para una red ni para la configuración del adaptador, se utiliza el perfil global predeterminado. Para asignar un perfil a un adaptador de red, seleccione el adaptador de red, haga clic en **Modificar** junto a **Perfiles asignados a adaptadores de red**, modifique el adaptador de red seleccionado y seleccione el perfil en el menú desplegable **Perfil de cortafuegos predeterminado**.

Cuando el cortafuegos cambia de perfil se muestra una notificación en la esquina inferior derecha, cerca del reloj del sistema.

4.3.2.1 Perfiles asignados a adaptadores de red

Cambie de perfil para aplicar varias modificaciones al comportamiento del cortafuegos rápidamente. Puede definir y aplicar reglas personalizadas para perfiles específicos. Las entradas de adaptador de red de todos los adaptadores disponibles en el ordenador se agregan automáticamente a la lista de **adaptadores de red**.

Columnas

Nombre: nombre del adaptador de la red.

Perfil de cortafuegos predeterminado: el perfil predeterminado se utiliza cuando la red a la que está conectado no tiene ningún perfil configurado o el adaptador de la red está configurado para que no utilice un perfil de red.

Preferir perfil de la red: si está activada la opción **Preferir el perfil del cortafuegos de la red conectada**, el adaptador de la red utiliza el perfil del cortafuegos asignado a una red conectada siempre que es posible.

Elementos de control

Agregar: agrega un adaptador de red nuevo.

Modificar: le permite editar un adaptador de red existente.

Quitar: seleccione un adaptador de red y haga clic en **Quitar** para quitar de la lista un adaptador de red.

Aceptar/Cancelar : haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

4.3.3 Configuración y uso de reglas

Las reglas representan un conjunto de condiciones que se utilizan para probar de manera significativa todas las conexiones de red y acciones asignadas a estas condiciones. Utilice las reglas del cortafuegos para definir la acción que se emprende al establecer diferentes tipos de conexión de red. Para acceder a la configuración del filtrado de reglas, vaya a **Configuración avanzada** (F5) > **Cortafuegos** > **Básico**. Algunas de las reglas predefinidas dependen de las casillas de verificación de **servicios permitidos** (Sistema de detección de intrusos y opciones avanzadas) y no se pueden desactivar directamente, sino a través de las casillas de verificación asociadas.

Las reglas se evalúan en orden descendente, no como en la versión anterior de ESET Internet Security. La acción de la primera regla coincidente se utiliza para todas las conexiones de red evaluadas. Este es un cambio de comportamiento muy importante con respecto a la versión anterior, en la que la prioridad de las reglas era automática y las reglas más específicas tenían prioridad sobre las reglas generales.

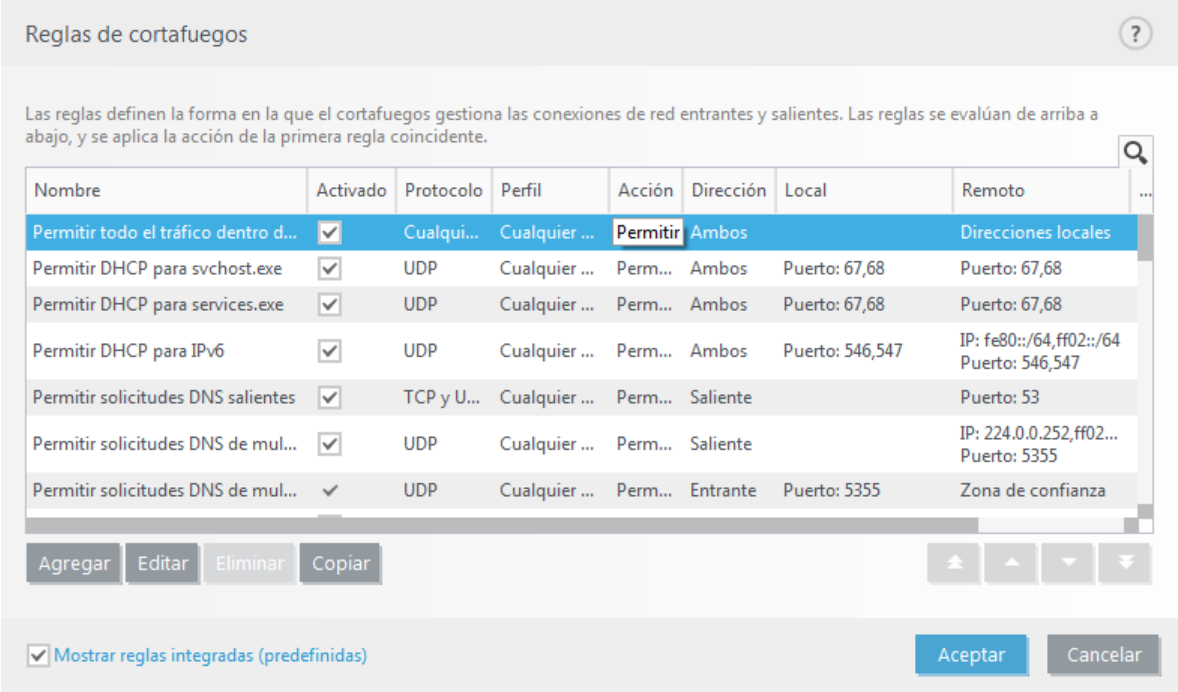
Las conexiones se pueden dividir en entrantes y salientes. Las conexiones entrantes se inician en ordenadores remotos que intenten establecer una conexión con el sistema local, Las conexiones salientes funcionan de la forma opuesta; es decir, el sistema local se comunica con el ordenador remoto.

Si se detecta una comunicación desconocida, debe considerar detenidamente el hecho de permitirla o denegarla. Las conexiones no solicitadas, no seguras o desconocidas suponen un riesgo de seguridad para el sistema. Si se establece una conexión de este tipo, debe prestar especial atención al ordenador remoto y a la aplicación que intente conectarse a su ordenador. Muchas amenazas intentan obtener y enviar datos privados, o descargar otras aplicaciones maliciosas en las estaciones de trabajo host. El cortafuegos le permite detectar e interrumpir estas conexiones.

4.3.3.1 Reglas de cortafuegos

Haga clic en **Modificar** junto a **Reglas** en la sección **Básico** para abrir la ventana **Reglas de cortafuegos**, donde se muestra una lista con todas las reglas. Las opciones **Agregar**, **Modificar** y **Quitar** le permiten agregar, configurar o eliminar las reglas. Puede ajustar el nivel de prioridad de una regla al seleccionar las reglas y hacer clic en **Superior/Arriba/Abajo/Inferior**.

CONSEJO: puede usar el campo **Buscar** para buscar una regla por nombre, protocolo o puerto.



Columnas

Nombre: nombre de la regla.

Habilitado: muestra si las reglas están activadas o desactivadas; marque la casilla de verificación para activar la regla.

Protocolo: indica el protocolo al que se aplica esta regla.

Perfil: muestra el perfil de cortafuegos al que se aplica esta regla.

Acción: muestra el estado de la comunicación (bloquear, permitir o preguntar).

Dirección: dirección de la comunicación (entrante, saliente o ambas).

Local: dirección IP y puerto del ordenador local.

Remoto: dirección IP y puerto del ordenador remoto.

Aplicaciones: indica la aplicación a la que se aplica la regla.

Elementos de control

Agregar: crea una nueva regla.

Modificar: le permite editar reglas ya existentes.

Quitar: elimina reglas existentes.

Mostrar reglas integradas (predefinidas): reglas predefinidas de ESET Internet Security que permiten o rechazan determinadas comunicaciones. Las reglas predefinidas pueden desactivarse, pero no eliminarse.

Superior/Arriba/Abajo/Inferior: le permite ajustar el nivel de prioridad de las reglas (las reglas se ejecutan de arriba hacia abajo).

4.3.3.2 Trabajo con las reglas

Esta modificación es necesaria cada vez que se cambia alguno de los parámetros controlados. La conexión podría rechazarse si, a causa de los cambios realizados, la regla no cumple las condiciones y la acción especificada no se puede aplicar. Esto puede provocar problemas de funcionamiento en la aplicación a la que se aplica la regla. Un ejemplo de este caso sería la modificación de la dirección de red o del número de puerto de la ubicación remota.

En la parte superior de la ventana están disponibles las tres fichas siguientes:

- **General**: especifique un nombre de regla, la dirección de la conexión, la acción (**Permitir**, **Bloquear**, **Preguntar**), el protocolo y el perfil al que se aplicarán la regla.
- **Local**: muestra información sobre el punto local de la conexión, incluido el número del puerto local, o el intervalo de puertos, y el nombre de la aplicación que intenta establecer la comunicación. Además le permite agregar aquí una zona predefinida o creada con un rango de direcciones IP al hacer clic en **Agregar**.
- **Remoto**: esta ficha contiene información acerca del puerto remoto (o intervalo de puertos). También le permite definir una lista de zonas o direcciones IP remotas para una regla determinada. Igualmente, le permite agregar aquí una zona predefinida o creada con un rango de direcciones IP al hacer clic en **Agregar**.

Cuando cree una regla nueva, debe introducir un nombre para la regla en el campo **Nombre**. Seleccione la dirección a la que se aplicará la regla en el menú desplegable **Dirección** y la acción que se debe ejecutar cuando una comunicación cumpla la regla en el menú desplegable **Acción**.

Protocolo representa el protocolo de transferencia utilizado para la regla. Seleccione el protocolo que desea utilizar para una regla dada en el menú desplegable.

El **código/tipo de ICMP** representa un mensaje ICMP identificado mediante un número (por ejemplo, 0 representa a "respuesta de eco").

Todas las reglas están activadas para **Cualquier perfil** de forma predeterminada. También puede seleccionar un perfil de cortafuegos personalizado en el menú desplegable **Perfil**.

Si activa **Registro**, la actividad relacionada con la regla se anotará en un registro. **Advertir al usuario** muestra una notificación cuando se aplica la regla.

NOTA

A continuación se proporciona un ejemplo donde se crea una regla nueva para permitir que la aplicación de navegador web acceda a la red. Debe configurarse lo siguiente:

- En la pestaña **General** active la comunicación saliente a través de los protocolos TCP y UDP.
- Agregue la aplicación de su navegador (para Internet Explorer es iexplore.exe) en la pestaña **Local**.
- En la ficha **Remoto**, active el número de puerto 80 si desea permitir la búsqueda estándar en Internet.

NOTA
Tenga en cuenta que solo pueden modificarse determinados valores de las reglas predefinidas.

4.3.4 Configuración de zonas

Una zona representa una recopilación de direcciones de red que conforman un grupo lógico de direcciones IP, muy útil cuando es necesario reutilizar el mismo conjunto de direcciones en varias reglas. A cada dirección del grupo concreto se le asignan reglas similares definidas de manera centralizada para todo el grupo. Un ejemplo de dicho grupo es una **Zona de confianza**. Una Zona de confianza representa un grupo de direcciones de red que no están bloqueadas de forma alguna por el cortafuegos. Estas zonas se pueden configurar en **Configuración avanzada** > **Cortafuegos**> **Avanzado**, haciendo clic en **Modificar** junto a **Zonas**. Para agregar una zona nueva, haga clic en **Agregar**, introduzca un **Nombre** para la zona, una **Descripción** y añada una dirección IP remota en el campo **Dirección del ordenador remoto (IPv4, IPv6, intervalo, máscara)**.

En la ventana de configuración **Zonas de cortafuegos**, puede especificar un nombre, una descripción y una lista de direcciones de red para la zona (consulte también Editor de redes conocidas).

4.3.5 Redes conocidas

Si utiliza un ordenador que se conecta con frecuencia a redes públicas o redes que se encuentran fuera de su red doméstica o de oficina habitual, le recomendamos que verifique la credibilidad de las redes nuevas a las que se conecte. Una vez que se han definido las redes, ESET Internet Security puede reconocer las redes de confianza (red doméstica o de oficina) utilizando varios parámetros de red configurados en **Identificación de red**. Es frecuente que los ordenadores accedan a redes con direcciones IP similares a la red de confianza. En estos casos, ESET Internet Security puede considerar que una red desconocida es de confianza (red doméstica o de oficina). Le recomendamos que utilice **Autenticación de red** para evitar este tipo de situación.

Cuando se conecta un adaptador de red a una red o se vuelven a configurar las opciones de red, ESET Internet Security busca en la lista de redes conocidas un registro que coincida con la nueva red. Si los valores de **Identificación de red** y **Autenticación de red** (opcional) coinciden, la red se marcará como conectada en esta interfaz. Cuando no se encuentre ninguna red conocida, la configuración de la identificación de red creará una nueva conexión de red para identificar la red la próxima vez que usted se conecte a ella. De forma predeterminada, la conexión de red nueva utiliza el tipo de protección **Red pública**. Se abrirá el cuadro de diálogo **Se ha detectado una conexión de red nueva**, donde tendrá que elegir entre el tipo de protección **Red pública**, **Red doméstica o de oficina** o **Utilizar ajuste de Windows**. Si se conecta un adaptador de red a una red conocida que está marcada como **Red doméstica o de oficina**, las subredes locales del adaptador se agregan a la zona de confianza.

Tipo de protección de las nuevas redes: seleccione una de las siguientes opciones: **Utilizar ajuste de Windows**, **Preguntar al usuario** o **Marcar como pública** se utiliza de forma predeterminada para las redes nuevas.

Redes conocidas le permite configurar el nombre de la red, la identificación de la red, el tipo de protección, etc. Para entrar en Editor de redes conocidas, haga clic en **Modificar**.

NOTA
Cuando seleccione **Utilizar ajuste de Windows** no aparecerá un cuadro de diálogo y la red a la que se conecte se marcará automáticamente según la configuración de Windows. Esto permitirá el acceso a determinadas características (por ejemplo, el uso compartido de archivos y el escritorio remoto) desde las redes nuevas.

4.3.5.1 Editor de redes conocidas

Las redes conocidas se pueden configurar manualmente en **Configuración avanzada** > **Protección de la red** > **Cortafuegos** > **Redes conocidas** haciendo clic en la opción **Modificar**.

Columnas

Nombre: nombre de la red conocida.

Tipo de protección: muestra si la red se ha definido como **Red doméstica o de oficina**, **Pública** o **Utilizar ajuste de Windows**.

Perfiles de cortafuegos: seleccione un perfil en el menú desplegable **Mostrar reglas usadas en el perfil** para mostrar el filtro de reglas de los perfiles.

Perfil de actualización: le permite aplicar el perfil de actualización creado cuando está conectado a esta red.

Elementos de control

Agregar: crea una red conocida nueva.

Modificar: haga clic aquí para editar una red conocida.

Quitar: seleccione una red y haga clic en **Quitar** para quitarla de la lista de redes conocidas.

Superior/Arriba/Abajo/Inferior: le permite ajustar el nivel de prioridad de las redes conocidas (las redes se evalúan de arriba abajo).

Las parámetros de configuración de red están organizados en las fichas siguientes:

Red

Aquí puede definir el **Nombre de red** y seleccionar el **Tipo de protección** (Red pública, Red doméstica o de oficina o Utilizar ajuste de Windows) para la red. Utilice el menú desplegable **Perfiles de cortafuegos** para seleccionar un perfil para esta red. Si la red utiliza el tipo de protección **Red doméstica o de oficina**, se consideran de confianza todas las subredes conectadas directamente a la red. Por ejemplo, si un adaptador de red está conectado a esta red con la dirección IP 192.168.1.5 y la máscara de subred 255.255.255.0, la subred 192.168.1.0/24 se agrega a la zona de confianza de dicho adaptador. Si el adaptador tiene más direcciones o subredes, todas serán de confianza, independientemente de la configuración de **Identificación de red** de la red conocida.

Además, las direcciones agregadas en **Direcciones de confianza adicionales** se añaden siempre a la zona de confianza de los adaptadores conectados a esta red (independientemente del tipo de protección de la red).

Advertencia sobre cifrado WiFi débil: ESET Internet Security le informará cuando se conecte a una red inalámbrica no protegida o a una red con un nivel de protección débil.

Perfiles de cortafuegos: seleccione el perfil de cortafuegos que desee utilizar cuando se conecte a esta red.

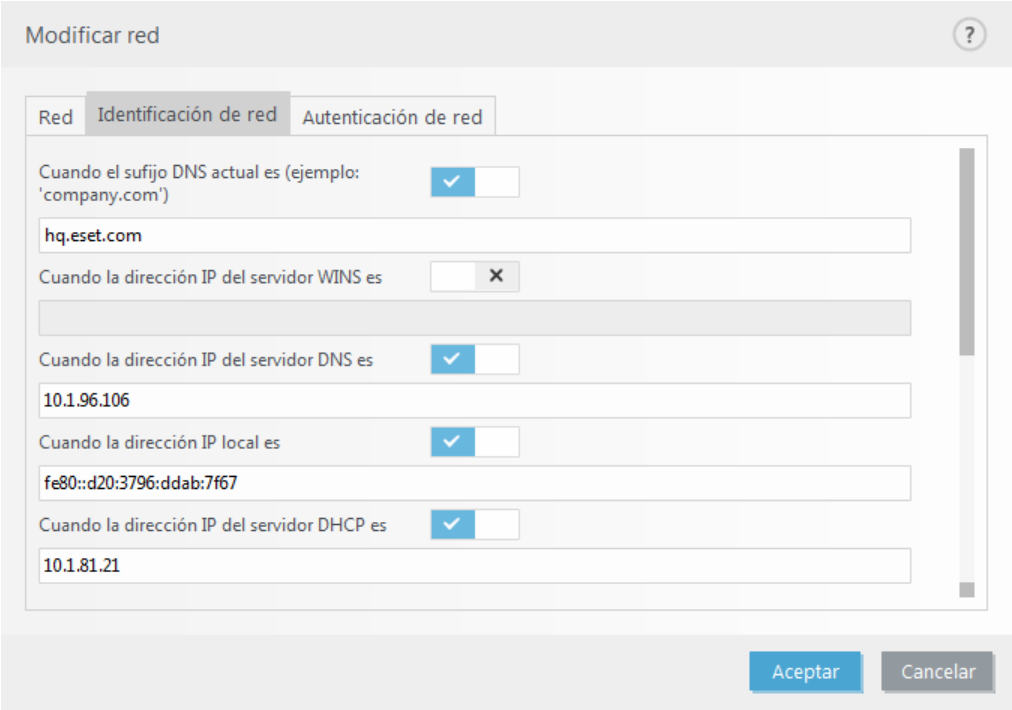
Perfil de actualización: seleccione el perfil de actualización que desee utilizar cuando se conecte a esta red.

Deben cumplirse las condiciones siguientes para que una red se marque como conectada en la lista de redes conectadas:

- Identificación de red: todos los parámetros especificados deben coincidir con los parámetros de la conexión activa.
- Autenticación de red: si se selecciona un servidor de autenticación, será necesaria una correcta autenticación con ESET Authentication Server.
- Restricciones de red (solo Windows XP): se deben respetar todas las restricciones globales seleccionadas.

Identificación de red

La identificación de red se realiza de acuerdo con los parámetros de un adaptador de red local. Todos los parámetros seleccionados se comparan con los parámetros reales de las conexiones de red activas. Se admiten direcciones IPv4 e IPv6.



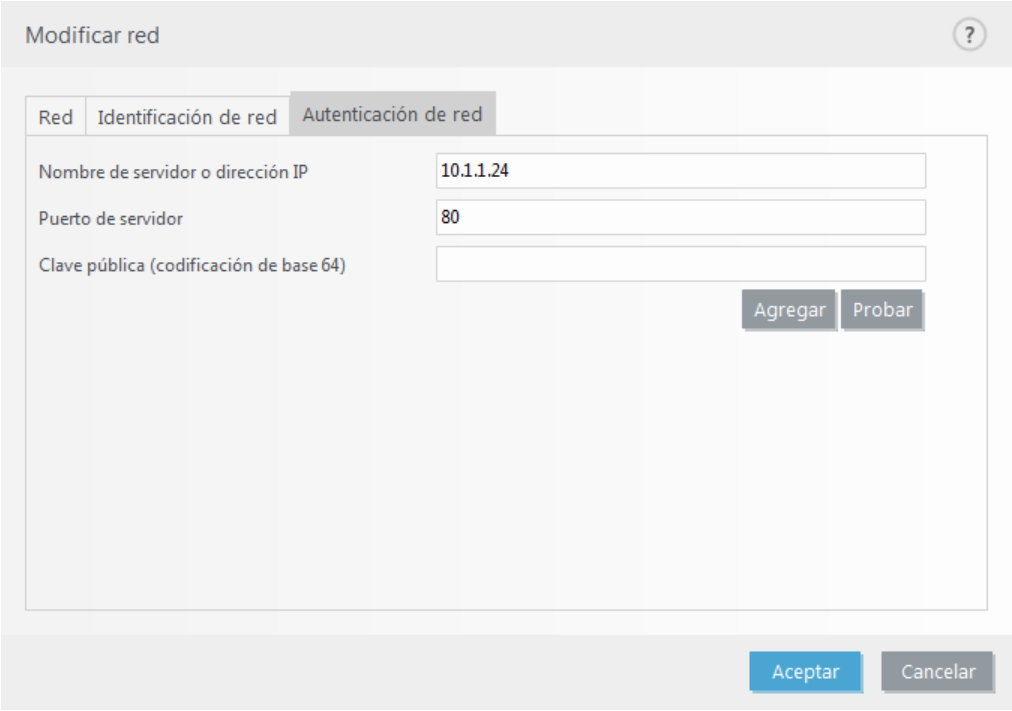
Autenticación de red

La autenticación de red busca un servidor específico de la red y utiliza el cifrado asimétrico (RSA) para autenticar al servidor. El nombre de la red que se va a autenticar debe coincidir con el nombre de la zona establecido en la configuración del servidor de autenticación. El nombre distingue entre mayúsculas y minúsculas. Especifique un nombre de servidor, un puerto de escucha del servidor y una clave pública correspondiente a la clave de servidor privado (consulte la sección Autenticación de red: configuración de servidor). El nombre del servidor se puede introducir como una dirección IP, un nombre de DNS o un nombre NetBios, y puede ir seguido de una ruta que especifique la ubicación de la clave en el servidor (por ejemplo, nombre_servidor_/directorio1/directorio2/autenticación). Si desea especificar otros servidores para utilizarlos como alternativa, añádalos al final de la ruta separados por punto y coma.

Descargue ESET Authentication Server.

La clave pública se puede importar con cualquiera de estos tipos de archivo:

- La clave pública cifrada PEM (.pem) se puede generar con ESET Authentication Server (consulte Autenticación de red: configuración de servidor).
- Clave pública cifrada.
- Certificado de clave pública (.crt).



Haga clic en **Probar** para probar su configuración. Si la autenticación es correcta, aparecerá *Autenticación del servidor correcta*. Si la autenticación no está configurada correctamente, aparecerá uno de los mensajes de error siguientes:

Error en la autenticación del servidor. Firma no válida o no concordante.
La firma del servidor no coincide con la clave pública introducida.

Error en la autenticación del servidor. El nombre de la red no coincide.
El nombre de la red configurada no se corresponde con el nombre de la zona del servidor de autenticación. Repase ambos nombres y asegúrese de que son idénticos.

Error en la autenticación del servidor. El servidor no respondió o la respuesta no es válida.
Si el servidor no se está ejecutando o no está accesible, el usuario no recibe ninguna respuesta. Puede recibir una respuesta no válida si hay otro servidor HTTP ejecutándose en la dirección especificada.

Clave pública introducida no válida.
Compruebe que el archivo de clave pública que ha introducido no esté dañado.

Restricciones de red (solo para Windows XP)

En los sistemas operativos modernos (Windows Vista y versiones más recientes), cada adaptador de red tiene su zona de confianza y perfil de cortafuegos activo propios. Lamentablemente, Windows XP no admite esta disposición, por lo que todos los adaptadores de red comparten siempre la misma zona de confianza y el mismo perfil de cortafuegos activo. Esto puede ser un riesgo potencial para la seguridad cuando la máquina se conecta a varias redes a la vez. En estos casos, se puede evaluar el tráfico de una red no fiable con la zona de confianza y el perfil de cortafuegos configurados para la otra red conectada. Utilice las restricciones siguientes para mitigar los riesgos de seguridad y evitar la aplicación global de una configuración de red cuando hay otra red conectada (que puede no ser fiable).

En Windows XP, la configuración de las redes conectadas (zona de confianza y perfil de cortafuegos) se aplican de forma global, a menos que esté activada una de las restricciones siguientes y no se cumpla:

a. Solo una conexión está activa
b. No se estableció ninguna conexión inalámbrica
c. No se estableció ninguna conexión inalámbrica no segura

4.3.5.2 Autenticación de red: configuración de servidor

Cualquier ordenador/servidor que esté conectado a la red en cuestión puede iniciar el proceso de autenticación. La aplicación ESET Authentication Server se debe instalar en un ordenador/servidor que siempre esté disponible para la autenticación cuando un cliente intente conectarse a la red. El archivo de instalación de la aplicación ESET Authentication Server se puede descargar del sitio web de ESET.

Una vez que haya instalado la aplicación ESET Authentication Server, aparecerá un cuadro de diálogo (puede acceder a la aplicación haciendo clic en **Inicio** > **Programas** > **ESET** > **ESET Authentication Server**).

Para configurar el servidor de autenticación, introduzca el nombre de la zona de autenticación, el puerto de escucha del servidor (el puerto predeterminado es 80) y la ubicación donde se almacena el par de claves pública y privada. A continuación, genere las claves pública y privada que se utilizarán en el proceso de autenticación. La clave privada permanecerá en el servidor y la clave pública hay que importarla en el cliente, en la sección Autenticación de zona, para configurar una zona en la configuración del cortafuegos.

Para obtener más información detallada, consulte este artículo de la base de conocimiento de ESET.

4.3.6 Registro

El cortafuegos de ESET Internet Security guarda todos los sucesos importantes en un archivo de registro que se puede ver directamente en el menú principal. Haga clic en **Herramientas** > **Archivos de registro** y, a continuación, seleccione **Protección de la red** en el menú desplegable **Registro**.

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

- Fecha y hora del suceso
- Nombre del suceso
- Origen
- Dirección de la red de destino
- Protocolo de comunicación de red
- Regla aplicada o nombre del gusano (si se identifica)
- Aplicación implicada
- Usuario

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

4.3.7 Establecimiento de una conexión: detección

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

El modo interactivo muestra una ventana informativa que notifica la detección de una nueva conexión de red, con información adicional acerca de dicha conexión. Tiene la opción de permitir la conexión o de rechazarla (bloquearla). Si permite la misma conexión en el cuadro de diálogo en repetidas ocasiones, es aconsejable que cree una regla nueva para la conexión. Para realizar esta tarea, seleccione **Crear regla y recordarla permanentemente** y guarde la acción como una regla nueva para el cortafuegos. Si el cortafuegos reconoce la misma conexión en el futuro, aplicará la regla existente sin necesidad de que intervenga el usuario.

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

- **Ubicación remota**: permitir únicamente conexiones a direcciones conocidas y de confianza.
- **Aplicación local**: no se aconseja permitir conexiones de aplicaciones y procesos desconocidos.
- **Número de puerto**: en circunstancias normales, se debe permitir la comunicación en puertos comunes (el número de puerto 80 para el tráfico de Internet, por ejemplo).

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

4.3.8 Solución de problemas con el cortafuegos personal de ESET

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

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

- Asistente de solución de problemas
- Registro y creación de reglas o excepciones del registro
- Creación de excepciones a partir de notificaciones del cortafuegos
- Registro PCAP avanzado
- Solución de problemas con el filtrado de protocolos

4.3.8.1 Asistente de solución de problemas

El asistente de solución de problemas supervisa silenciosamente todas las conexiones bloqueadas y le guía por el proceso de solución de problemas para corregir los problemas del cortafuegos con aplicaciones o dispositivos específicos. A continuación, el asistente le sugerirá un nuevo conjunto de reglas para que las aplique si está de acuerdo con ellas. El **asistente de solución de problemas** se encuentra en el menú principal, debajo de **Configuración** > **Protección de red**.

4.3.8.2 Registro y creación de reglas o excepciones del registro

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

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

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

4.3.8.2.1 Crear una regla desde un registro

La nueva versión de ESET Internet Security le permite crear una regla a partir del registro. En el menú principal, haga clic en **Herramientas** > **Más herramientas** > **Archivos de registro**. Seleccione **Cortafuegos** en el menú desplegable, haga clic con el botón derecho del ratón en la entrada del registro que desee y seleccione **No bloquear sucesos similares en el futuro** en el menú contextual. Se abrirá una ventana de notificación con la nueva regla.

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

- Defina el nivel mínimo de detalle al registrar en **Diagnóstico**, en **Configuración avanzada** (F5) > **Herramientas** > **Archivos de registro**.
- Active **Mostrar notificaciones al recibir ataques que aprovechen de fallos de seguridad** en **Configuración avanzada** (F5) > **Cortafuegos** > **Sistema de detección de intrusiones y opciones avanzadas** > **Detección de intrusiones**.

4.3.8.3 Creación de excepciones a partir de notificaciones del cortafuegos personal

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

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

4.3.8.4 Registro PCAP avanzado

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

1. Vaya a **Configuración avanzada** > **Herramientas** > **Diagnóstico** y active **Activar registro avanzado del cortafuegos**.
2. Intente repetir los pasos que provocaron el problema.
3. Desactive el registro PCAP avanzado.
4. El archivo de registro PCAP se encuentra en el mismo directorio donde se generan los volcados de memoria de diagnóstico:

- Microsoft Windows Vista o versiones posteriores

  C:\ProgramData\ESET\ESET Internet Security\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

4.3.8.5 Solución de problemas con el filtrado de protocolos

Si tiene problemas con su navegador o cliente de correo electrónico, lo primero que debe hacer es comprobar si la causa es el filtrado de protocolos. Para ello, desactive de forma temporal el filtrado de protocolos de la aplicación en la configuración avanzada (no se olvide de volver a activarlo cuando haya terminado, de modo que el navegador y el cliente de correo electrónico estén protegidos). Si el problema desaparece al desactivar el filtrado, consulte esta lista de problemas habituales y soluciones:

Problemas de comunicación segura o actualización

Si su aplicación le comunica que no se puede actualizar o el canal de comunicación no es seguro:

- Si tiene activado el filtrado del protocolo SSL, desactívelo temporalmente. Si esto soluciona el problema, siga utilizando el filtrado SSL y excluya la comunicación problemática en el proceso de actualización. establezca en interactivo el modo de filtrado del protocolo SSL. Vuelva a ejecutar la actualización. Debería aparecer un cuadro de diálogo para informarle sobre el tráfico de red cifrado. Asegúrese de que la aplicación coincide con la que tiene el problema y que el certificado procede del servidor desde el que se está actualizando. A continuación, seleccione la opción Recordar acción para este certificado y haga clic en Omitir. Si no se muestra ningún otro cuadro de diálogo, puede volver a poner el modo de filtrado en automático. El problema debería estar resuelto.
- Si la aplicación no es un navegador o un cliente de correo electrónico, puede excluirla totalmente del filtrado de protocolos (si hace esto para un navegador o cliente de correo electrónico, quedaría muy expuesto). Todas las aplicaciones cuya comunicación se haya filtrado previamente deberían aparecer en la lista que se le proporcionó al agregar una excepción, por lo que no tendría que añadirlas de forma manual.

Problemas de acceso a un dispositivo de la red

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

Problemas con un sitio web determinado

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

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

Cuando se activa el filtrado del protocolo SSL, ESET Internet Security crea un certificado a su almacén de certificados para asegurarse de que las aplicaciones instaladas confíen en su método de filtrado del protocolo SSL. Esta operación no se puede realizar en algunas aplicaciones mientras se ejecutan, como en Firefox y Opera. Asegúrese de que no se está ejecutando ninguna de ellas (la mejor manera de hacerlo es abrir el Administrador de tareas y comprobar que no haya ninguna entrada firefox.exe ni opera.exe en la ficha Procesos). A continuación, pulse Reintentar.

Error de emisor no fiable o firma no válida

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

4.4 Herramientas de seguridad

La configuración de Herramientas de seguridad permite ajustar los siguientes módulos:

- Protección de pagos y banca online
- Control parental
- Antirrobo

4.4.1 Control parental

En el módulo Control parental, puede definir la configuración del control parental, que proporciona a los padres herramientas automáticas que les ayudan a proteger a sus hijos y definir restricciones para dispositivos y servicios. El objetivo de esta función es impedir que los niños y adolescentes tengan acceso a páginas con contenido inapropiado o perjudicial.

El control parental le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo. Asimismo, los padres pueden prohibir el acceso a más de 40 categorías predefinidas y más de 140 subcategorías de sitios web.

Para activar el control parental para una cuenta de usuario específica, siga los pasos que se indican a continuación:

1. El control parental está desactivado de forma predeterminada en ESET Internet Security. Hay dos métodos para activar el control parental:
   - Haga clic en  en **Configuración** > **Herramientas de seguridad** > **Control parental** en la ventana principal del programa y cambie el estado del control parental a activado.
   - Pulse F5 para acceder al árbol **Configuración avanzada**, desplácese hasta **Web y correo electrónico** > **Control parental** y, a continuación, active el interruptor junto a **Integrar en el sistema**.
2. Haga clic en **Configuración** > **Herramientas de seguridad** > **Control parental** en la ventana principal del programa. Aunque aparezca **Activado** junto a **Control parental**, debe configurarlo para la cuenta deseada haciendo clic en **Proteger cuenta infantil** o **Cuenta paterna**. En la siguiente ventana, seleccione la fecha de nacimiento para determinar el nivel de acceso y las páginas web recomendadas según la edad. El control parental ahora estará activado en esa cuenta de 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 ficha Categorías. Para permitir o bloquear páginas web personalizadas que no concuerdan con ninguna categoría, haga clic en la ficha Excepciones.

Si hace clic en **Configuración** > **Herramientas de seguridad** > **Control parental** en la ventana principal del producto ESET Internet Security, observará que la ventana principal incluye:

Cuentas de usuario de Windows

Si ha creado un rol para una cuenta existente, se mostrará aquí. Haga clic en el control deslizante para que se muestre una marca de verificación verde junto a Control parental para la cuenta. En la cuenta activa, haga clic en Contenido y configuración bloqueados... para ver la lista de categorías de páginas web permitidas para esta cuenta, y las páginas web bloqueadas y permitidas.

IMPORTANTE
Para crear una cuenta nueva (por ejemplo, para un niño), utilice las siguientes instrucciones paso a paso para Windows 7 o Windows Vista:

1. Abra **Cuentas de usuario** haciendo clic en el botón **Inicio** (situado en el lado inferior izquierdo del escritorio), en **Panel de control** y, por último, en **Cuentas de usuario**.
2. Haga clic en **Administrar cuenta de usuario**. Si se le pide una confirmación o contraseña de administrador, escriba la contraseña y proporcione la confirmación.
3. Haga clic en **Crear una nueva cuenta**.
4. Escriba el nombre que desea para la cuenta de usuario, haga clic en un tipo de cuenta y, a continuación, haga clic en **Crear cuenta**.
5. Vuelva a abrir el panel del Control parental haciendo clic desde la ventana principal del programa de ESET Internet Security en **Configurar** > **herramientas de seguridad** > **Control parental**.

La parte inferior de una ventana contiene

Añadir una excepción para un sitio web... : puede permitirse o bloquearse el sitio web específico de acuerdo con sus preferencias para cada cuenta parental de forma independiente.

Mostrar registros: aquí puede ver un registro detallado de la actividad del Control parental (páginas bloqueadas, cuenta en la que se bloqueó una página, categoría, etc.). También puede filtrar este registro basándose en los criterios que elija usando el botón **Filtrado**.

Control parental

Tras desactivar el Control parental, se mostrará la ventana **¿Desea desactivar el control parental?**, donde puede definir el intervalo de tiempo durante el que estará desactivada la protección. A continuación, la opción cambia a **En pausa** o **Desactivado permanentemente**.

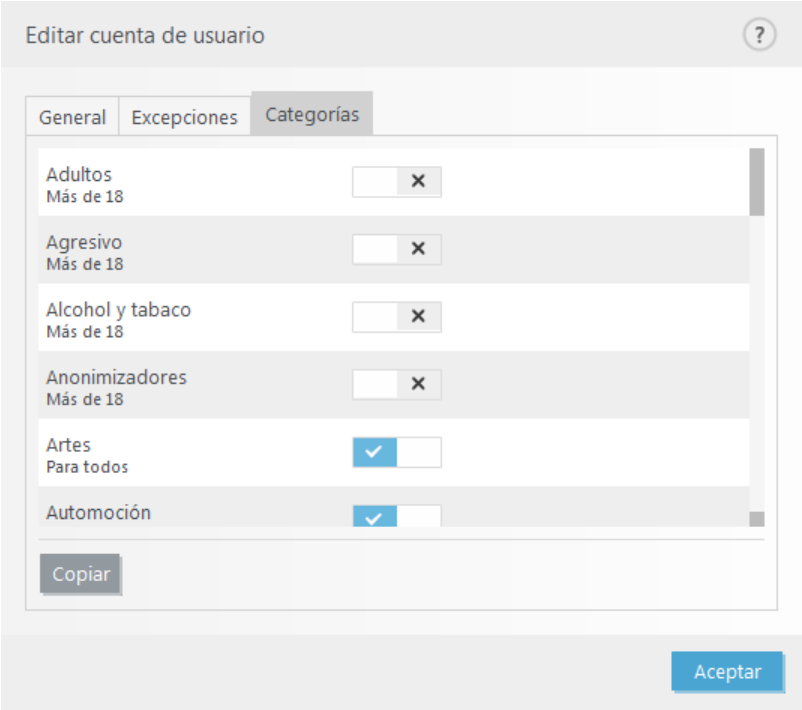
Es importante proteger la configuración de ESET Internet Security mediante una contraseña, que se puede definir en la sección Configuración de acceso. Si no se establece ninguna contraseña, se mostrará la siguiente alerta: **Proteja toda la configuración con una contraseña**. Las restricciones definidas en Control parental afectan únicamente a las cuentas de usuario estándar. Los administradores pueden ignorar las restricciones, de modo que estas no tendrán ningún efecto en su cuenta.

De forma predeterminada, la comunicación HTTPS (SSL) no se filtra. Por tanto, el Control parental no puede bloquear las páginas web que empiezan por *https://*. Para activar esta característica, active el ajuste **Activar el filtrado del protocolo SSL/TLS** en el árbol **Configuración avanzada** en **Web y correo electrónico** > **SSL/TLS**.

NOTA
El Control parental necesita que se activen las opciones Filtrado de contenido de protocolo de aplicación, Comprobación del protocolo HTTPS y Cortafuegosl para funcionar correctamente. Todas estas funcionalidades se activan de forma predeterminada.

4.4.1.1 Categorías

Active el conmutador situado junto a una categoría para indicar que desea permitirla. Si lo mantiene desactivado, la categoría no se permitirá para dicha cuenta.

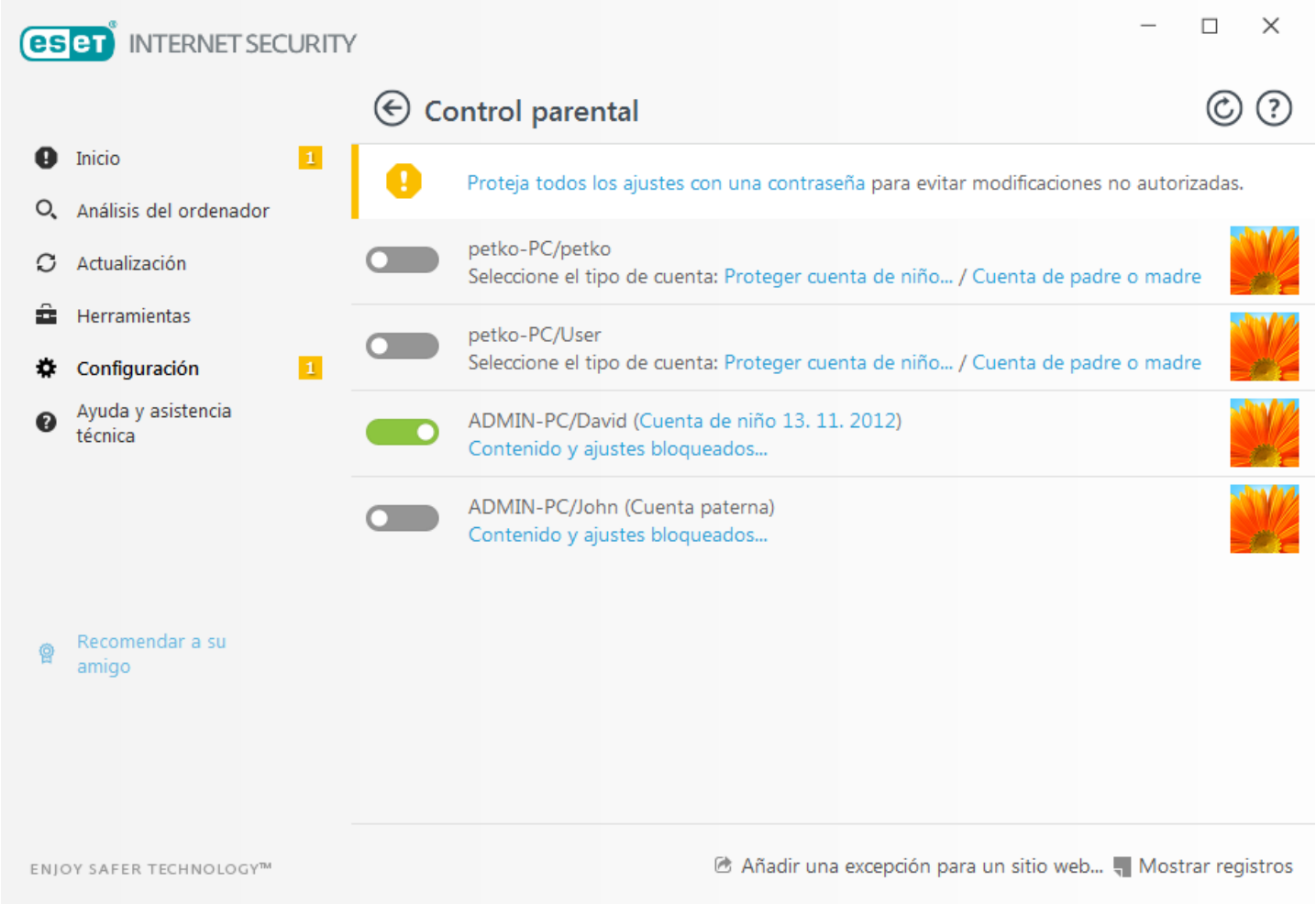


Estos son algunos ejemplos de categorías (grupos) que pueden no resultar muy familiares a los usuarios:

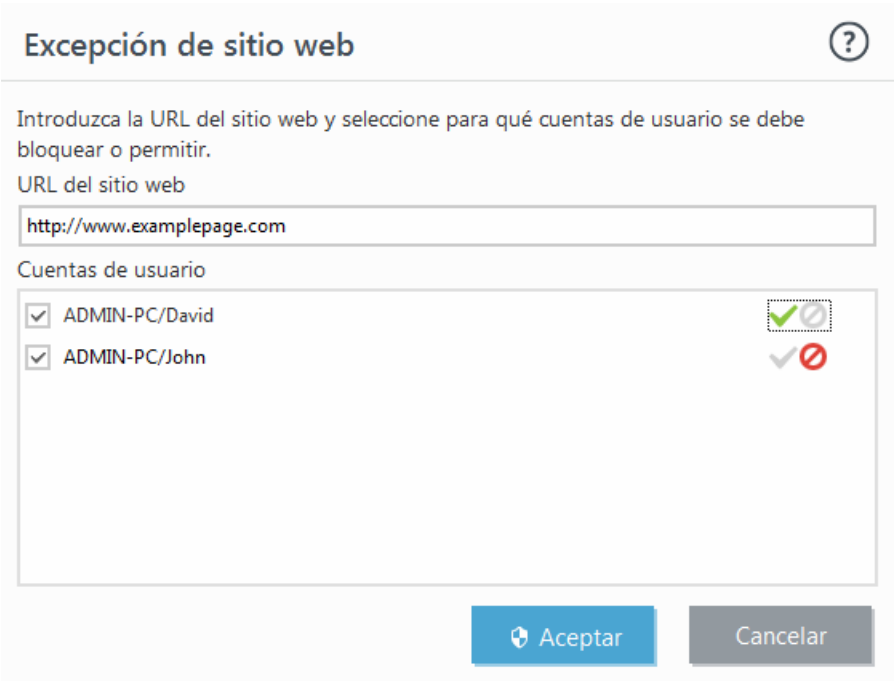
- **Varios**: suelen ser direcciones IP privadas (locales) como intranets, 127.0.0.0/8, 192.168.0.0/16, etc. Cuando obtiene un código de error 403 o 404, el sitio web también coincidirá con esta categoría.
- **Sin resolver**: esta categoría incluye páginas web que no se resuelven debido a un error al conectarse al motor de base de datos del Control parental.
- **No clasificar**: páginas web desconocidas que todavía no se encuentran en la base de datos del Control parental.
- **Dinámico**: páginas web que redirigen a otras páginas de otros sitios web.

4.4.1.2 Excepciones de sitio web

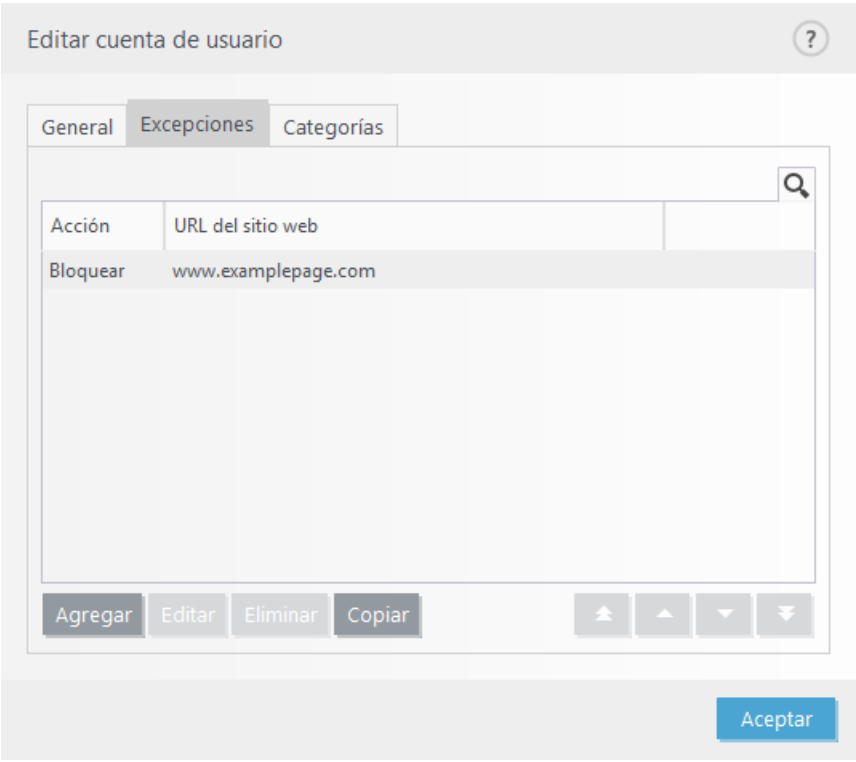
Para agregar una excepción para un sitio web, haga clic en **Configuración** > **Herramientas de seguridad** > **Control parental** y, a continuación, haga clic en **Añadir una excepción para un sitio web**.



Introduzca una URL en el campo **URL del sitio web**, seleccione ✔ (permitida) o ⊘ (bloqueada) para cada cuenta de usuario y, a continuación, haga clic en **Aceptar** para añadirla a la lista.



Para eliminar una dirección URL de la lista, haga clic en **Configuración** > **Herramientas de seguridad** > **Control parental**, haga clic en **Contenido y configuración bloqueados** en la cuenta de usuario que desee, haga clic en la ficha **Excepción**, seleccione la excepción y haga clic en **Quitar**.



En las listas de direcciones URL, no pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). Por ejemplo, las direcciones de páginas web con varios TLD se deben escribir manualmente *(ejemplopágina.com*, *ejemplopágina.sk*, etc.). Cuando agrega un dominio a la lista, todo el contenido ubicado en este dominio y todos los subdominios (por ejemplo, *sub.ejemplopágina.com*) se bloqueará o permitirá en función de la acción basada en una URL elegida.

NOTA
La acción de bloquear o permitir una página web específica puede ser más precisa que su aplicación a una categoría de páginas web. Sea precavido a la hora de cambiar esta configuración y agregar una categoría o página web a la lista.

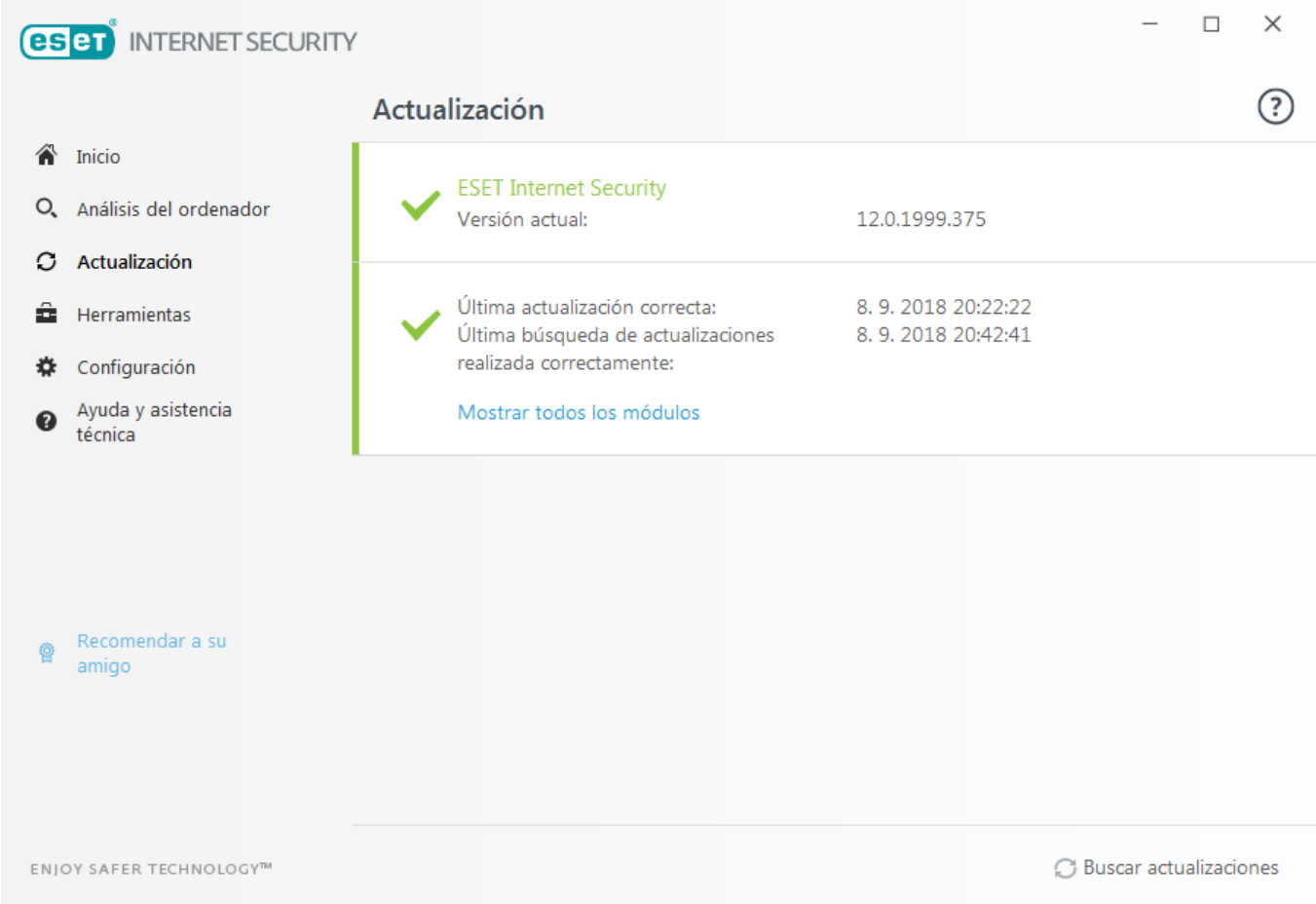
4.5 Actualización del programa

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

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

Además de las actualizaciones automáticas, puede hacer clic en **Buscar actualizaciones** para activar una actualización manual. La actualización periódica de los módulos y componentes del programa es un aspecto importante a la hora de mantener una protección completa contra el código malicioso. Preste especial atención a su configuración y funcionamiento. Debe activar su producto con su clave de licencia para recibir actualizaciones. Si no lo hizo durante la instalación, puede introducir su clave de licencia para activar su producto cuando actualice para acceder a los servidores de actualización de ESET.

NOTA
ESET le facilita la clave de licencia en un correo electrónico tras la compra de ESET Internet Security.



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

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

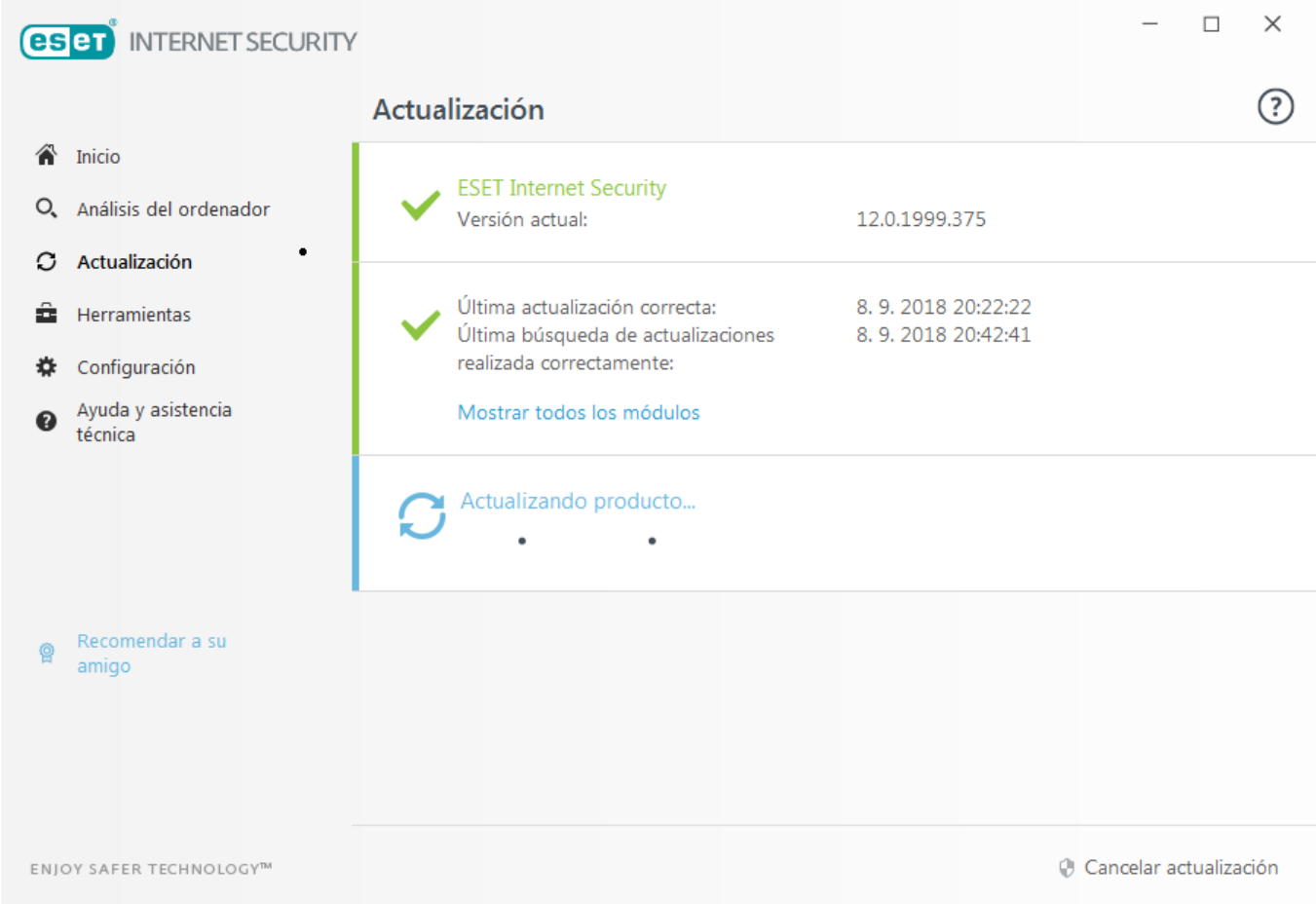
Última búsqueda de actualizaciones correcta: muestra la fecha de la última búsqueda de actualizaciones correcta.

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

Haga clic en **Buscar actualizaciones** para detectar la versión disponible más reciente de ESET Internet Security.

Proceso de actualización

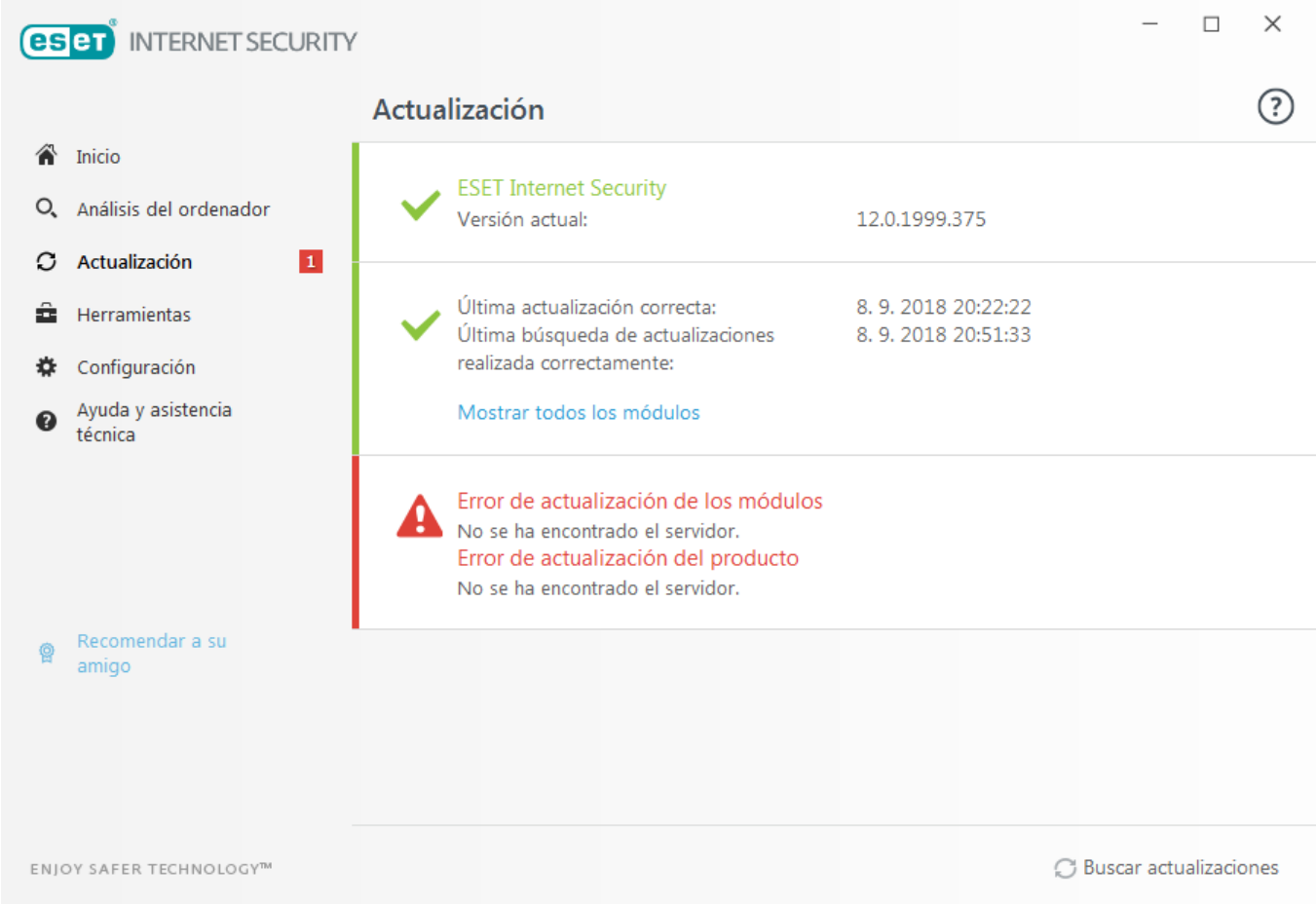
La descarga se inicia al hacer clic en **Buscar actualizaciones**. Se muestran una barra de progreso de la descarga y el tiempo que falta para que finalice la descarga. Para interrumpir la actualización, haga clic en **Cancelar actualización**.



IMPORTANTE
En circunstancias normales verá la marca de verificación verde en la ventana **Actualización**, lo que indica que el programa está actualizado. En caso contrario, el programa no estará actualizado y es más vulnerable a la infección. Actualice los módulos a la mayor brevedad posible.

Si recibe un mensaje indicándole que no se ha podido realizar la actualización, puede deberse a los siguientes problemas:

1. **Licencia no válida**: la clave de licencia se ha introducido en la configuración de actualización de forma incorrecta. Recomendamos que compruebe sus datos de autenticación. La ventana Configuración avanzada (haga clic en **Configuración** en el menú principal y, a continuación, en **Configuración avanzada**, o pulse **F5** en el teclado) ofrece más opciones de actualización. Haga clic en **Ayuda y soporte** > **Cambiar licencia** en el menú principal para introducir una nueva clave de licencia.
2. **Se ha producido un error al descargar los archivos de actualización**: puede deberse a una configuración de la conexión a Internet incorrecta. Es recomendable que compruebe la conectividad a Internet (por ejemplo, abriendo un sitio web en el navegador web). Si el sitio web no se abre, es probable que no se haya establecido ninguna conexión a Internet o que haya problemas de conectividad con el ordenador. Consulte a su proveedor de servicios de Internet (ISP) si no tiene una conexión activa a Internet.



IMPORTANTE
Le recomendamos que reinicie el ordenador tras una actualización correcta para asegurarse de que todos los módulos del programa se hayan actualizado correctamente.

NOTA
Consulte este artículo de la Base de conocimiento de ESET para obtener más información.

4.5.1 Configuración de actualización

Las opciones de configuración de actualizaciones están disponibles en el árbol de **Configuración avanzada** (F5), en **Actualización** > **Básico**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización utilizados y sus datos de autenticación.

Básico

El perfil de actualización que se está utilizando (a menos que se establezca uno concreto en **Configuración avanzada** > **Cortafuegos** > **Redes conocidas**) se muestra en el menú desplegable **Seleccionar perfil de actualización predeterminado**.

Cambio automático de perfil: le permite cambiar el perfil de una red concreta.

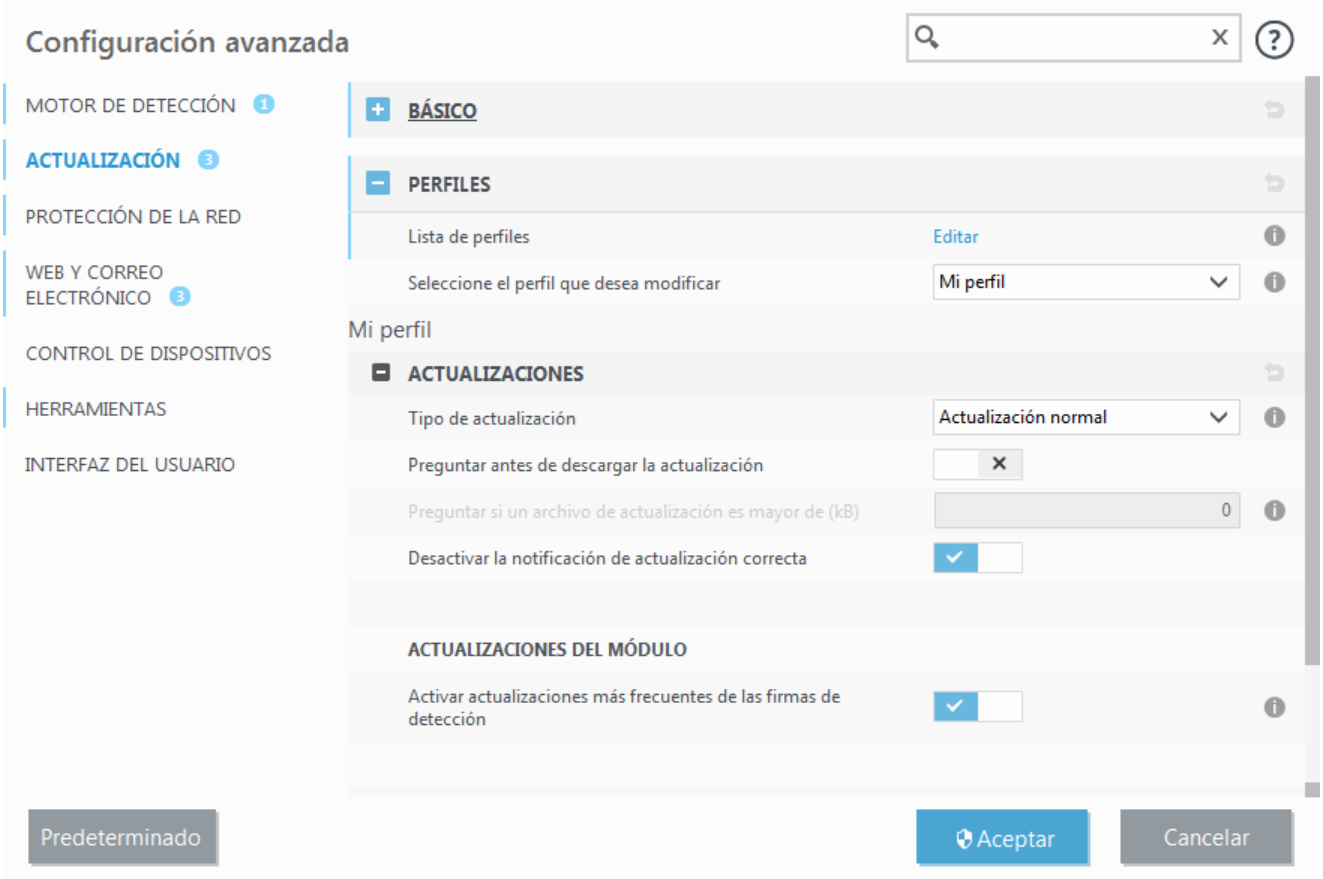
Si está experimentando problemas a la hora de descargar actualizaciones del motor de detección, haga clic en **Borrar** para eliminar los archivos de actualización temporales/la caché.

Reversión de módulos

Si sospecha que una nueva actualización de la base de firmas de virus o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

ESET Internet Security registra instantáneas del motor de detección y los módulos del programa para usarlas con la función de *reversión*. Para crear instantáneas de la base de firmas de virus, deje activado el conmutador **Crear instantáneas de archivos de actualización**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas de la base de firmas de virus anteriores que se guardan.

Si hace clic en **Revertir** (**Configuración avanzada** [F5] > **Actualización** > **Básico**), deberá seleccionar un intervalo de tiempo en el menú desplegable que represente el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.



Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente todos los parámetros de actualización. Si utiliza un cortafuegos, asegúrese de que su programa de ESET goza de permiso para comunicarse con Internet (por ejemplo, comunicación HTTP).

Perfiles

Se pueden crear perfiles de actualización para diferentes tareas y configuraciones de actualización. Estos perfiles son especialmente útiles para los usuarios móviles, que necesitan un perfil alternativo para las propiedades de conexión a Internet que cambian periódicamente.

El menú desplegable **Seleccione el perfil que desea modificar** muestra el perfil seleccionado actualmente y está definido como **Mi perfil** de forma predeterminada. Para crear un perfil nuevo, haga clic en **Modificar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**.

Actualizaciones

De forma predeterminada, el menú **Tipo de actualización** está definido en **Actualización normal** para garantizar que todos los archivos de actualización se descarguen automáticamente del servidor de ESET cuando la carga de red sea menor. Las actualizaciones de prueba (opción **Actualización de prueba**) son actualizaciones que han superado rigurosas pruebas internas y estarán pronto disponibles. Puede beneficiarse de activar las actualizaciones de prueba mediante el acceso a los métodos y soluciones de detección más recientes. No obstante, la actualización de prueba no siempre es estable, por lo que NO debe utilizarse en servidores de producción y estaciones de trabajo que requieran un elevado nivel de disponibilidad y estabilidad.

Preguntar antes de descargar actualizaciones: el programa mostrará una notificación en la que podrá confirmar o rechazar las descargas de archivos de actualización.

Preguntar si un archivo de actualización es mayor de (kB): el programa mostrará una notificación si el tamaño del archivo de actualización es mayor que el valor especificado.

Desactivar la notificación de actualización correcta: desactiva la notificación de la bandeja del sistema en la esquina inferior derecha de la pantalla. Selecciónela si está ejecutando un juego o una aplicación a pantalla completa. Tenga en cuenta que el modo de juego desactiva todas las notificaciones.

Actualizaciones del módulo

Activar actualizaciones más frecuentes de firmas de detección: las firmas de detección se actualizarán en intervalos más cortos. Desactivar este ajuste puede afectar negativamente a la velocidad de detección.

Actualización de componentes del programa

Actualización de la aplicación: si es necesario reinstalar, se mostrará un cuadro de diálogo de confirmación.

4.5.1.1 Configuración avanzada de actualizaciones

Entre las opciones avanzadas de la configuración de actualizaciones se incluyen **Tipo de actualización** y **Proxy HTTP**.

4.5.1.1.1 Tipo de actualización

La ficha **Modo de actualización** contiene las opciones relacionadas con las actualizaciones del programa periódicas. Esta configuración le permite predefinir el comportamiento del programa cuando hay disponibles una nueva versión del motor de detección o actualizaciones de los componentes del programa.

Entre las actualizaciones de los componentes del programa se incluyen nuevas funciones o realizan cambios en funciones de versiones anteriores, y se incluyen como parte de las actualizaciones periódicas (motor de detección). Después de instalar una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador.

Están disponibles los siguientes ajustes:

Actualización de la aplicación: cuando esta opción está activada, la actualización de cada componente del programa se realizará automáticamente y silenciosamente sin que se actualice el producto completo.

Activar actualización manual de componentes del programa: está desactivado de forma predeterminada. Cuando esta opción esté activado y tenga a su disposición una versión más reciente de ESET Internet Security, podrá buscar actualizaciones en el panel **Actualización** e **instalar** la versión más actualizada.

Preguntar antes de descargar la actualización: cuando esta opción esté activa, se mostrará una notificación y se le pedirá que confirme la instalación de las actualizaciones disponibles antes de instalarlas.

Preguntar si un archivo de actualización es mayor de (kB): si el archivo de actualización presenta un tamaño superior al especificado aquí, se mostrará una notificación y se le pedirá que confirme la instalación de las posibles actualizaciones disponibles antes de su instalación.

4.5.1.1.2 Opciones de conexión

Para acceder a las opciones de configuración del servidor proxy de un perfil de actualización concreto, haga clic en **Actualización** en el árbol **Configuración avanzada** (F5) y, a continuación, haga clic en **Perfiles** > **Actualizaciones** > **Opciones de conexión**. Haga clic en el menú desplegable **Modo proxy** y seleccione una de estas tres opciones:

- No usar servidor Proxy
- Conexión a través de un servidor Proxy específico
- Utilizar la configuración predeterminada

Seleccione **Usar la configuración global del servidor proxy** para utilizar las opciones de configuración del servidor proxy ya especificadas en la sección **Herramientas** > **Servidor proxy** del árbol de configuración avanzada.

Seleccione **No usar servidor Proxy** para especificar que no se utilice ningún servidor Proxy para actualizar ESET Internet Security.

La opción **Conexión a través de un servidor proxy** debe seleccionarse si:

- Se utiliza un servidor proxy distinto del definido en **Herramientas** > **Servidor proxy** para actualizar ESET Internet Security. En esta configuración, la información del nuevo proxy se debe especificar en **Servidor proxy**: dirección, **Puerto** de comunicación (3128 de forma predeterminada), **Nombre de usuario** y **Contraseña** del servidor proxy, en caso de ser necesarios.
- La configuración del servidor proxy no se ha definido globalmente, pero ESET Internet Security se conecta a un servidor proxy para las actualizaciones.
- El ordenador se conecta a Internet mediante un servidor Proxy. La configuración se obtiene de Internet Explorer durante la instalación del programa; no obstante, si se modifica (por ejemplo, al cambiar de proveedor de Internet), asegúrese de que la configuración del servidor proxy HTTP que aparece en esta ventana es la correcta. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

La configuración predeterminada del servidor Proxy es **Utilizar la configuración predeterminada**.

Usar conexión directa si el proxy no está disponible: si no puede accederse al proxy durante la actualización, se omitirá.

NOTA
Los campos **Nombre de usuario** y **Contraseña** de esta sección son específicos del servidor proxy. Rellene estos campos únicamente si es necesario introducir un nombre de usuario y una contraseña para acceder al servidor proxy. En estos campos no debe introducir su contraseña y nombre de usuario de ESET Internet Security, únicamente debe proporcionar estos datos si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor proxy.

4.5.2 Reversión de actualización

Si sospecha que una nueva actualización del motor de detección o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

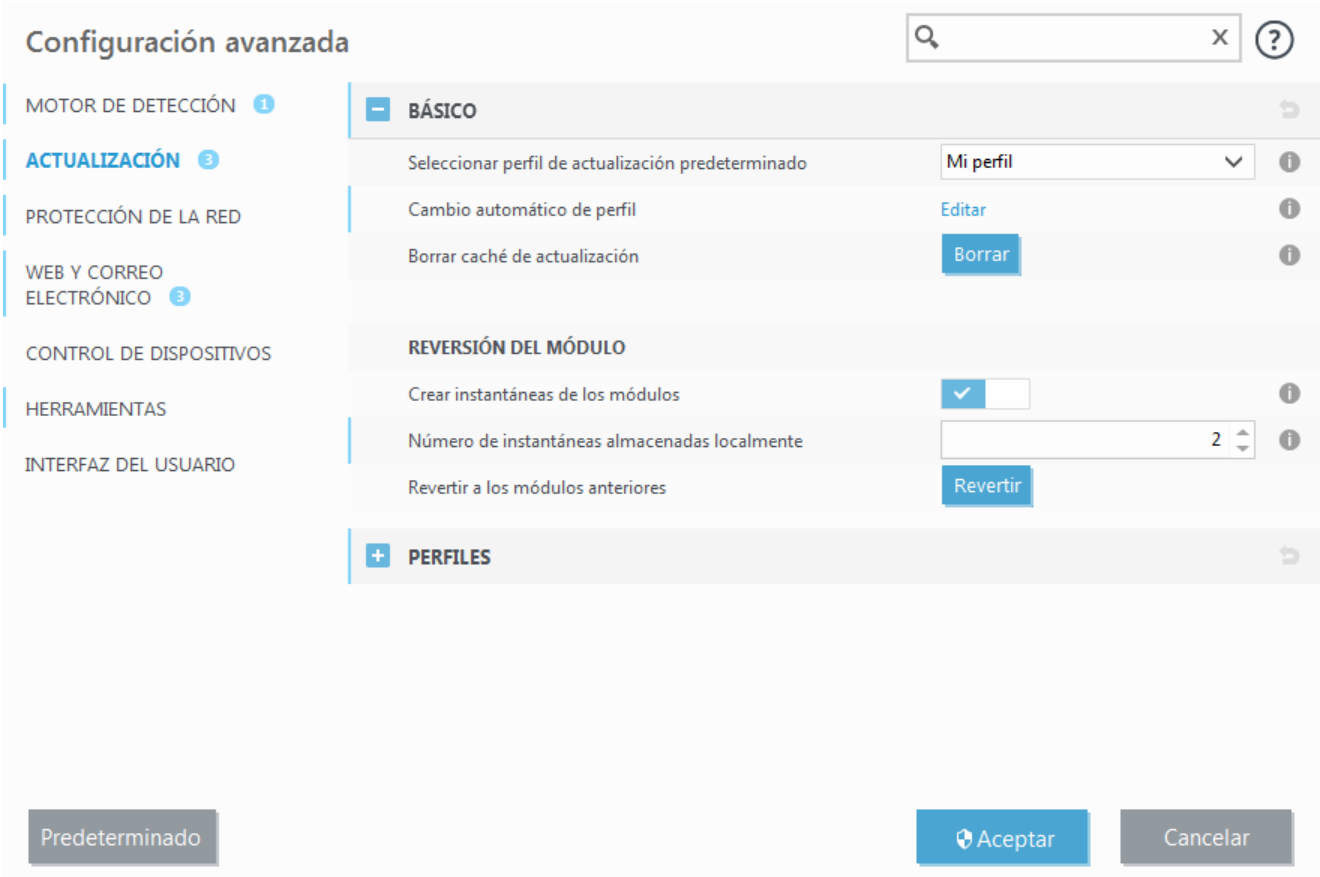
ESET Internet Security registra instantáneas del motor de detección y los módulos del programa para usarlas con la función de *reversión*. Para crear instantáneas de del motor de detección, deje marcada la casilla de verificación **Crear instantáneas de archivos de actualización**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas de la base de firmas de virus anteriores que se guardan.

Si hace clic en **Revertir** (**Configuración avanzada** [F5] > **Actualización** > **Básico**), deberá seleccionar un intervalo de tiempo en el menú desplegable **Duración** que represente el periodo de tiempo durante el que estarán interrumpidas las actualizaciones del motor de detección y del módulo del programa.

Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, no recomendamos que se seleccione esta opción.

Si se lleva a cabo una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. No se permitirán actualizaciones para el intervalo de tiempo seleccionado en el menú desplegable **Suspender actualizaciones**. La

versión del motor de detección se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del ordenador local.



NOTA

Supongamos que el número 6871 es la versión más reciente del motor de detección. Se almacenan 6870 y 6868 como instantáneas del motor de detección. Observe que 6869 no está disponible porque, por ejemplo, el ordenador estuvo apagado y había disponible una actualización más reciente antes de que se descargara 6869. Si se ha definido 2 en el campo **Número de instantáneas almacenadas localmente** y hace clic en **Revertir**, el motor de detección (incluidos los módulos del programa) se restaurará a la versión número 6868. Este proceso puede tardar un tiempo. Compruebe si la versión del motor de detección se ha degradado en la ventana principal del programa de ESET Internet Security en la sección Actualización.

4.5.3 Cómo crear tareas de actualización

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

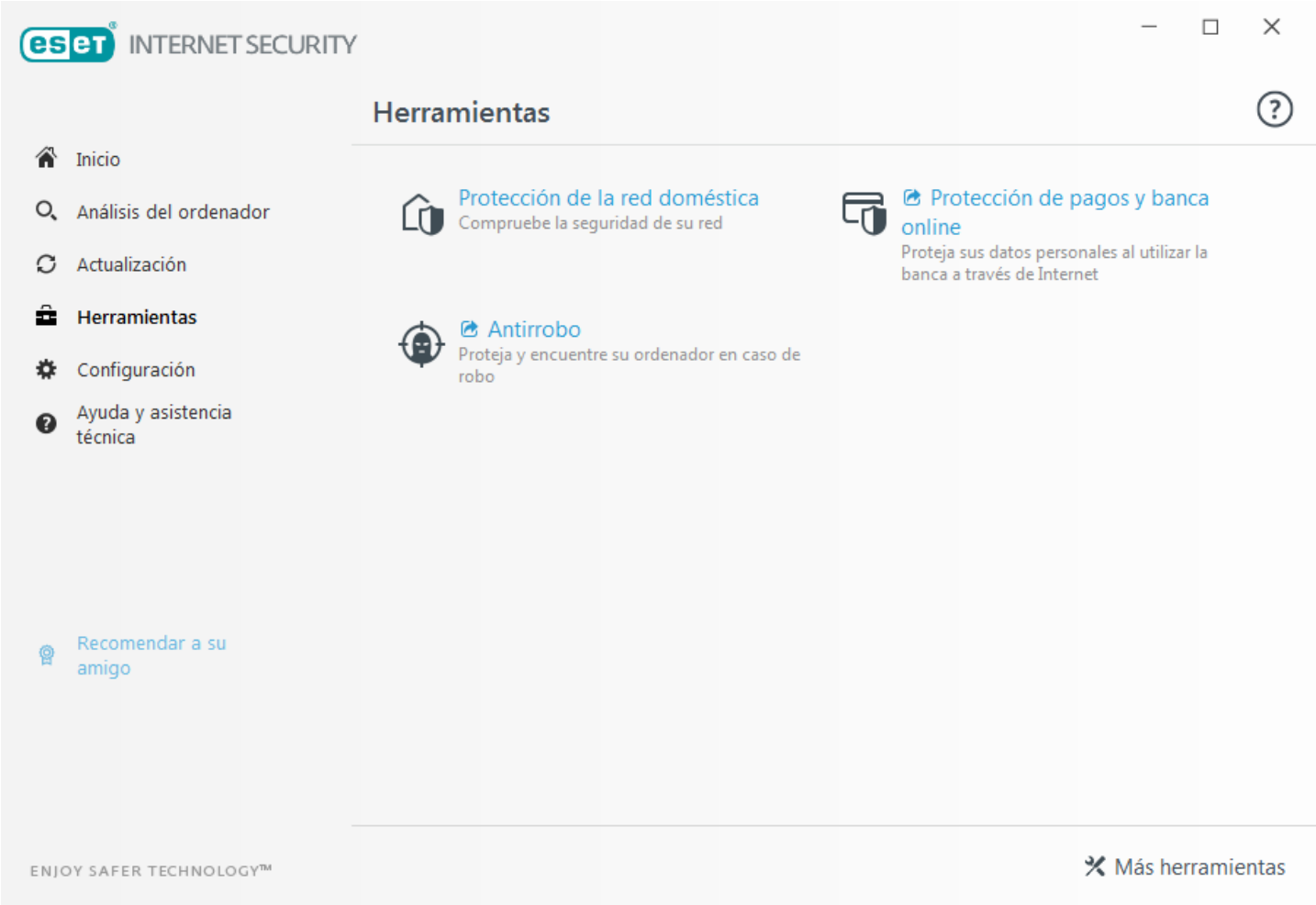
Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Planificador de tareas**. Las siguientes tareas están activadas de forma predeterminada en ESET Internet Security:

- **Actualización automática de rutina**
- **Actualización automática tras conexión de acceso telefónico**
- **Actualización automática después del registro del usuario**

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

4.6 Herramientas

El menú **Herramientas** incluye módulos que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.



Protección de la red doméstica: reduzca el riesgo de que surjan problemas de seguridad al conectarse a una red. Si desea obtener más información, haga clic aquí.

Protección de pago y banca: ESET Internet Security protege los números de tarjetas de crédito y otros datos personales confidenciales mientras utiliza sitios web de banca o pago a través de Internet. Se abrirá un navegador protegido para ofrecer transacciones de banca más seguras. Consulte este artículo de la Base de conocimiento de ESET para obtener más información.

Haga clic en Más herramientas para mostrar otras herramientas con las que proteger el ordenador.

4.6.1 Protección de la red doméstica

Protección de la red doméstica puede ayudar a identificar vulnerabilidades en su red doméstica, como puertos abiertos o una contraseña débil del router. También le ofrece una lista de fácil acceso de los dispositivos conectados clasificados por tipo (p. ej., impresoras, routers, dispositivos móviles, etc.) para mostrarle qué dispositivos hay conectados a la red doméstica. No reconfigura el router por usted. Debe hacer los cambios usted utilizando la interfaz especializada del router. Los routers domésticos pueden ser altamente vulnerables al malware que se utiliza para lanzar ataques de denegación de servicio distribuidos (DDoS). Si el usuario no ha cambiado la contraseña predeterminada del router, los hackers podrán adivinarla fácilmente y, a continuación, iniciar sesión en el router y modificar su configuración o poner su red en peligro.

ADVERTENCIA

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

Todos los dispositivos conectados a la red se mostrarán en vista de sonar. Coloque el cursor sobre el icono de un dispositivo para ver información básica, como el nombre de la red y la fecha de la última conexión. Haga clic en el icono del dispositivo para ver información detallada del mismo.

Si desea mostrar información de todos los dispositivos conectados en la vista de lista, haga clic en  . La vista de lista contiene los mismos datos que la vista de sonar, pero en formato de lista. Con el menú desplegable puede filtrar los dispositivos según los siguientes criterios:

- Solo dispositivos conectados a la red actual
- Dispositivos sin clasificar
- Dispositivos conectados a todas las redes

El módulo Protección de la red doméstica muestra dos tipos de notificaciones:

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

NOTA
Ambos tipos de notificación le informan de que un dispositivo no autorizado está intentando conectarse a la red.

NOTA
Los dispositivos recientemente conectados se muestran más cerca del router, para que pueda detectarlos fácilmente.

Protección de la red doméstica le ayuda a identificar las vulnerabilidades de un router y aumenta el nivel de protección cuando se establece conexión con una red externa.

Haga clic en **Analizar la red** para realizar manualmente un análisis de la red a la que está conectado.

Tiene las siguientes opciones de análisis:

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

ADVERTENCIA
Realice análisis de red solo en su propia red doméstica. Si lo hace en las redes de otras personas, debe tener en cuenta los posibles riesgos.

Una vez finalizado el análisis se mostrará una notificación que incluye un enlace a información básica sobre el dispositivo, y también puede hacer doble clic en el dispositivo sospechoso en una vista de lista o sonar. Haga clic en **Solucionar problemas** para ver las comunicaciones recientemente bloqueadas.

NOTA
Para obtener más información sobre la solución de problemas con el cortafuegos, haga clic aquí.

4.6.1.1 Dispositivo de red

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

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

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

Eliminar dispositivo: puede quitar el dispositivo conectado anteriormente a su red si ya no está presente.

4.6.2 Protección de cámara web

Protección de cámara web le permite ver los procesos y las aplicaciones que acceden a la cámara web del ordenador. Si una aplicación no deseada intenta acceder a la cámara, se mostrará una ventana de notificación. Puede **permitir** o **bloquear** que los procesos o aplicaciones no deseados accedan a la cámara.

4.6.3 Herramientas en ESET Internet Security

El menú **Más herramientas** incluye módulos que ayudan a simplificar la administración del programa y ofrece opciones adicionales para usuarios avanzados.

Este menú incluye las herramientas siguientes:

 Archivos de registro

 Informe de seguridad

 Observar actividad

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

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

 ESET SysInspector

 ESET SysRescue Live: redirige a la página de ESET SysRescue Live, desde la que puede descargar la imagen de ESET SysRescue Live o Live CD/USB Creator para sistemas operativos Microsoft Windows.

 Planificador de tareas

 Desinfección del sistema: le ayuda a restaurar el ordenador a un estado utilizable tras desinfectar la amenaza.

 Enviar muestra para su análisis: le permite enviar un archivo sospechoso para que lo analicen en el laboratorio de investigación de ESET. La ventana de diálogo mostrada al hacer clic en esta opción se describe en esta sección.

 Cuarentena

NOTA
Puede que ESET SysRescue no esté disponible para Windows 8 en versiones más antiguas de productos de ESET. En tal caso, se recomienda que actualice su producto o que cree un disco de ESET SysRescue en otra versión de Microsoft Windows.

4.6.3.1 Archivos de registro

Los archivos de registro contienen información relacionada con los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. El registro constituye una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según el nivel de detalle de los registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno de ESET Internet Security, donde también se pueden archivar registros.

Se puede acceder a los archivos de registro desde la ventana principal del programa haciendo clic en **Herramientas** > **Más herramientas** > **Archivos de registro**. Seleccione el tipo de registro que desee en el menú desplegable **Registro**. Están disponibles los siguientes registros:

- **Amenazas detectadas**: el registro de amenazas contiene información detallada acerca de las amenazas detectadas por ESET Internet Security. La información del registro incluye el momento de la detección, el nombre de la amenaza, la ubicación, la acción adoptada y el nombre del usuario registrado en el momento en que se detectó la amenaza. Haga doble clic en la entrada del registro para ver los detalles en una ventana independiente.
- **Sucesos**: todas las acciones importantes realizadas por ESET Internet Security se registran en el registro de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para que los administradores del sistema y los usuarios puedan solucionar problemas. Con frecuencia, la información aquí disponible puede ayudarle a encontrar una solución para un problema del programa.
- **Análisis del ordenador**: en esta ventana se muestran los resultados de todos los análisis manuales o programados completados. Cada línea se corresponde con un control informático individual. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.

- **HIPS**: contiene registros de reglas específicas de HIPS que se marcaron para su registro. El protocolo muestra la aplicación que activó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla.
- **Protección de la red**: el registro de protección de la red muestra todos los ataques remotos detectados por el cortafuegos. Aquí encontrará información sobre todos los ataques a su ordenador. En la columna *Suceso* se incluyen los ataques detectados. En la columna *Origen* se proporciona más información sobre el atacante. En la columna *Protocolo* se indica el protocolo de comunicación que se utilizó para el ataque. El análisis del registro de protección de la red puede ayudarle a detectar a tiempo amenazas del sistema, para así poder evitar el acceso no autorizado al sistema.
- **Sitios web filtrados**: Esta lista es útil si desea ver una lista de sitios web que la Protección del tráfico de Internet o el Control parental ha bloqueado. Cada registro incluye la hora, la dirección URL, el usuario y la aplicación que creó una conexión con un sitio web en cuestión.
- **Protección Antispam**: contiene los registros relacionados con los mensajes de correo electrónico que se marcaron como correo no deseado.
- **Control parental**: muestra las páginas web bloqueadas o permitidas por Control parental. Las columnas *Tipo de coincidencia* y *Valores de coincidencia* informan de cómo se aplicaron las reglas de filtrado.
- **Control de dispositivos**: contiene registros de los dispositivos o medios extraíbles conectados al ordenador. Solo los dispositivos con reglas de control de dispositivos correspondientes se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, no se creará una entrada de registro para un dispositivo conectado. Puede ver también detalles como el tipo de dispositivo, número de serie, nombre del fabricante y tamaño del medio (si está disponible).
- **Protección de cámara web**: contiene registros sobre las aplicaciones bloqueadas mediante la protección de la cámara web.

Seleccione el contenido de un registro y pulse **Ctrl + C** para copiarlo en el portapapeles. Mantenga pulsadas las teclas **Ctrl** y **Mayús** para seleccionar varias entradas.

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

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

- **Mostrar**: muestra información detallada sobre el registro seleccionado en una ventana nueva.
- **Filtrar los mismos registros**: tras activar este filtro solo verá registros del mismo tipo (diagnósticos, advertencias, etc.).
- **Filtrar/Buscar**: después de hacer clic en esta opción, en la ventana Buscar en el registro podrá definir los criterios de filtrado para entradas de registro específicas.
- **Activar filtro**: activa la configuración del filtro.
- **Desactivar filtro**: borra todos los ajustes del filtro (tal como se describe arriba).
- **Copiar/Copiar todo**: copia información sobre todos los registros de la ventana.
- **Eliminar/Eliminar todo**: elimina los registros seleccionados o todos los registros mostrados. Se necesitan privilegios de administrador para poder realizar esta acción.
- **Exportar...**: exporta información acerca de los registros en formato XML.
- **Exportar todo...**: exporta información acerca de todos los registros en formato XML.
- **Desplazar registro**: deje esta opción activada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana **Archivos de registro**.

4.6.3.1.1 Registro de configuración

La configuración de registros de ESET Internet Security está disponible en la ventana principal del programa. Haga clic en **Configuración** > **Entrar a la configuración avanzada** > **Herramientas** > **Archivos de registro**. La sección de registros se utiliza para definir cómo se gestionarán los registros. El programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro. Puede especificar las siguientes opciones para los archivos de registro:

Nivel mínimo de detalle al registrar: especifica el nivel de contenido mínimo de los sucesos que se van a registrar.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo *"Error al descargar el archivo"*.
- **Grave**: registra únicamente los errores graves (errores al iniciar la protección antivirus, el cortafuegos, etc.).

Las entradas de registro anteriores al número de días especificado en el campo **Eliminar automáticamente los registros con una antigüedad de más de (días)** se eliminarán de manera automática.

Optimizar archivos de registro automáticamente: si se marca esta opción, los archivos de registro se desfragmentarán automáticamente si el porcentaje es superior al valor especificado en **Si la cantidad de registros no usados supera el (%)**.

Haga clic en **Optimizar** para empezar la desfragmentación de los archivos de registro. Todas las entradas de registro vacías se eliminan durante este proceso, lo cual aumenta el rendimiento y la velocidad del proceso de registro. Esta mejora es especialmente notable cuando los registros contienen muchas entradas.

Active **Habilitar formato del texto** para activar el almacenamiento de registros en otro formato de archivo, independiente de Archivos de registro:

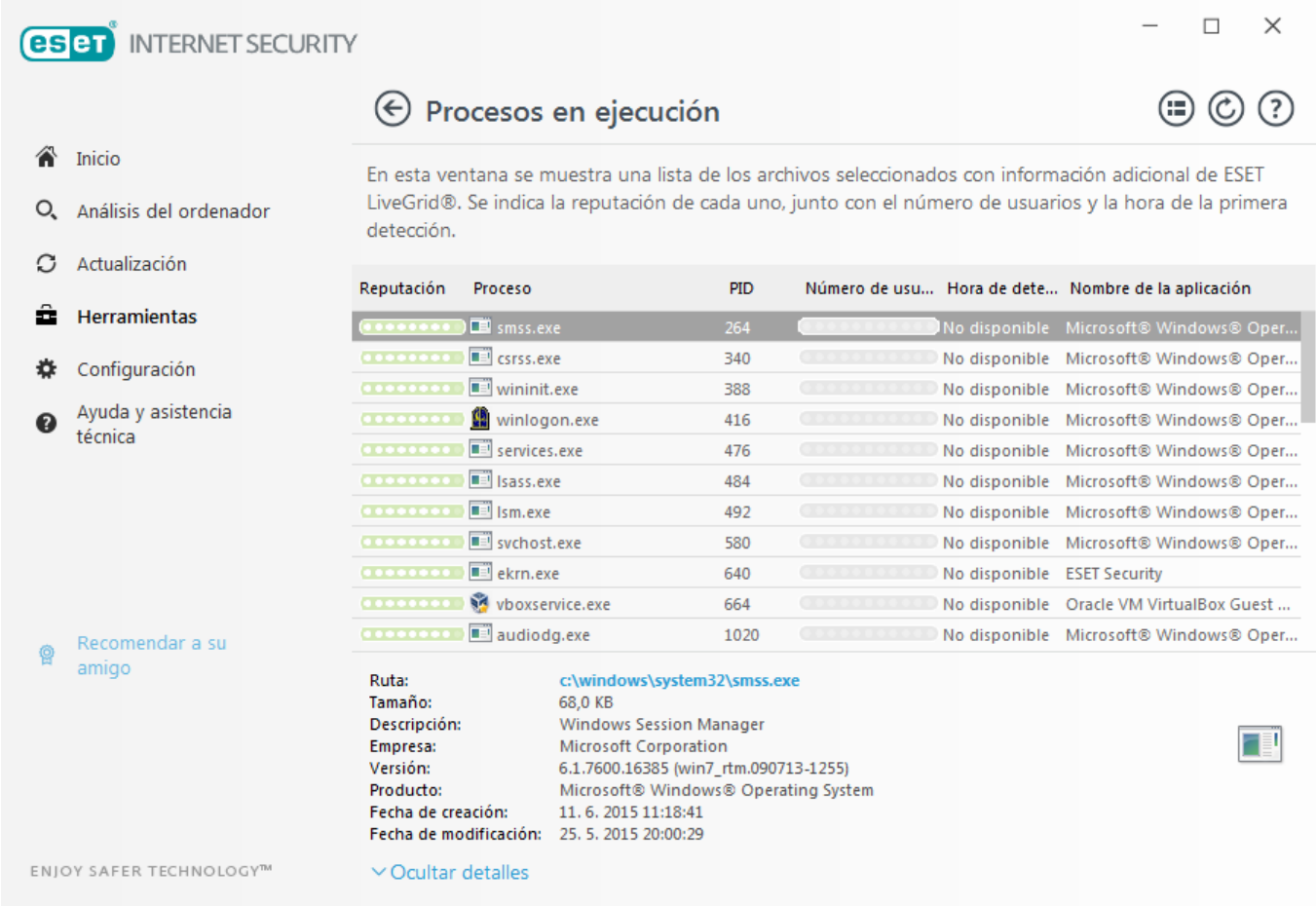
- **Directorio de destino**: directorio donde se almacenarán los archivos de registro (solo se aplica a los formatos de texto y CSV). Cada sección de registros tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, *virlog.txt* para la sección **Amenazas detectadas** de Archivos de registro, si se utiliza el formato de archivo de texto plano para almacenar registros).
- **Tipo**: si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto y los datos se separarán mediante tabuladores. El comportamiento es el mismo para el formato de archivo **CSV** con datos separados por comas. Si selecciona **Suceso**, los registros se almacenarán en el registro de eventos de Windows (que se puede ver en el Visor de eventos del Panel de control), en vez de en un archivo.

Eliminar todos los archivos de registro: borra todos los registros almacenados que se seleccionen en el menú desplegable **Tipo**. Se mostrará una notificación sobre la correcta eliminación de los archivos de registro.

NOTA
ESET podría solicitarle los registros de su ordenador para agilizar la solución de problemas. ESET Log Collector facilita la recopilación de los datos necesarios. Para obtener más información sobre ESET Log Collector, consulte el artículo de la base de conocimiento de ESET.

4.6.3.2 Procesos en ejecución

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



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

Nivel de riesgo: generalmente, ESET Internet Security y la tecnología ThreatSense asignan un nivel de riesgo a los objetos (archivos, procesos, claves del registro, etc.). Para ello, utilizan una serie de reglas heurísticas que examinan las características de cada objeto y, después, ponderan el 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).

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

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

Número de usuarios: el número de usuarios que utilizan una aplicación determinada. La tecnología ThreatSense se encarga de recopilar esta información.

Hora de la detección: tiempo transcurrido desde que la tecnología ThreatSense detectó la aplicación.

NOTA
Una aplicación marcada como Desconocido (naranja) no tiene por qué ser software malicioso. Normalmente, se trata de una aplicación reciente. Si el archivo le plantea dudas, puede enviarlo para su análisis al laboratorio de

investigación de ESET. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una actualización futura.

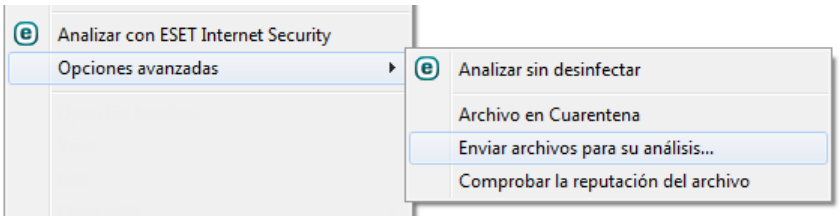
Nombre de aplicación: nombre de un programa o un proceso.

Abrir en una ventana nueva: la información de los procesos en ejecución se abrirá en una ventana nueva.

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

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

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



4.6.3.3 Informe de seguridad

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

Páginas web bloqueadas: muestra el número de páginas web bloqueadas (URL de aplicaciones potencialmente indeseables (PUA), phishing, router, IP o certificado hackeados).
Objetos de correo electrónico infectados detectados: muestra el número de objetos de correo electrónico infectados que se han detectado.
Páginas web bloqueadas en Control parental: muestra el número de páginas web bloqueadas en Control parental.
Aplicación potencialmente indeseable detectada: muestra el número de aplicaciones potencialmente indeseables (PUA).
Correos electrónicos no deseados detectados: muestra el número de mensajes de correo electrónico no deseados detectados.
Accesos a la webcam bloqueados: muestra el número de accesos a la webcam que se han bloqueado.
Accesos a la banca a través de Internet protegidos: muestra el número de accesos a la banca a través de Internet que se han protegido.
Documentos comprobados: muestra el número de objetos de documento analizados.
Aplicaciones comprobadas: muestra el número de objetos ejecutables analizados.
Otros objetos comprobados: muestra el número de otros objetos analizados.
Objetos de páginas web comprobados: muestra el número de objetos de página web analizados.
Objetos de correo electrónico comprobados: muestra el número de objetos de correo electrónico analizados.

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

Debajo de las categorías puede ver la situación de virus real en el mapa del mundo. La presencia de virus en cada país se indica mediante colores (cuanto más oscuro es el color, más alto es el número). Los países de los que no hay datos aparecen atenuados. Coloque el cursor del ratón sobre el país para mostrar datos del país seleccionado. Puede seleccionar un continente y se aplicará zoom automáticamente.

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

- Password Manager
- Secure Data
- Control parental
- Antirrobo

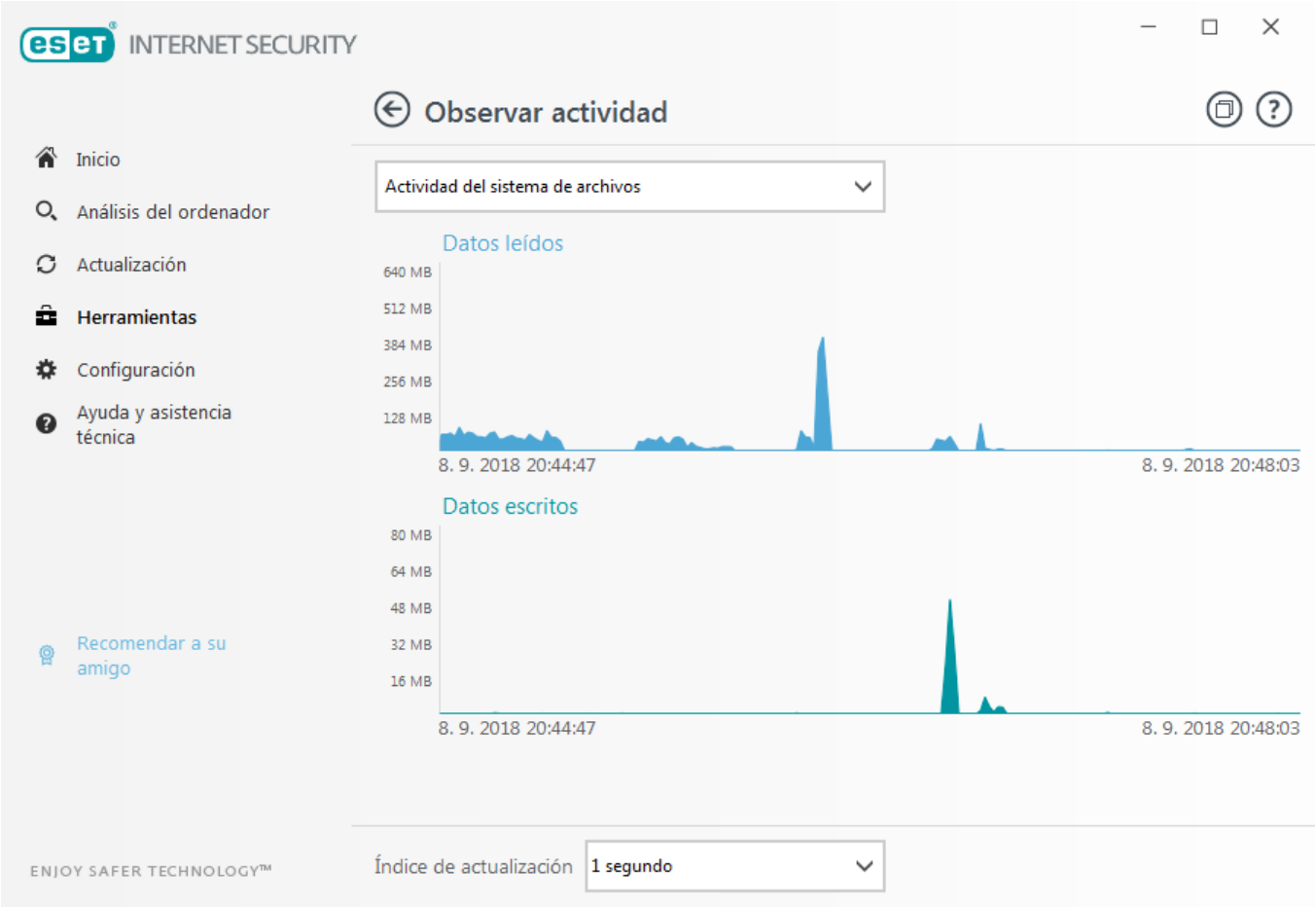
Cuando se active una función, dejará de aparecer como no operativa en el informe de seguridad.

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

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

4.6.3.4 Observar actividad

Para ver la **Actividad del sistema de archivos** actual en un gráfico, haga clic en **Herramientas** > **Más herramientas** > **Observar actividad**. En la parte inferior del gráfico hay una línea cronológica que registra la actividad del sistema de archivos en tiempo real en el intervalo de tiempo seleccionado. Si desea cambiar el intervalo de tiempo, realice la selección en el menú desplegable **Índice de actualización**.



Están disponibles las opciones siguientes:

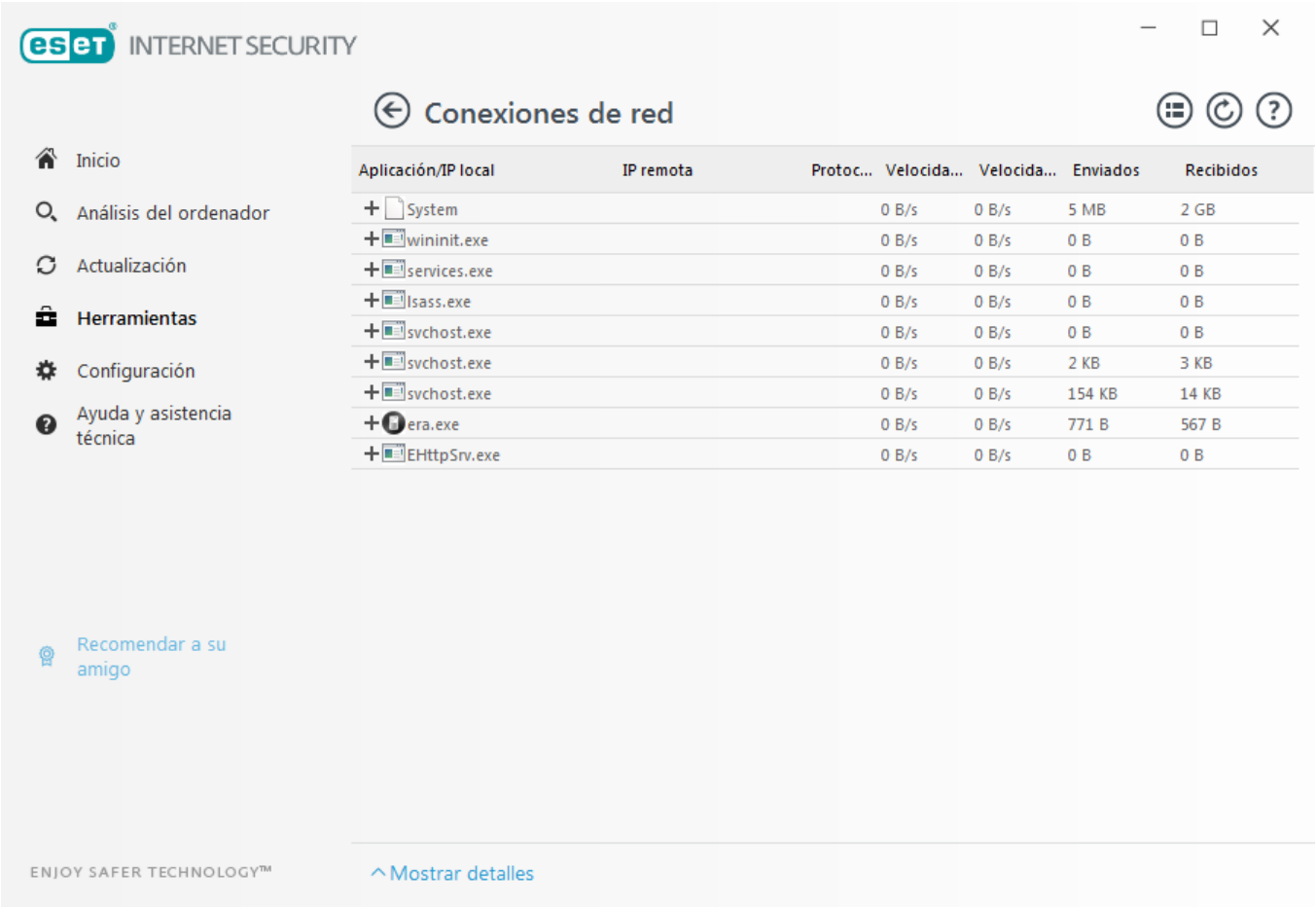
- **Pasar 1 segundo**: el gráfico se actualiza cada segundo y la línea cronológica abarca los últimos 10 minutos.
- **Pasar 1 minuto (últimas 24 horas)**: el gráfico se actualiza cada minuto y la línea cronológica abarca las últimas 24 horas.
- **Pasar 1 hora (último mes)**: el gráfico se actualiza cada hora y la línea cronológica abarca el último mes.
- **Pasar 1 hora (mes seleccionado)**: el gráfico se actualiza cada hora y la línea cronológica abarca los últimos X meses seleccionados.

El eje vertical del **Gráfico de actividad del sistema de archivos** representa los datos leídos (azul) y escritos (rojo). Ambos valores se ofrecen en KB (kilobytes), MB o GB. Si pasa el ratón por encima de los datos leídos o escritos en la leyenda disponible debajo del gráfico, el gráfico solo mostrará los datos de ese tipo de actividad.

En el menú desplegable también puede seleccionar **Actividad de red**. La visualización y las opciones del gráfico para la **Actividad del sistema de archivos** y la **Actividad de red** son las mismas, con la única diferencia de que el último muestra datos recibidos (rojo) y datos enviados (azul).

4.6.3.5 Conexiones de red

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



En la primera línea se muestran el nombre de la aplicación y la velocidad de transferencia de datos. Para ver la lista de conexiones establecidas por la aplicación (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 de un ordenador remoto determinado.

Protocolo: protocolo de transferencia utilizado.

Velocidad de subida/Velocidad de bajada: la velocidad actual de los datos salientes y entrantes.

Enviado/Recibido: cantidad de datos intercambiados dentro de la conexión.

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

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

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

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

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

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

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

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

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

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

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

4.6.3.6 ESET SysInspector

ESET SysInspector es una aplicación que inspecciona a fondo el ordenador, recopila información detallada sobre los componentes del sistema (como los controladores y aplicaciones instalados, las conexiones de red o las entradas importantes del registro) y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa de un comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de código malicioso.

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

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

Están disponibles las siguientes acciones:

- **Mostrar**: abre el registro creado. También puede hacer clic con el botón derecho del ratón sobre un archivo de registro determinado y seleccionar **Mostrar** en el menú contextual.
- **Comparar**: compara dos registros existentes.
- **Crear...**: crea un registro nuevo. Espere hasta que ESET SysInspector finalice (el estado del registro se mostrará como Creado) antes de intentar acceder al registro.
- **Eliminar**: elimina de la lista los archivos de registro seleccionados.

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

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).
- **Comparar**: compara dos registros existentes.
- **Crear...**: crea un registro nuevo. Espere hasta que ESET SysInspector finalice (el estado del registro se mostrará como Creado) antes de intentar acceder al registro.
- **Eliminar**: elimina de la lista los archivos de registro seleccionados.
- **Eliminar todos**: elimina todos los registros.
- **Exportar**: exporta el registro a un archivo *.xml* o *.xml* comprimido.

4.6.3.7 Planificador de tareas

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

Se puede acceder a las Tareas programadas desde la ventana principal del programa de ESET Internet Security haciendo clic en **Herramientas** > **Más herramientas** > **Tareas programadas**. El **Planificador de tareas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

El Planificador de tareas sirve para programar las siguientes tareas: módulos de actualización, tarea de análisis, verificación de archivos en el inicio del sistema y mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana principal de Tareas programadas (haga clic en **Agregar tarea** o **Eliminar** en la parte inferior). Puede restaurar los valores predeterminados de la lista de tareas programadas y eliminar todos los cambios haciendo clic en **Predeterminado**. Haga clic con el botón derecho en cualquier parte de la ventana Planificador de tareas para realizar las siguientes acciones: mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente. Utilice las casillas de verificación disponibles al comienzo de cada entrada para activar o desactivar las tareas.

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

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática tras conexión de acceso telefónico**
- **Actualización automática después del registro del usuario**
- **Búsqueda periódica de la última versión del producto** (consulte Tipo de actualización)
- **Verificación automática de archivos en el inicio** (tras inicio de sesión del usuario)
- **Verificación de la ejecución de archivos en el inicio** (después de actualizar correctamente el motor de detección)

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

Agregar una nueva tarea

1. Haga clic en **Agregar tarea**, en la parte inferior de la ventana.
2. Introduzca un nombre para la tarea.

3. Seleccione la tarea deseada en el menú desplegable:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear una instantánea de estado del equipo**: crea una instantánea del ordenador de ESET SysInspector, recopila información detallada sobre los componentes del sistema (por ejemplo, controladores y aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

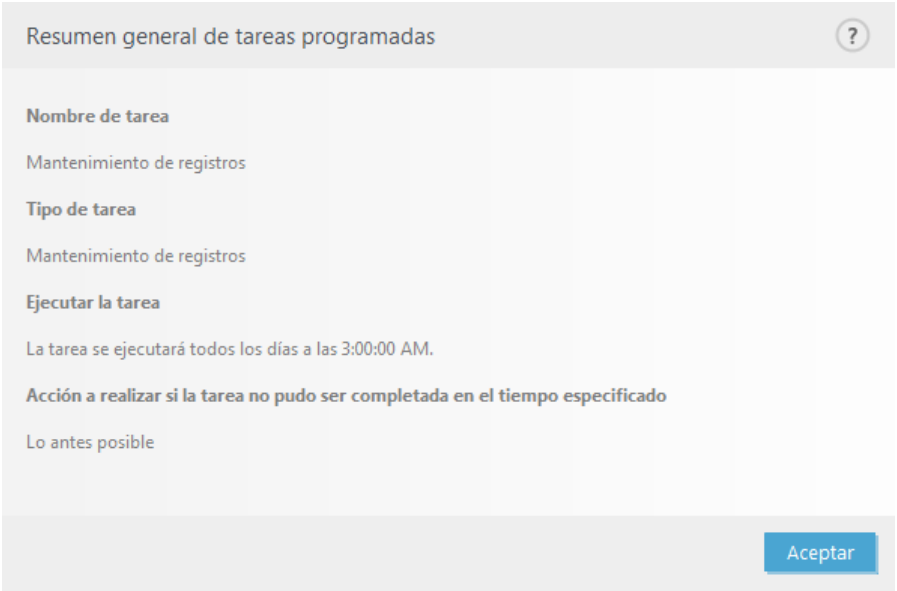
4. Active la opción **Activado** si desea activar la tarea (puede hacerlo más adelante mediante casilla de verificación situada en la lista de tareas programas), haga clic en **Siguiente** y seleccione una de las opciones de programación:

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

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

   - **En la siguiente hora programada**
   - **Lo antes posible**
   - **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución**)

Si desea revisar la tarea programada, haga clic con el botón derecho del ratón y, después, haga clic en **Mostrar detalles de la tarea**.



4.6.3.8 Desinfección del sistema

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

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

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

La desinfección del sistema puede solicitarse en las siguientes situaciones:

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

Puede revisar los cambios y restablecer la configuración si procede.

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

4.6.3.9 ESET SysRescue

ESET SysRescue es una utilidad que le permite crear un disco de inicio que contenga una de las soluciones de ESET Security, ya sea ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium o determinados productos diseñados para servidores. La principal ventaja de ESET SysRescue es que la solución ESET Security se puede ejecutar de forma independiente del sistema operativo host, pero tiene acceso directo al disco y a todo el sistema de archivos. Gracias a esto, es posible eliminar las amenazas que normalmente no se podrían suprimir como, por ejemplo, cuando el sistema operativo se está ejecutando.

4.6.3.10 Protección en la nube

ESET LiveGrid® (que se basa en el sistema avanzado de alerta temprana ThreatSense.Net) utiliza los datos enviados por usuarios de ESET de todo el mundo y los envía al laboratorio de investigación de ESET. ESET LiveGrid® proporciona metadatos y muestras sospechosas en estado salvaje, lo cual nos permite reaccionar de forma inmediata a las necesidades de nuestros clientes y hace posible la respuesta de ESET a las amenazas más recientes. Puede obtener más información sobre ESET LiveGrid® en el glosario.

Los usuarios pueden consultar la reputación de los archivos y procesos en ejecución directamente en la interfaz del programa o en el menú contextual; además, disponen de información adicional en ESET LiveGrid®. Existen dos opciones:

1. La activación de ESET LiveGrid® no es obligatoria. El software no perderá funcionalidad, pero puede que ESET Internet Security responda más rápido a las nuevas amenazas que la actualización del motor de detección cuando ESET Live Grid está activado.
2. Puede configurar ESET LiveGrid® para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso. Este archivo se puede enviar a ESET para que realice un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar sus funciones de detección de amenazas.

ESET LiveGrid® recopilará información anónima del ordenador relacionada con las amenazas detectadas recientemente. Esta información puede incluir una muestra o copia del archivo donde ha aparecido la amenaza, la ruta de acceso a ese archivo, el nombre del archivo, la fecha y la hora, el proceso por el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

De forma predeterminada, ESET Internet Security está configurado para enviar archivos sospechosos para su análisis detallado en el laboratorio de virus de ESET. Los archivos con determinadas extensiones, como *.doc* o *.xls*, se excluyen siempre. También puede agregar otras extensiones para excluir los archivos que usted o su empresa no deseen enviar.

El sistema de reputación ESET LiveGrid® ofrece listas blancas y negras basadas en la nube. Si desea acceder a la configuración de ESET LiveGrid®, pulse **F5** para ir a Configuración avanzada y despliegue **Motor de detección** > Protección en la nube.

Activar el sistema de reputación ESET LiveGrid® (recomendado): el sistema de reputación ESET LiveGrid® mejora la eficiencia de las soluciones contra software malicioso de ESET mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.

Activar sistema de respuesta ESET LiveGrid®: los datos se enviarán al laboratorio de investigación de ESET para su análisis.

Enviar informes de bloqueo y datos de diagnóstico: se envían datos como informes de bloqueo y volcados de la memoria de los módulos.

Enviar estadísticas anónimas: permita a ESET recopilar información sobre nuevas amenazas detectadas, como el nombre de la amenaza, la fecha y hora en las que se detectó, el método de detección y los metadatos asociados. la versión del producto y la configuración del mismo, incluida información sobre su sistema.

Correo electrónico de contacto (opcional): su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

Envío de muestras

Enviar muestras infectadas: si activa esta opción, enviará a ESET todas las muestras infectadas para que las analice y mejore la detección futura. Están disponibles las opciones siguientes:

- Todas las muestras infectadas
- Todas las muestras excepto los documentos
- No enviar

Enviar muestras sospechosas

Ejecutables: incluye archivos como .exe, .dll y .sys.
Archivos comprimidos: incluye tipos de archivo comprimido como .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc y .cab.
Scripts: incluye tipos de archivo de script como .bat, .cmd, .hta, .js, .vbs y .ps1.
Otros: incluye tipos de archivo como .jar, .reg, .msi, .sfw y .lnk.
Correos electrónicos con posible spam: esto permitirá el envío de correos electrónicos con posible contenido de spam o correos electrónicos que en su totalidad sean spam con archivos adjuntos a ESET para que los analice. Activar esta opción mejora la detección global de spam, y usted también disfrutará de las futuras mejoras en la detección de spam.
Documentos: incluye documentos de Microsoft Office o PDF con contenido activo.

Exclusiones: esta opción le permite excluir del envío determinados archivos o carpetas (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Si utilizó ESET LiveGrid® anteriormente pero lo desactivó, es posible que aún haya paquetes de datos pendientes de envío. Estos paquetes se enviarán a ESET incluso después de la desactivación. Una vez que se haya enviado toda la información actual, no se crearán más paquetes.

4.6.3.10.1 Archivos sospechosos

Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio de investigación de ESET. Si resulta ser una aplicación maliciosa, su detección se agregará a la siguiente actualización de la base de firmas de virus.

Filtro de exclusión: esta opción le permite excluir del envío determinados archivos o carpetas. Los archivos mostrados en la lista nunca se enviarán al laboratorio de investigación de ESET para su análisis, aunque contengan código sospechoso. Esta opción puede ser útil, por ejemplo, para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

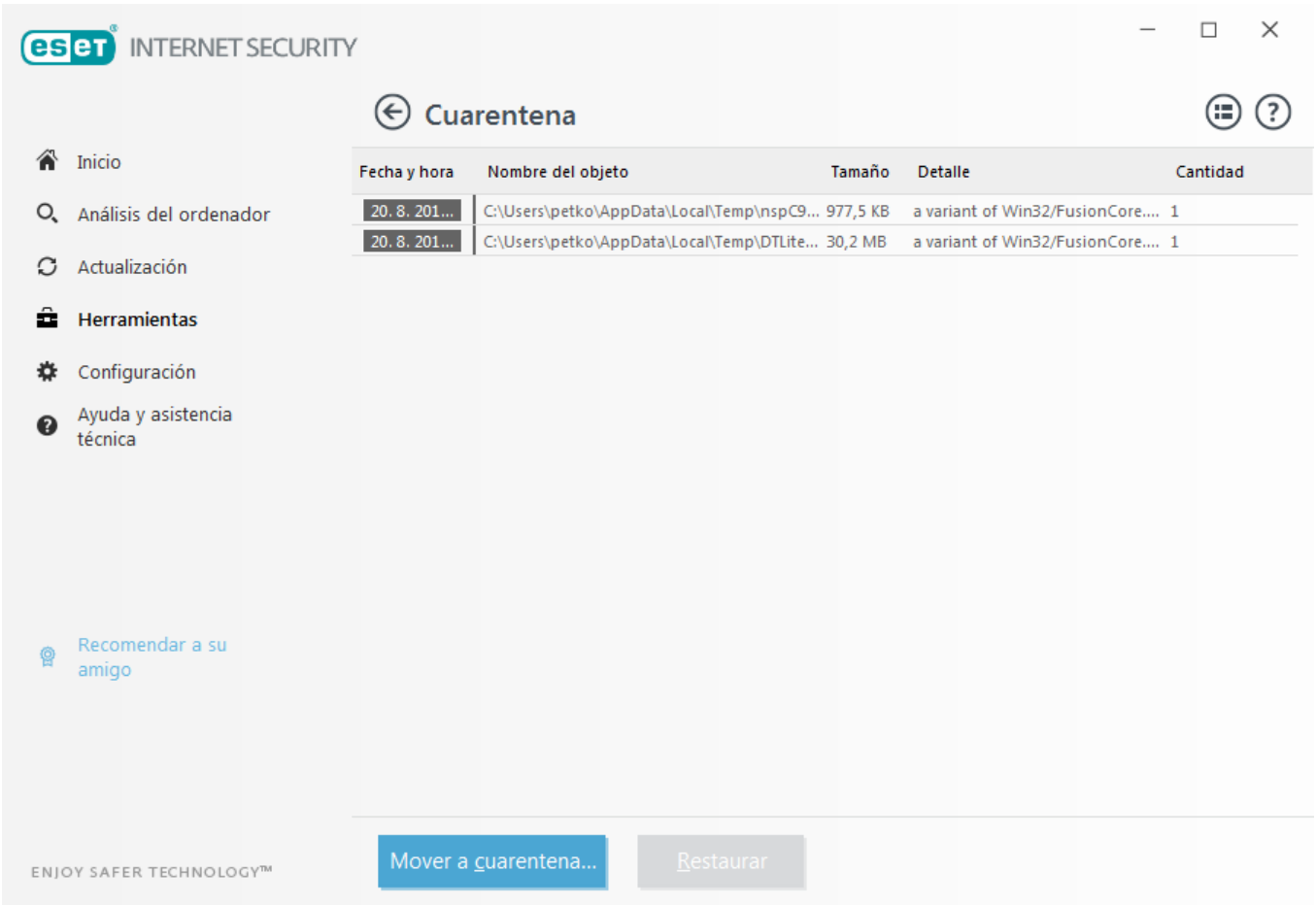
Correo electrónico de contacto (opcional): su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

Seleccione **Activar el registro de sucesos** para crear un registro de sucesos en el que anotar los envíos de archivos e información estadística. Permitirá agregar anotaciones al registro de sucesos cuando se envíen archivos o información estadística.

4.6.3.11 Cuarentena

La función principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Internet Security los detecta incorrectamente como infectados.

Es posible poner en cuarentena cualquier archivo. La cuarentena se recomienda cuando el comportamiento de un archivo es sospechoso y el análisis no lo ha detectado. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de investigación de ESET.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, por ejemplo) y el número de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias amenazas).

Puesta de archivos en cuarentena

ESET Internet Security copia en cuarentena automáticamente los archivos eliminados (si no ha cancelado esta opción en la ventana de alerta). Si lo desea, puede copiar en cuarentena cualquier archivo sospechoso de forma manual, haciendo clic en el botón **Cuarentena...** En este caso, el archivo original no se eliminará de su ubicación original. El menú contextual también se puede utilizar con este fin; haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Para realizar esta tarea, utilice la opción **Restaurar**, disponible en el menú contextual que se abre al hacer clic con el botón derecho del ratón en un archivo en la ventana de cuarentena. Si un archivo está marcado como aplicación potencialmente indeseable, se activa la opción **Restaurar y excluir del análisis**. Puede obtener más información sobre este tipo de aplicación en el glosario. El menú contextual también ofrece la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

Eliminación de la cuarentena: haga clic con el botón derecho del ratón en el elemento que desee y seleccione **Eliminar de la cuarentena**, o seleccione el elemento que desee eliminar y pulse **Suprimir** en el teclado. Es posible seleccionar varios elementos y eliminarlos al mismo tiempo.

NOTA
Si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

Envío de un archivo de cuarentena

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

4.6.3.12 Servidor Proxy

En las redes LAN de gran tamaño, un servidor proxy puede mediar en la comunicación entre el ordenador e Internet. Si se usa esta configuración se deberán definir los siguientes parámetros. De lo contrario, el programa no se podrá actualizar de manera automática. En ESET Internet Security, el servidor proxy se puede configurar en dos secciones diferentes del árbol de Configuración avanzada.

En primer lugar, se puede configurar en **Configuración avanzada**, bajo **Herramientas** > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para ESET Internet Security. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar la configuración del servidor proxy en este nivel, seleccione **Usar servidor proxy** y especifique la dirección del servidor proxy en el campo **Servidor proxy** y su número de **Puerto**.

Si la comunicación con el servidor proxy requiere autenticación, seleccione **El servidor proxy requiere autenticación** e introduzca un **nombre de usuario** y una **contraseña** válidos en los campos correspondientes. Haga clic en **Detectar** para detectar y cumplimentar la configuración del servidor proxy de forma automática. Se copiarán los parámetros especificados en Internet Explorer.

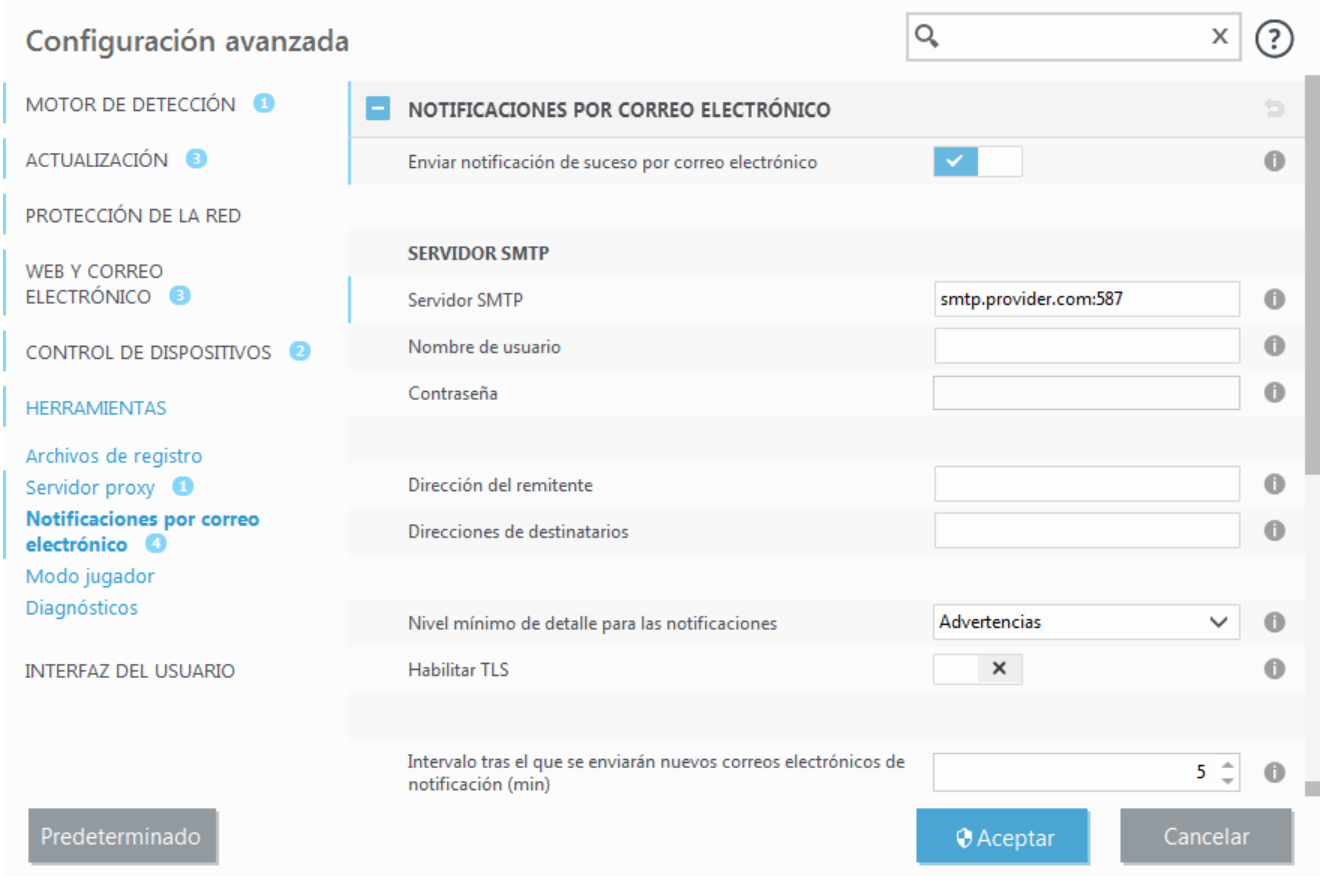
NOTA
Debe especificar el nombre de usuario y la contraseña manualmente en la configuración del **Servidor proxy**.

Usar conexión directa si el proxy no está disponible: si un producto está configurado para utilizar un proxy HTTP y el proxy está inaccesible, el producto ignorará el proxy y se comunicará directamente con los servidores de ESET.

La configuración del servidor proxy también se puede definir en Configuración avanzada de actualizaciones (**Configuración avanzada** > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión**; para ello, seleccione **Conexión a través de un servidor proxy** en el menú desplegable **Modo proxy**). Esta configuración se aplica al perfil de actualización dado y se recomienda para ordenadores portátiles que suelen recibir actualizaciones de firmas de virus de ubicaciones remotas. Para obtener más información sobre este ajuste, consulte la sección Configuración avanzada de actualizaciones.

4.6.3.13 Notificaciones por correo electrónico

ESET Internet Security puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Active **Enviar notificaciones de sucesos por correo electrónico** para activar las notificaciones por correo electrónico.



Servidor SMTP

Servidor SMTP: el servidor SMTP que se utiliza para enviar notificaciones (por ejemplo, *smtp.provider.com:587*, el puerto predefinido es 25).

> **NOTA**
> Los servidores SMTP con cifrado TLS son compatibles con ESET Internet Security.

Nombre de usuario y **contraseña**: si el servidor SMTP requiere autenticación, estos campos deben cumplimentarse con un nombre de usuario y una contraseña válidos que faciliten el acceso al servidor SMTP.

Dirección del remitente: defina la dirección de correo del emisor que se mostrará en el encabezado de los mensajes de correo electrónico de notificación.

Direcciones de destinatarios: defina las direcciones de correo de los destinatarios que se mostrarán en el encabezado de los mensajes de correo electrónico de notificación. Es posible incluir varios valores; utilice el punto y coma como separador.

En el menú desplegable **Nivel mínimo de detalle para las notificaciones** puede seleccionar el nivel de gravedad inicial de las notificaciones que desea enviar.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, como los sucesos de red no convencionales, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra los errores graves y los mensajes de advertencia (la tecnología Anti-Stealth no está funcionando adecuadamente o el proceso de actualización ha fallado).
- **Errores**: se registran los errores (protección de documentos no iniciada) y los errores graves.
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus o de infección del sistema).

Habilitar TLS: active el envío de mensajes de notificación y alerta que admite el cifrado TLS.

Intervalo tras el que se enviarán nuevos correos electrónicos de notificación (min): intervalo en minutos tras el cual se enviarán nuevas notificaciones al correo electrónico. Si define este valor en 0, las notificaciones se enviarán de forma inmediata.

Enviar cada notificación en un correo electrónico distinto: si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría suponer la recepción de numerosos correos electrónicos en un breve periodo de tiempo.

Formato de mensajes

Para notificar la ocurrencia de sucesos: formato de los mensajes de suceso que se muestran en los ordenadores remotos.

Para alertar sobre amenazas: los mensajes de notificación y alerta de amenazas tienen un formato predefinido de forma predeterminada. Le aconsejamos que no modifique este formato. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes.

Conjunto de caracteres: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI según la configuración regional de Windows (por ejemplo, windows-1250), Unicode (UTF-8), ACSII 7-bit (por ejemplo "á" se cambiará a "a" y un símbolo desconocidoa "?") o japonés (ISO-2022-JP).

Usar codificación Quoted-printable: el origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo pude transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (áéíóú).

4.6.3.13.1 Formato de mensajes

Aquí puede configurar el formato de los mensajes de sucesos que aparece en los ordenadores remotos.

Los mensajes de alerta de amenaza y de notificación tienen un formato predefinido de forma predeterminada. Le aconsejamos que no modifique este formato. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes.

Las palabras clave (cadenas separadas por signos %) se sustituyen en el mensaje por la información real especificada. Están disponibles las siguientes palabras clave:

- **%TimeStamp%**: fecha y hora del suceso.
- **%Scanner%**: módulo correspondiente.
- **%ComputerName%**: nombre del ordenador en el que se produjo la alerta.
- **%ProgramName%**: programa que generó la alerta.
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectado.
- **%VirusName%**: identificación de la infección.
- **%Action%**: acción adoptada respecto a la amenaza.
- **%ErrorDescription%**: descripción de un suceso que no está relacionado con un virus.

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se utilizan en los mensajes de alerta de amenaza y **%ErrorDescription%**, en los mensajes de sucesos.

Usar caracteres del alfabeto local: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI basándose en la configuración regional de Windows (p. ej., windows-1250). Si deja esta opción sin marcar, se convertirá y codificará un mensaje en ACSII de 7 bits (por ejemplo, "á" se cambiará a "a", y un símbolo desconocido a "?").

Usar codificación de caracteres locales: el origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo pude transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (áéíóú).

4.6.3.14 Seleccionar muestra para el análisis

El cuadro de diálogo de envío de archivos le permite enviar un archivo o un sitio a ESET para que lo analice; esta opción está disponible en **Herramientas** > **Enviar muestra para el análisis**. Si encuentra un archivo en su ordenador que se comporta de manera sospechosa o un sitio sospechoso en Internet, puede enviarlo al laboratorio de investigación de ESET para su análisis. Si resulta que el archivo es una aplicación o un sitio web malicioso, su detección se agregará a una actualización futura.

También puede enviar el archivo por correo electrónico. Si prefiere esta opción, comprima los archivos con WinRAR/ZIP, proteja el archivo comprimido con la contraseña "infected" y envíelo a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el archivo (por ejemplo, el sitio web del que lo descargó).

> **NOTA**
> Antes de enviar un archivo a ESET, asegúrese de que cumple uno o más de los siguientes criterios:
>
> - El archivo no se detecta en absoluto.
> - El archivo se detecta como una amenaza, pero no lo es.
>
> No recibirá ninguna respuesta a menos que se requiera información adicional para poder realizar el análisis.

Seleccione la descripción en el menú desplegable **Motivo de envío del archivo** que mejor se ajuste a su mensaje:

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

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

Correo electrónico de contacto: la dirección de correo de contacto se envía a ESET junto con los archivos sospechosos y se puede utilizar para el contacto con usted en caso de que sea necesario enviar más información para poder realizar el análisis. No es obligatorio introducir una dirección de correo electrónico de contacto. La muestra puede **enviarse de forma anónima**. No obtendrá ninguna respuesta de ESET a menos que sea necesario enviar información adicional, ya que cada día nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.

4.6.3.15 Microsoft Windows® update

La característica Windows Update es un componente importante de protección de los usuarios de software malicioso, por eso es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Internet Security le informa sobre las actualizaciones que le faltan, según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **No hay actualizaciones**: no se ofrecerá ninguna actualización del sistema para la descarga.
- **Actualizaciones opcionales**: se ofrecerán para la descarga las actualizaciones marcadas como de baja prioridad y de niveles superiores.
- **Actualizaciones recomendadas**: se ofrecerán para la descarga las actualizaciones marcadas como habituales y de niveles superiores.
- **Actualizaciones importantes**: se ofrecerán para la descarga las actualizaciones marcadas como importantes y de niveles superiores.
- **Actualizaciones críticas**: solo se ofrecerá la descarga de actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará después de la verificación del estado con el servidor de actualización. Por tanto, es posible que la información de actualización del sistema no esté disponible inmediatamente después de guardar los cambios.

4.6.3.16 CMD de ESET

Se trata de una función que activa comandos de ecmd avanzados. Le permite exportar e importar la configuración utilizando la línea de comandos (ecmd.exe). Hasta ahora, solo era posible exportar la configuración utilizando la interfaz gráfica de usuario. La configuración de ESET Internet Security puede exportarse a un archivo *.xml*.

Si tiene activado el CMD de ESET, dispone de dos métodos de autorización:

- **Ninguno**: sin autorización. No le recomendamos este método, ya que permite importar configuraciones no firmadas, lo que supone un riesgo.
- **Configuración avanzada de contraseña**: se requiere contraseña para importar una configuración de un archivo *.xml*. Este archivo debe estar firmado (consulte cómo se firma un archivo de configuración *.xml* más adelante). Debe introducirse la contraseña especificada en Configuración de acceso para poder importar una nueva configuración. Si no ha activado la configuración de acceso, la contraseña no coincide o el archivo de configuración *.xml* no está firmado, la configuración no se importará.

Una vez que CMD de ESET esté activado, podrá utilizar la línea de comandos para importar o exportar configuraciones de ESET Internet Security. Podrá hacerlo manualmente o crear un script con fines de automatización.

IMPORTANTE
Para poder utilizar comandos de ecmd avanzados, deberá ejecutarlos con privilegios de administrador, o abrir el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**. De lo contrario, se mostrará el mensaje **Error executing command.**. Asimismo, a la hora de exportar una configuración, deberá existir una carpeta de destino. El comando de exportación sigue funcionando cuando se desactiva el ajuste CMD de ESET.

EJEMPLO
Comando para exportar configuración:

```
ecmd /getcfg c:\config\settings.xml
```

Comando para importar configuración:

```
ecmd /setcfg c:\config\settings.xml
```

NOTA
Los comandos de ecmd avanzados solo pueden ejecutarse de forma local.

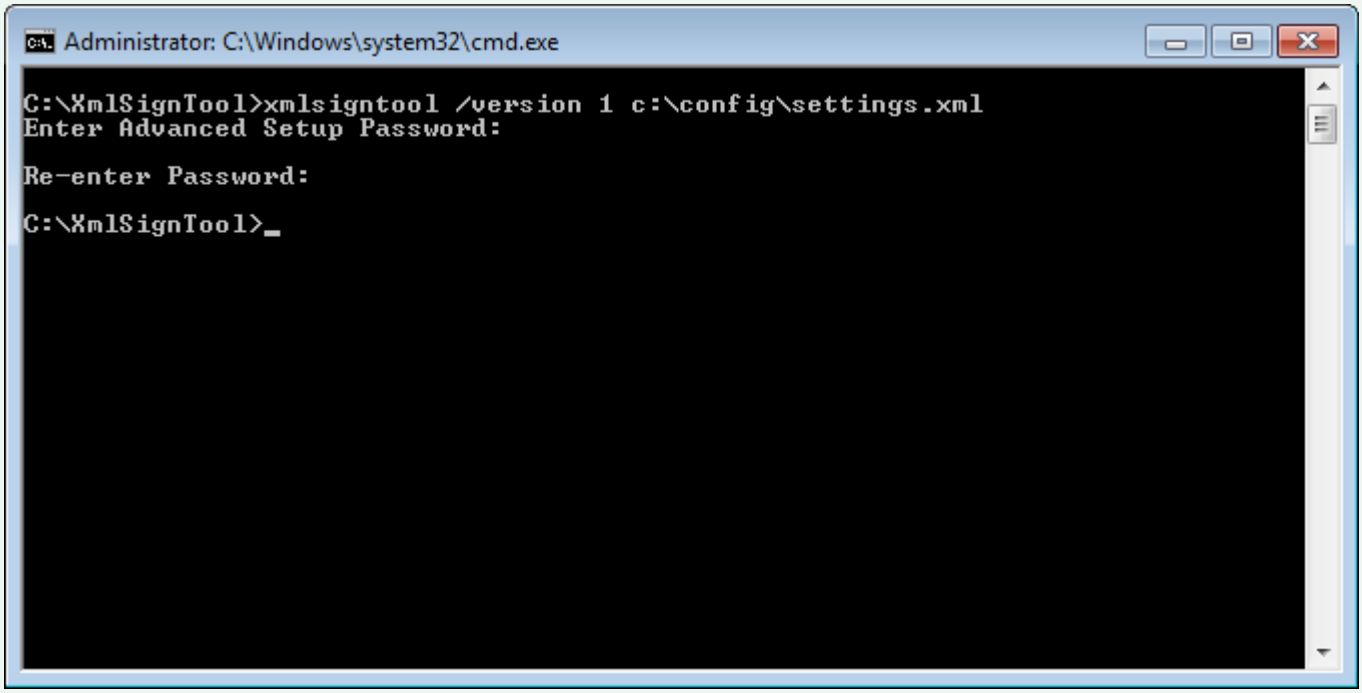
Cómo firmar un archivo de configuración *.xml*:

1. Descargue el archivo ejecutable XmlSignTool.
2. Abra el símbolo del sistema de Windows (cmd) utilizando **Ejecutar como administrador**.
3. Vaya a la ubicación en la que se ha guardado `xmlsigntool.exe`.
4. Ejecute un comando para firmar el archivo de configuración *.xml*, uso: `xmlsigntool /version 1|2 <xml_file_path>`

IMPORTANTE
El valor del parámetro `/version` depende de su versión de ESET Internet Security. Utilice `/version 1` para versiones de ESET Internet Security anteriores a 11.1. Utilice `/version 2` para la versión actual de ESET Internet Security.

5. Introduzca y vuelva a introducir la contraseña de Configuración avanzada cuando se lo solicite XmlSignTool. Su archivo de configuración *.xml* ya estará firmado y podrá utilizarse para importar otra instancia de ESET Internet Security con CMD de ESET utilizando el método de autorización de contraseña.

EJEMPLO
Comando para firmar un archivo de configuración exportado:
`xmlsigntool /version 1 c:\config\settings.xml`



NOTA
Si la contraseña de Configuración de acceso cambia y desea importar una configuración firmada anteriormente con una contraseña antigua, tendrá que volver a firmar el archivo de configuración *.xml* utilizando la contraseña actual. Esto le permitirá utilizar un archivo de configuración más antiguo sin necesidad de exportarlo a otro equipo que ejecute ESET Internet Security antes de la importación.

4.7 Interfaz de usuario

En la sección **Interfaz de usuario** es posible configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa.

La herramienta Gráficos le permite ajustar el aspecto visual del programa y los efectos utilizados.

En la configuración de Alertas y notificaciones, puede cambiar el comportamiento de las alertas de amenaza detectadas y las notificaciones del sistema, que se pueden adaptar a las necesidades de cada uno.

Si desea disponer del máximo nivel de seguridad del software de seguridad, proteja la configuración mediante una contraseña para impedir los cambios no autorizados con la herramienta Configuración de acceso.

4.7.1 Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz de usuario de ESET Internet Security le permiten ajustar el entorno de trabajo según sus necesidades. Estas opciones de configuración están disponibles en la sección **Configuración avanzada** > **Interfaz de usuario** > **Elementos de la interfaz de usuario**.

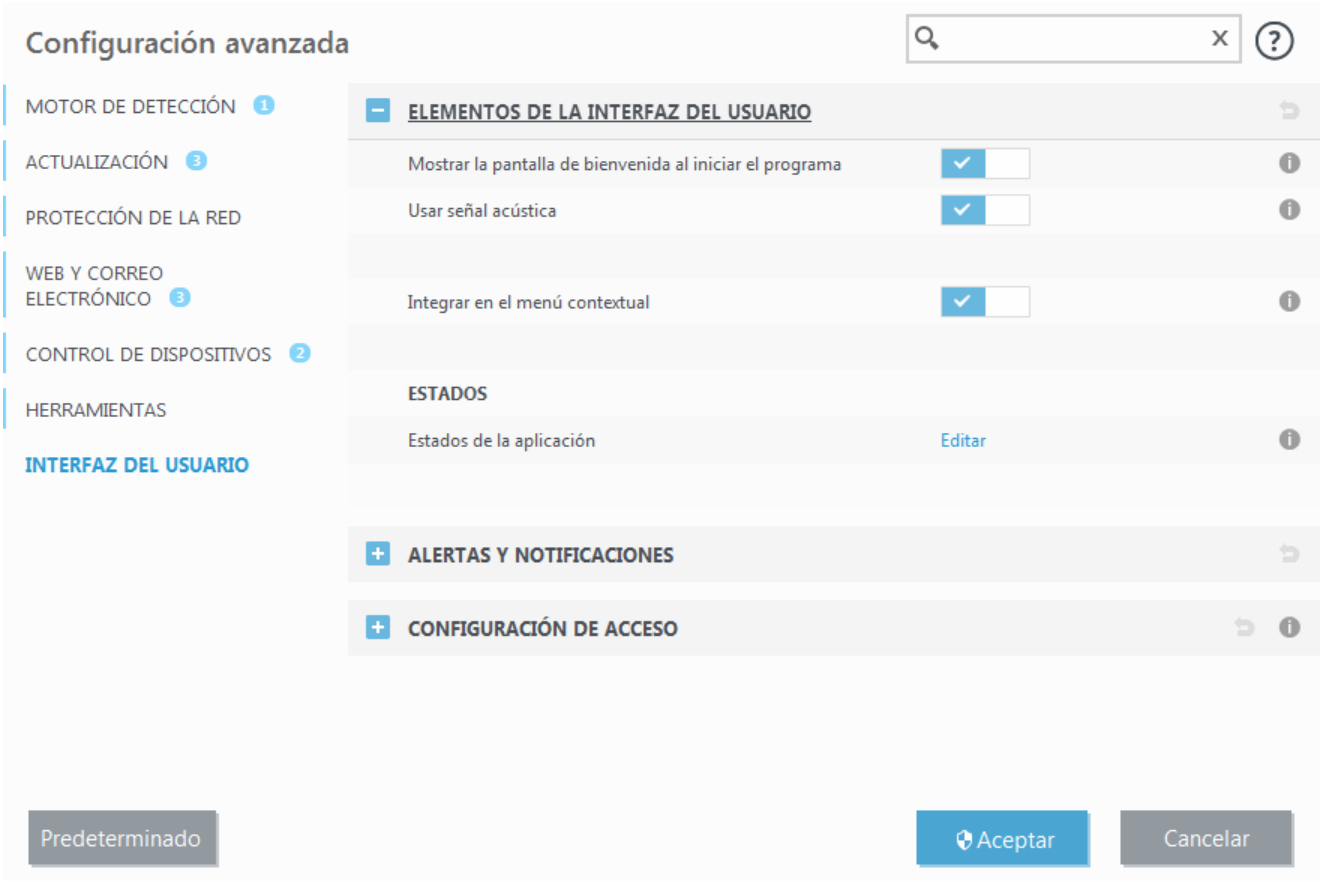
Si desea desactivar la pantalla inicial de ESET Internet Security, anule la selección de **Mostrar pantalla inicial con la carga del sistema**.

Si desea que ESET Internet Security reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis, seleccione **Usar señal acústica**.

Integrar en el menú contextual: integra los elementos de control de ESET Internet Security en el menú contextual.

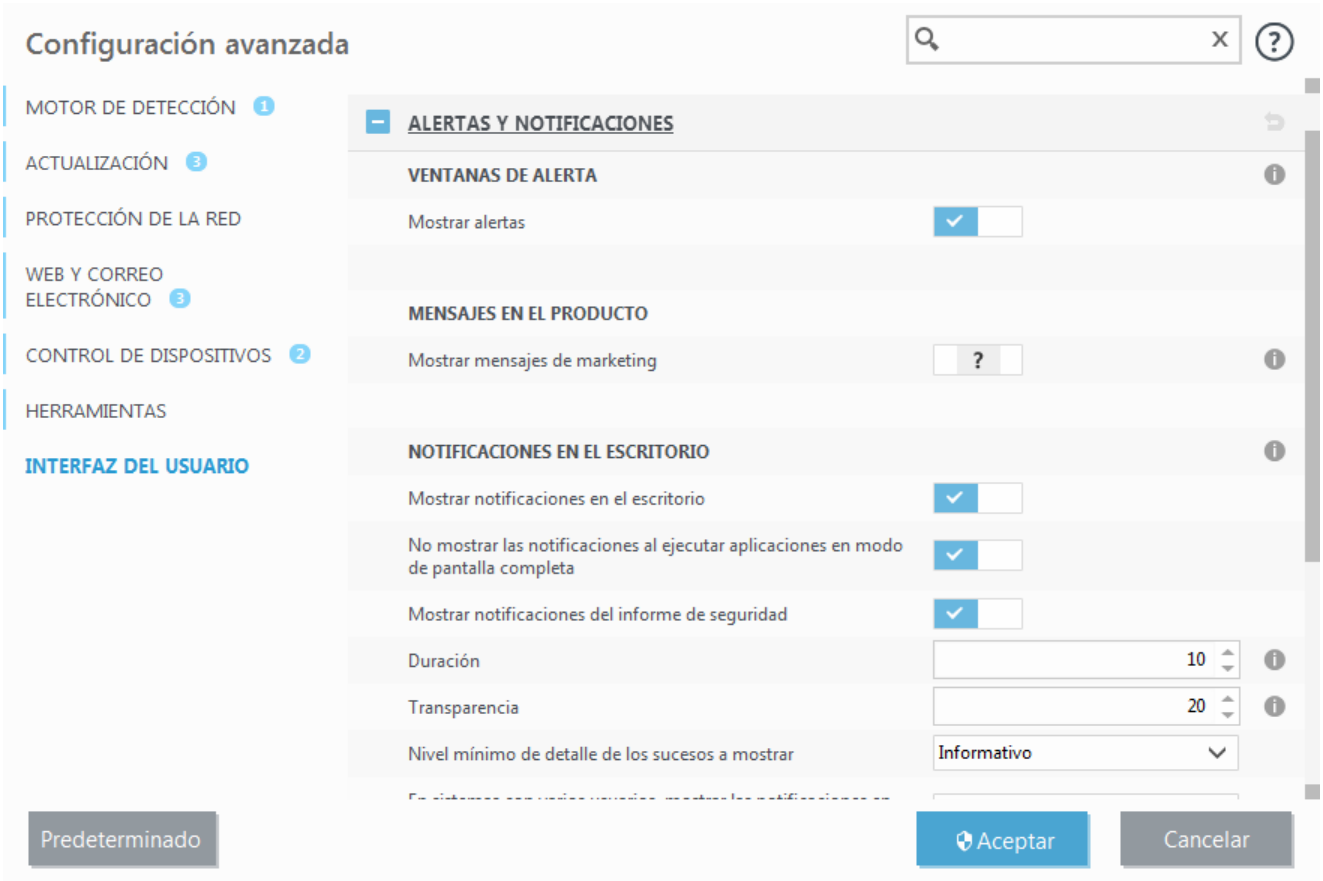
Estados

Estados de la aplicación: haga clic en el botón **Editar** para administrar (desactivar) los estados que se muestran en el primer panel del menú principal.



4.7.2 Alertas y notificaciones

La sección de **Alertas y notificaciones** de **Interfaz de usuario** le permite configurar cómo gestiona ESET Internet Security las notificaciones del sistema (por ejemplo, mensajes de actualización correcta) y las alertas de amenaza. También puede definir si se muestra la hora y la transparencia de las notificaciones de la bandeja del sistema (esto se aplica únicamente a los sistemas que admiten notificaciones en la bandeja del sistema).



Ventanas de alerta

Si desactiva la opción **Mostrar alertas**, se cancelarán todos los mensajes de alerta. Solo resulta útil para una serie de situaciones muy específicas. Para la mayoría de los usuarios, se recomienda mantener la configuración predeterminada (activada).

Mensajes en el producto

Mostrar mensajes de marketing: se han designado mensajes en el producto para informar a los usuarios acerca de noticias de ESET y otras comunicaciones. Para enviar mensajes de marketing es necesario el consentimiento del usuario. Por lo tanto, los mensajes de marketing no se envían a los usuarios de forma predeterminada (se muestran como un signo de interrogación). Al activar esta opción, acepta recibir mensajes de marketing de ESET. Si no le interesa recibir material de marketing de ESET, desactive la opción.

Notificaciones en el escritorio

Las notificaciones del escritorio y los globos de sugerencias son medios de información que no requieren la intervención del usuario. Se muestran en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para activar las notificaciones de escritorio, seleccione **Mostrar notificaciones en el escritorio**.

Active **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa** para suprimir todas las notificaciones que no sean interactivas. A continuación encontrará más opciones avanzadas, como la modificación del tiempo de visualización de las notificaciones y la transparencia de las ventanas.

Mostrar notificaciones del informe de seguridad: puede activar o desactivar las notificaciones del informe de seguridad.

En el menú desplegable **Nivel mínimo de detalle de los sucesos a mostrar** se puede seleccionar el nivel de gravedad de las alertas y notificaciones que se mostrarán. Están disponibles las opciones siguientes:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus, cortafuegos integrado, etc.).

La última característica de esta sección le permite configurar el destino de las notificaciones en un entorno con varios usuarios. En el campo **En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este usuario** se especifica el usuario que recibirá notificaciones del sistema y de otro tipo en sistemas que permitan la conexión de varios usuarios al mismo tiempo. Normalmente, este usuario es un administrador de sistemas o de redes. Esta opción resulta especialmente útil para servidores de terminal, siempre que todas las notificaciones del sistema se envíen al administrador.

Buzones de correo

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione la opción **Cerrar ventanas de notificación automáticamente**. Si no se cierran de forma manual, las ventanas de alerta se cerrarán automáticamente cuando haya transcurrido el período de tiempo especificado.

Mensajes de confirmación: muestra una lista de mensajes de confirmación que se pueden seleccionar para que se muestren o no.

4.7.2.1 Configuración avanzada

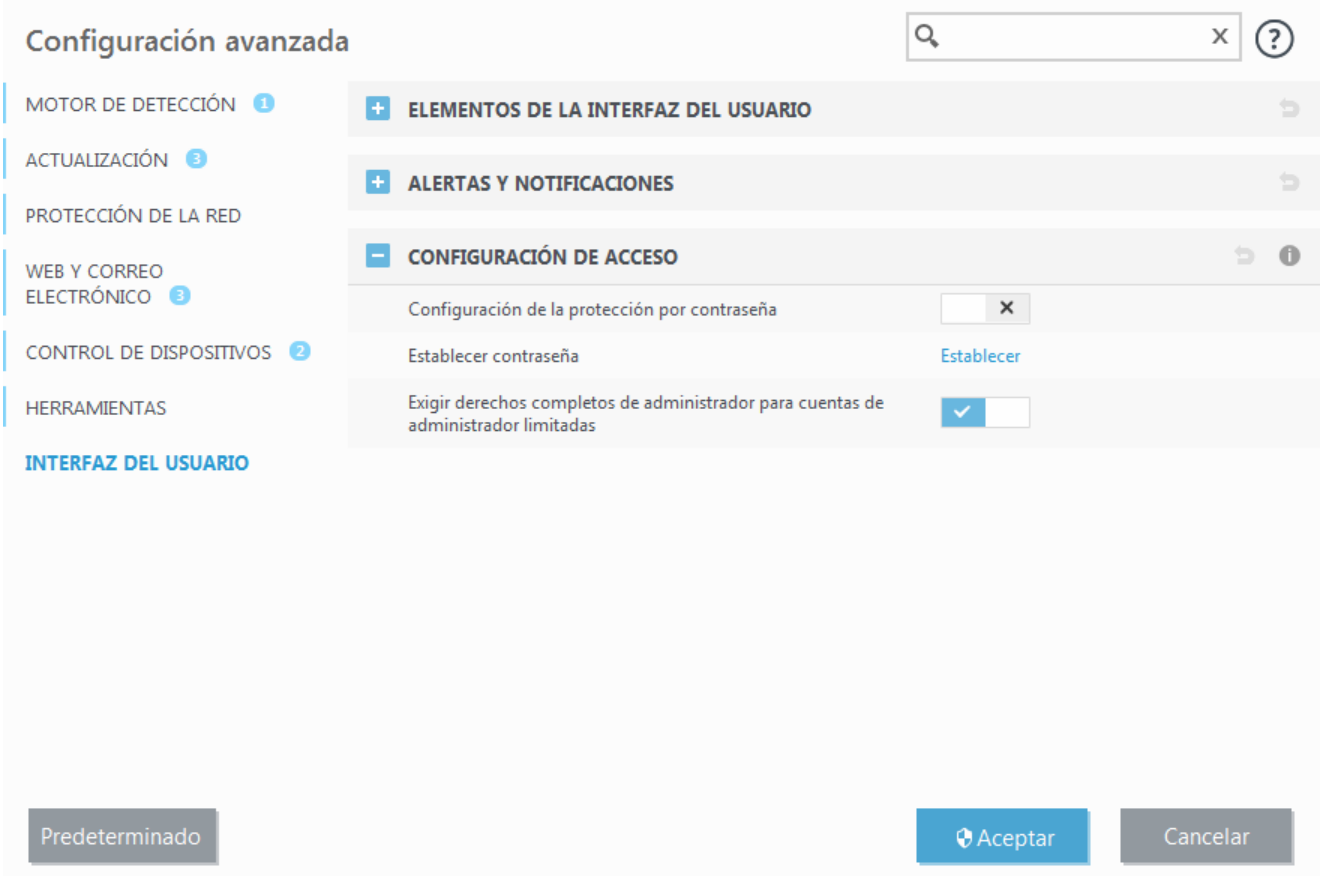
En el menú desplegable **Nivel mínimo de detalle de los eventos a mostrar**, puede seleccionar el nivel de gravedad inicial de las alertas y notificaciones que se mostrarán.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo *"Error al descargar el archivo"*.
- **Grave**: registra únicamente los errores graves (errores al iniciar la protección antivirus, el cortafuegos, etc.).

La última característica de esta sección le permite configurar el destino de las notificaciones en un entorno con varios usuarios. En el campo **En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este usuario** se especifica el usuario que recibirá notificaciones del sistema y de otro tipo en sistemas que permitan la conexión de varios usuarios al mismo tiempo. Normalmente, este usuario es un administrador de sistemas o de redes. Esta opción resulta especialmente útil para servidores de terminal, siempre que todas las notificaciones del sistema se envíen al administrador.

4.7.3 Configuración de acceso

La configuración de ESET Internet Security es una parte crucial de la política de seguridad. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Internet Security se pueden proteger mediante contraseña.



Configuración de la protección por contraseña: indique la configuración de la contraseña. Haga clic para abrir la ventana de configuración de contraseña.

Para configurar o cambiar una contraseña para proteger los parámetros de configuración, haga clic en **Definir**.

NOTA
Cuando intenta acceder a la Configuración avanzada protegida , se muestra la ventana de introducción de contraseña. Si olvida o pierde la contraseña, haga clic en la opción **Restaurar contraseña** que aparece a continuación e introduzca la dirección de correo electrónico que utilizó para registrar la licencia. ESET le enviará un mensaje de correo electrónico con el código de verificación e instrucciones sobre cómo restablecer la contraseña. Para obtener más información, haga clic aquí.

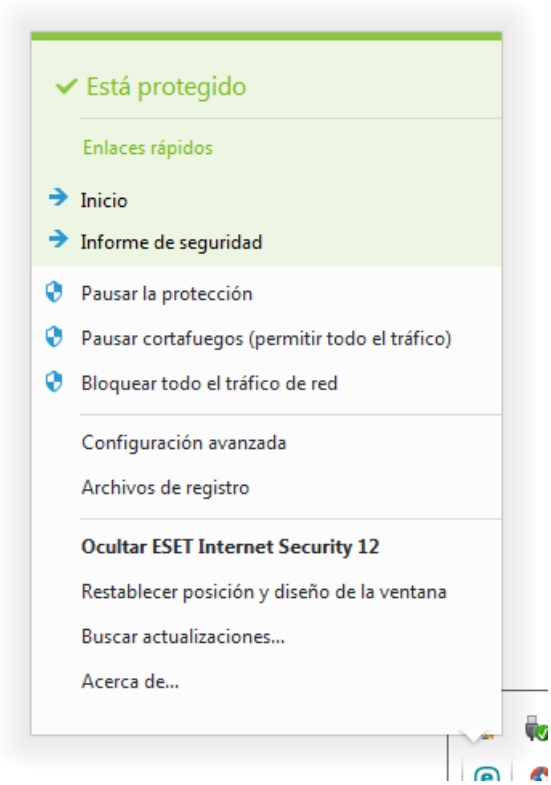
Exigir derechos de administrador completos a las cuentas de administrador limitadas: seleccione esta opción para solicitar al usuario actual (si no tiene derechos de administrador) que introduzca el nombre de usuario y la contraseña de administrador al modificar determinados parámetros del sistema (parecido al control de cuentas de usuario (UAC) en Windows Vista y Windows 7). Entre estas modificaciones se incluye la desactivación de los módulos de protección y del cortafuegos. En sistemas con Windows XP en los que no se ejecuta el UAC, los usuarios tendrán disponible la opción **Exigir derechos de administrador (sistema sin soporte UAC)**.

Solo para Windows XP:

Exigir derechos de administrador (sistema sin soporte UAC): active esta opción para que ESET Internet Security solicite las credenciales de administrador.

4.7.4 Menú del programa

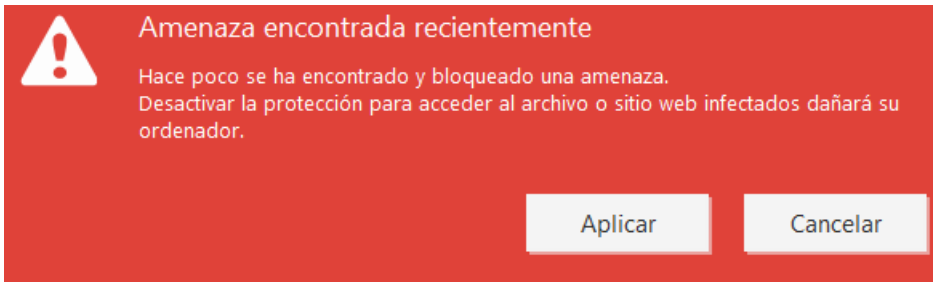
Algunas de las opciones y características de configuración más importantes están disponibles al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema.



Vínculos rápidos: muestra las partes de ESET Internet Security que se utilizan con mayor frecuencia. Puede acceder a estas secciones rápidamente desde el menú del programa.

Pausar protección: muestra el cuadro de diálogo de confirmación que desactiva la Protección antivirus y antiespía, que protege el sistema frente a ataques maliciosos al sistema mediante el control de archivos, Internet y la comunicación por correo electrónico.

En el menú desplegable **Intervalo de tiempo** se indica el período de tiempo durante el que estará desactivada la protección antivirus y antiespía.



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

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

Configuración avanzada: seleccione esta opción para acceder al árbol de **Configuración avanzada**. La configuración avanzada también se puede abrir pulsando la tecla F5 o desde **Configuración** > **Configuración avanzada**.

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

Ocultar ESET Internet Security: oculta la ventana de ESET Internet Security de la pantalla.

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

Buscar actualizaciones: inicia la actualización del motor de detección (anteriormente conocido como "base de firmas de virus) para garnatizar el nivel de protección contra el código malicioso.

Acerca de: contiene información del sistema y detalles acerca de la versión instalada de ESET Internet Security, así como de los módulos del programa instalados. Aquí también puede encontrar la fecha de expiración de la licencia e información sobre el sistema operativo y los recursos del sistema.

5. Usuario avanzado

5.1 Perfiles

El administrador de perfiles se utiliza en dos secciones de ESET Internet Security: en **Análisis del ordenador** y en **Actualización**.

Análisis del ordenador

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

Para crear un perfil nuevo, abra la ventana Configuración avanzada (F5) y haga clic en **Motor de detección** > **Análisis de malware** > **Análisis a petición** > **Lista de perfiles**. En la ventana **Administrador de perfiles** encontrará el menú desplegable **Perfil seleccionado** con los perfiles de análisis existentes y la opción para crear uno nuevo. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección Configuración de parámetros del motor ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

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

Actualización

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

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

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

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

5.2 Accesos directos del teclado

Puede utilizar los siguientes accesos directos del teclado para mejorar la navegación en su producto de ESET:

F1	abre las páginas de ayuda
F5	abre la Configuración avanzada
Flechas arriba/abajo	navegación por los elementos del producto
-	contrae los nodos del árbol de configuración avanzada
TABULADOR	mueve el cursor en una ventana

Esc	cierra el cuadro de diálogo activo
Ctrl+U	muestra información sobre la licencia (Detalles para atención al cliente)
Ctrl+R	restablece la ventana del producto al tamaño y la posición predeterminados en la pantalla

5.3 Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, *ekrn*). Cuando una aplicación se bloquea, se genera un volcado de memoria que puede ayudar a los desarrolladores a depurar y arreglar varios problemas de ESET Internet Security. Haga clic en el menú desplegable situado junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Desactivar** (predeterminada) para desactivar esta característica.
- **Mini**: registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado, pero dada la poca información que contiene, es posible que el análisis de este archivo no detecte los errores que no estén relacionados directamente con el subproceso que se estaba ejecutando cuando se produjo el problema.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.

Activar registro avanzado de la protección de la red: registrar los datos de red que pasan a través del cortafuegos en formato PCAP. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el cortafuegos.

Activar el registro avanzado del filtrado de protocolos: registrar los datos que pasan a través del motor de filtrado de protocolos en formato PCAP. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el filtrado de protocolos.

Activar registro avanzado del motor de actualización: registrar todos los eventos que se producen durante el proceso de actualización. Esto puede ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el motor de actualización.

Activar registro avanzado de Control parental: registra todos los sucesos que tienen lugar en Control parental. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el Control parental.

Activar registro avanzado de las licencias: registrar toda la comunicación del producto con el servidor de licencias.

Activar registro avanzado del motor antirrobo: registrar todos los sucesos que se produzcan en Antirrobo para permitir diagnosticar y resolver problemas.

Activar registro avanzado del motor antispam: registrar todos los sucesos que tienen lugar durante el análisis antispam. Esto puede ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el motor antispam de ESET.

Activar registro avanzado del sistema operativo: se recopilará información adicional sobre el sistema operativo, tal como los procesos en ejecución, la actividad de la CPU, las operaciones del disco, etc. Estos datos pueden ayudar a los desarrolladores a diagnosticar y corregir problemas relacionados con el producto de ESET que se ejecuta en su sistema operativo (disponible para Windows 10).

Los archivos de registro se pueden encontrar en:
C:\ProgramData\ESET\ESET Internet Security\Diagnostics en Windows Vista y versiones posteriores o en *C:\Documents and Settings\All Users\...* en versiones anteriores de Windows.

Directorio de destino: directorio en el que se genera el volcado durante el bloqueo.

Abrir la carpeta de diagnóstico: haga clic en **Abrir** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

Crear volcado de diagnóstico: haga clic en **Crear** para crear archivos de volcado de diagnóstico en el **Directorio de destino**.

5.4 Importar y exportar configuración

Puede importar o exportar el archivo de configuración .xml de ESET Internet Security del menú **Configuración**.

La importación y la exportación de un archivo de configuración son útiles cuando necesita realizar una copia de seguridad de la configuración actual de ESET Internet Security para utilizarla en otro momento. La opción de exportación de configuración también es de utilidad para los usuarios que desean utilizar su configuración preferida en varios sistemas, ya que les permite importar fácilmente el archivo *.xml* para transferir estos ajustes.

Importar la configuración es muy fácil. En la ventana principal del programa, haga clic en **Configuración** > **Importar y exportar configuración** y, a continuación, seleccione la opción **Importar configuración**. Introduzca el nombre del archivo de configuración o haga clic en el botón **...** para buscar el archivo de configuración que desea importar.

Los pasos para exportar una configuración son muy similares. En la ventana principal del programa, haga clic en **Configuración** > **Importar y exportar configuración**. Seleccione **Exportar configuración** e introduzca el nombre del archivo de configuración (por ejemplo, *export.xml*). Utilice el navegador para seleccionar la ubicación del ordenador donde desee guardar el archivo de configuración.

NOTA
Puede encontrarse con un error al exportar la configuración si no dispone de derechos suficientes para escribir el archivo exportado en el directorio especificado.

5.5 ESET SysInspector

5.5.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el ordenador a fondo y muestra los datos recopilados de forma exhaustiva. La información sobre los controladores y aplicaciones instalados, las conexiones de red o las entradas de registro importantes, por ejemplo, puede ayudarle en la investigación de un comportamiento sospechoso del sistema, ya sea debido a incompatibilidades del software o hardware o a una infección por malware.

Puede acceder a ESET SysInspector de dos formas: desde la versión integrada en las soluciones de ESET Security o descargando la versión independiente (SysInspector.exe) de forma gratuita desde el sitio web de ESET. Ambas versiones funcionan igual y tienen los mismos controles del programa. La única diferencia es cómo se administran los resultados. Las versiones independiente e integrada le permiten exportar instantáneas del sistema a un archivo *.xml* y guardarlas en el disco. Sin embargo, la versión integrada también permite almacenar las instantáneas del sistema directamente en **Herramientas** > **ESET SysInspector** (excepto ESET Remote Administrator).

Espere lo necesario mientras ESET SysInspector analiza el ordenador. Puede tardar entre 10 segundos y unos minutos en función de la configuración del hardware, el sistema operativo y el número de aplicaciones instaladas en el ordenador.

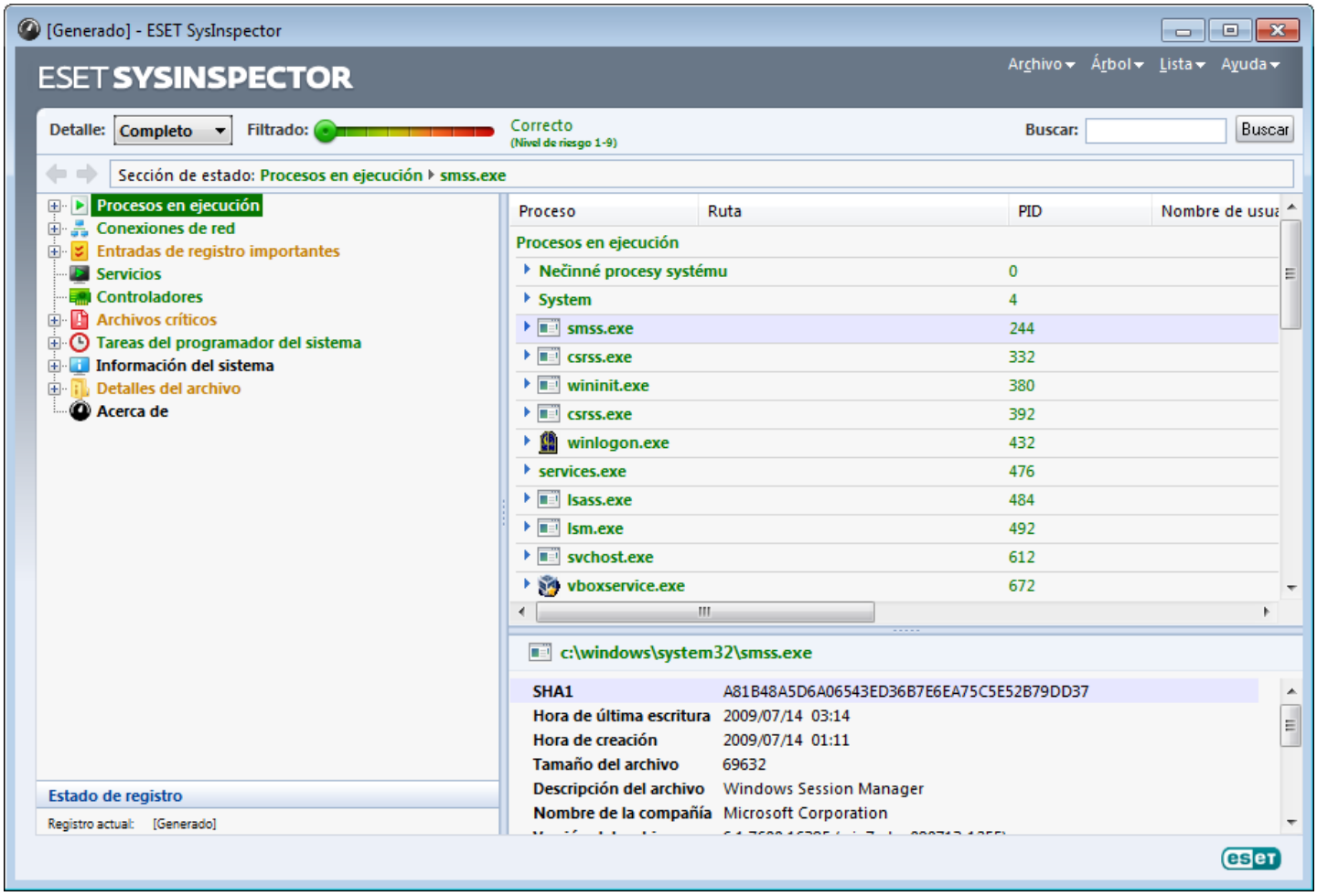
5.5.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector simplemente tiene que ejecutar el archivo *SysInspector.exe* que descargó del sitio web de ESET.

Espere mientras la aplicación examina el sistema. El proceso de inspección puede tardar varios minutos.

5.5.2 Interfaz de usuario y uso de la aplicación

Para un uso sencillo, la ventana principal del programa se divide en cuatro secciones: Controles de programa, en la parte superior de la ventana principal del programa; la ventana de navegación, situada a la izquierda; la ventana Descripción, situada a la derecha; y la ventana Detalles, situada en la parte inferior de la ventana principal. La sección Estado del registro incluye los parámetros básicos de un registro (filtro utilizado, tipo de filtro, etc.) e indica si el registro es el resultado de una comparación.



5.5.2.1 Controles de programa

Esta sección contiene la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo

Al hacer clic en **Archivo**, puede guardar el estado actual del sistema para examinarlo más tarde o abrir un registro guardado anteriormente. Para la publicación, es recomendable que genere un registro **Adecuado para su envío**. De esta forma, el registro omite la información confidencial (nombre del usuario actual, nombre del ordenador, nombre del dominio, privilegios del usuario actual, variables de entorno, etc.).

NOTA: los informes previamente almacenados de ESET SysInspector se pueden abrir arrastrándolos y colocándolos en la ventana principal del programa.

Árbol

Le permite expandir o cerrar todos los nodos, y exportar las secciones seleccionadas al script de servicio.

Lista

Contiene funciones para una navegación más sencilla por el programa y otras funciones como, por ejemplo, la búsqueda de información en línea.

Ayuda

Contiene información sobre la aplicación y sus funciones.

Detalle

Este ajuste modifica la información mostrada en la ventana principal del programa para que pueda trabajar con ella más fácilmente. En el modo "Básico", tiene acceso a información utilizada para buscar soluciones a problemas comunes de su sistema. En el modo "Medio", el programa muestra información menos utilizada. En el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado

Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Mediante el ajuste del control deslizante, puede filtrar elementos por su nivel de riesgo. Si el control deslizante se coloca en el extremo izquierdo (nivel de riesgo 1), se muestran todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos que tienen un nivel de riesgo inferior al actual y muestra solo los elementos con un nivel de sospecha superior al mostrado. Si el control deslizante se encuentra en el extremo derecho, el programa muestra únicamente los elementos dañinos conocidos.

Todos los elementos que tengan un nivel de riesgo entre 6 y 9 pueden constituir un riesgo de seguridad. Si no está utilizando una solución de seguridad de ESET, le recomendamos que analice su sistema con ESET Online Scanner cuando ESET SysInspector encuentre un elemento de este tipo. ESET Online Scanner es un servicio gratuito.

NOTA: el nivel de riesgo de un elemento se puede determinar rápidamente comparando el color del elemento con el color del control deslizante del nivel de riesgo.

Comparar

Cuando se comparan dos registros, puede elegir que se visualicen todos los elementos, solo los elementos agregados, solo los elementos eliminados y solo los elementos sustituidos.

Buscar

Esta opción se puede utilizar para buscar rápidamente un elemento específico por su nombre o parte del nombre. Los resultados de la solicitud de búsqueda aparecerán en la ventana de descripción.

Retorno

Al hacer clic en las flechas hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana Descripción. Puede utilizar la tecla Retroceso y la tecla de espacio, en lugar de hacer clic en las flechas atrás y adelante.

Sección de estado

Muestra el nodo actual en la ventana de navegación.

Importante: los elementos destacados en rojo son elementos desconocidos, motivo por el que el programa los marca como potencialmente peligrosos. Que un elemento aparezca marcado en rojo no significa que deba eliminar el archivo. Antes de eliminarlo, asegúrese de que el archivo es realmente peligroso o innecesario.

5.5.2.2 Navegación por ESET SysInspector

ESET SysInspector divide los tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional expandiendo los subnodos de cada nodo. Para abrir o contraer un nodo, haga doble clic en el nombre del nodo o haga clic en ⊞ o ⊟, junto al nombre del nodo. Cuando examine la estructura de árbol de nodos y subnodos en la ventana de navegación, puede encontrar información variada de cada nodo en la ventana de descripción. Si examina los elementos en la ventana de descripción, es posible que se muestre información adicional de cada uno de los elementos en la ventana de detalles.

A continuación se encuentran las descripciones de los nodos principales de la ventana de navegación e información relacionada en las ventanas de descripción y detalles.

Procesos en ejecución

Este nodo contiene información sobre aplicaciones y procesos que se ejecutan al generar el registro. En la ventana de descripción, puede encontrar información adicional de cada proceso como, por ejemplo, bibliotecas dinámicas utilizadas por el proceso y su ubicación en el sistema, el nombre del proveedor de la aplicación y el nivel de riesgo del archivo.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

NOTA: un sistema operativo incluye varios componentes de kernel importantes que se ejecutan constantemente y proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, dichos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por \??\. Estos símbolos optimizan el inicio previo de esos procesos; son seguros para el sistema.

Conexiones de red

La ventana de descripción contiene una lista de procesos y aplicaciones que se comunican a través de la red utilizando el protocolo seleccionado en la ventana de navegación (TCP o UDP), así como la dirección remota a la que se conecta la aplicación. También puede comprobar las direcciones IP de los servidores DNS.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

Entradas de registro importantes

Contiene una lista de entradas de registro seleccionadas que suelen estar asociadas a varios problemas del sistema, como las que especifican programas de arranque, objetos auxiliares del navegador (BHO), etc.

En la ventana de descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana de detalles.

Servicios

La ventana de descripción contiene una lista de archivos registrados como Windows Services (Servicios de Windows). En la ventana de detalles, puede consultar la forma de inicio establecida para el servicio e información específica del archivo.

Controladores

Lista de los controladores instalados en el sistema.

Archivos críticos

En la ventana de descripción se muestra el contenido de los archivos críticos relacionados con el sistema operativo Microsoft Windows.

Tareas del programador del sistema

Contiene una lista de las tareas desencadenadas por el Programador de tareas de Windows a una hora/intervalo especificado.

Información del sistema

Contiene información detallada sobre el hardware y el software, así como información sobre las variables de entorno, los derechos de usuario y los registros de eventos del sistema establecidos.

Detalles del archivo

La lista de los archivos del sistema y los archivos de la carpeta Archivos de programa importantes. Se puede encontrar información adicional específica de los archivos en las ventanas de descripción y detalles.

Acerca de

Información acerca de la versión de ESET SysInspector y la lista de los módulos de programa.

5.5.2.2.1 Accesos directos del teclado

Los accesos directos que se pueden utilizar en ESET SysInspector son:

Archivo

Ctrl+O	Abrir el registro existente
Ctrl+S	Guardar los registros creados

Generar

Ctrl+G	Generar una instantánea de estado del ordenador estándar
Ctrl+H	Generar una instantánea de estado del ordenador que también puede registrar información confidencial

Filtrado de elementos

1, O	Seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9
2	Seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9
3	Seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9
4, U	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 4 a 9
5	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9
6	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9
7, B	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9
8	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9
9	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 9
-	Disminuir el nivel de riesgo
+	Aumentar el nivel de riesgo

Ctrl+9	Modo de filtrado, mismo nivel o superior
Ctrl+0	Modo de filtrado, sólo mismo nivel

Ver

Ctrl+5	Ver por proveedor, todos los proveedores
Ctrl+6	Ver por proveedor, sólo Microsoft
Ctrl+7	Ver por proveedor, resto de proveedores
Ctrl+3	Mostrar todos los detalles
Ctrl+2	Mostrar la mitad de los detalles
Ctrl+1	Visualización básica
Retroceso	Volver un paso atrás
Espacio	Continuar con el paso siguiente
Ctrl+W	Expandir el árbol
Ctrl+Q	Contraer el árbol

Otros controles

Ctrl+T	Ir a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl+P	Mostrar la información básica de un elemento
Ctrl+A	Mostrar la información completa de un elemento
Ctrl+C	Copiar el árbol del elemento actual
Ctrl+X	Copiar elementos
Ctrl+B	Buscar información en Internet acerca de los archivos seleccionados
Ctrl+L	Abrir la carpeta en la que se encuentra el archivo seleccionado
Ctrl+R	Abrir la entrada correspondiente en el editor de registros
Ctrl+Z	Copiar una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl+F	Activar el campo de búsqueda
Ctrl+D	Cerrar los resultados de búsqueda
Ctrl+E	Ejecutar el script de servicio

Comparación

Ctrl+Alt+O	Abrir el registro original/comparativo
Ctrl+Alt+R	Cancelar la comparación
Ctrl+Alt+1	Mostrar todos los elementos
Ctrl+Alt+2	Mostrar sólo los elementos agregados, el registro incluirá los elementos presentes en el registro actual
Ctrl+Alt+3	Mostrar sólo los elementos eliminados, el registro incluirá los elementos presentes en el registro anterior
Ctrl+Alt+4	Mostrar sólo los elementos sustituidos (archivos incluidos)
Ctrl+Alt+5	Mostrar sólo las diferencias entre los registros
Ctrl+Alt+C	Mostrar la comparación
Ctrl+Alt+N	Mostrar el registro actual
Ctrl+Alt+P	Abrir el registro anterior

Varios

F1	Ver la Ayuda
Alt+F4	Cerrar el programa
Alt+Mayús+F4	Cerrar el programa sin preguntar
Ctrl+I	Estadísticas del registro

5.5.2.3 Comparar

La característica Comparar permite al usuario comparar dos registros existentes. El resultado es un conjunto de elementos no comunes a ambos registros. Esta herramienta permite realizar un seguimiento de los cambios introducidos en el sistema, una característica muy útil para la detección de código malicioso.

Una vez iniciada, la aplicación crea un nuevo registro, que aparecerá en una ventana nueva. Haga clic en **Archivo** > **Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, haga clic en **Archivo** > **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro cada vez.

La ventaja de comparar dos registros es que puede ver un registro actualmente activo y un registro guardado en un archivo. Para comparar registros, haga clic en **Archivo** > **Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en las ventanas principales del programa. El registro comparativo sólo mostrará las diferencias entre estos dos registros.

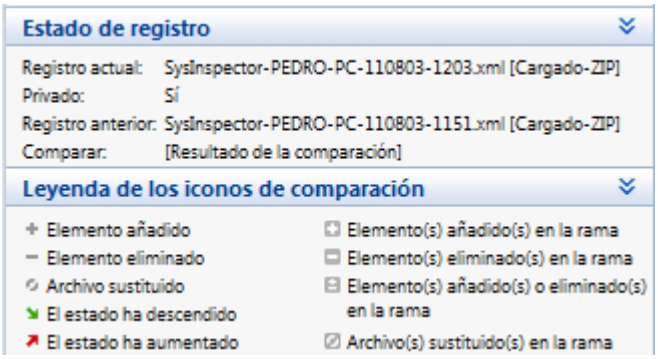
NOTA: si compara dos archivos de registro, haga clic en **Archivo** > **Guardar registro** para guardarlo como archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, se compararán automáticamente los registros que contiene.

Junto a los elementos mostrados, ESET SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

- + Nuevo valor que no se encuentra en el registro anterior.
- Sección de estructura de árbol contiene nuevos valores.
- – Valor eliminado que sólo se encuentra en el registro anterior.
- Sección de estructura de árbol contiene valores eliminados.
- Se ha cambiado un valor o archivo.
- Sección de estructura de árbol que contiene valores o archivos modificados.
- Ha disminuido el nivel de riesgo o era superior en el registro anterior.
- Ha aumentado el nivel de riesgo o era inferior en el registro anterior.

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos y muestra los nombres de los registros que se están comparando.



Se puede guardar cualquier registro comparativo en un archivo y abrirlo posteriormente.

Ejemplo

Genere y guarde un registro, en el que se recopile información original sobre el sistema, en un archivo con el nombre previo.xml. Tras realizar los cambios en el sistema, abra ESET SysInspector y permita que genere un nuevo registro. Guárdelo en un archivo con el nombre *actual.xml*.

Para realizar un seguimiento de los cambios entre estos dos registros, haga clic en **Archivo** > **Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

Se puede lograr el mismo resultado si utiliza la siguiente opción de la línea de comandos:

SysIsnpector.exe actual.xml previo.xml

5.5.3 Parámetros de la línea de comandos

ESET SysInspector admite la generación de informes desde la línea de comandos con estos parámetros:

/gen	genera un registro directamente desde la línea de comandos, sin ejecutar la interfaz gráfica.
/privacy	genera un registro omitiendo la información personal.
/zip	guarda el registro obtenido en un archivo comprimido zip.
/silent	cancela la ventana de progreso cuando se genera un registro desde la línea de comandos.
/blank	inicia ESET SysInspector sin generar o cargar un registro.

Ejemplos

Uso:
`Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]`

Para cargar un registro determinado directamente en el navegador, utilice: *SysInspector.exe .\clientlog.xml*
Para generar un registro desde la línea de comandos, utilice: *SysInspector.exe /gen=.\mynewlog.xml*
Para generar un registro que no incluya la información confidencial directamente como archivo comprimido, utilice: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Para comparar dos archivos de registro y examinar las diferencias, utilice: *SysInspector.exe new.xml old.xml*

NOTA: si el nombre del archivo o la carpeta contiene un espacio, debe escribirse entre comillas.

5.5.4 Script de servicio

El script de servicio es una herramienta que ofrece ayuda a los clientes que utilizan ESET SysInspector eliminando de forma sencilla objetos no deseados del sistema.

El script de servicio permite al usuario exportar el registro completo de ESET SysInspector o únicamente las partes seleccionadas. Tras la exportación, puede marcar los objetos no deseados que desee eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es útil para usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden provocar daños en el sistema operativo.

Ejemplo

Si sospecha que el ordenador está infectado por un virus que el antivirus no detecta, siga estas instrucciones:

1. Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
2. Seleccione el primer elemento de la sección que se encuentra a la izquierda (en la estructura de árbol), pulse Mayús y seleccione el último elemento para marcarlos todos.
3. Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio**.
4. Los objetos seleccionados se exportarán a un nuevo registro.
5. Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de no marcar ningún archivo/objeto importante del sistema operativo.
6. Abra ESET SysInspector, haga clic en **Archivo** > **Ejecutar script de servicio** e introduzca la ruta del script.
7. Haga clic en **Aceptar** para ejecutar el script.

5.5.4.1 Generación de scripts de servicio

Para generar un script de servicio, haga clic con el botón derecho del ratón en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione **Exportar todas las secciones al script de servicio** o **Exportar secciones seleccionadas al script de servicio**.

NOTA: cuando se comparan dos registros, el script de servicio no se puede exportar.

5.5.4.2 Estructura del script de servicio

En la primera línea del encabezado del script encontrará información sobre la versión del motor (ev), la versión de la interfaz gráfica de usuario (gv) y la versión del registro (lv). Puede utilizar estos datos para realizar un seguimiento de los posibles cambios del archivo .xml que genere el script y evitar las incoherencias durante la ejecución. Esta parte del script no se debe modificar.

El resto del archivo se divide en secciones, donde los elementos se pueden modificar (indique los que procesará el script). Para marcar los elementos que desea procesar, sustituya el carácter "-" situado delante de un elemento por el carácter "+". En el script, las secciones se separan mediante una línea vacía. Cada sección tiene un número y un título.

01) Running processes (Procesos en ejecución)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

En este ejemplo se ha seleccionado (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el script.

02) Loaded modules (Módulos cargados)

En esta sección se enumeran los módulos del sistema que se utilizan actualmente.

Ejemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

En este ejemplo, se marcó el módulo khbekhb.dll con el signo "+". Cuando se ejecute, el script reconocerá los procesos mediante el módulo específico y los finalizará.

03) TCP connections (Conexiones TCP)

En esta sección se incluye información sobre las conexiones TCP existentes.

Ejemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445
(microsoft-ds), owner: System
[...]
```

Cuando se ejecute, el script localizará al propietario del socket en las conexiones TCP marcadas y detendrá el socket, liberando así recursos del sistema.

04) UDP endpoints (Puntos finales UDP)

En esta sección se incluye información sobre los puntos finales UDP existentes.

Ejemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Cuando se ejecute, el script aislará al propietario del socket en los puntos finales UDP marcados y detendrá el socket.

05) DNS server entries (Entradas del servidor DNS)

En esta sección se proporciona información sobre la configuración actual del servidor DNS.

Ejemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Las entradas marcadas del servidor DNS se eliminarán al ejecutar el script.

06) Important registry entries (Entradas de registro importantes)

En esta sección se proporciona información sobre las entradas de registro importantes.

Ejemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:
\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Cuando se ejecute el script, las entradas marcadas se eliminarán, se reducirán a valores de 0 bytes o se restablecerán en sus valores predeterminados. La acción realizada en cada entrada depende de su categoría y del valor de la clave en el registro específico.

07) Services (Servicios)

En esta sección se enumeran los servicios registrados en el sistema.

Ejemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe,
state: Running, startup: Automatic
- Name: Application Experience Service, exe path: c:
\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:
\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]
```

Cuando se ejecute el script, los servicios marcados y los servicios dependientes se detendrán y desinstalarán.

08) Drivers (Controladores)

En esta sección se enumeran los controladores instalados.

Ejemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys,
state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:
\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Cuando se ejecuta el script, los controladores seleccionados se detendrán. Tenga en cuenta que algunos controladores no permiten su detención.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos que son críticos para el correcto funcionamiento del sistema operativo.

Ejemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

10) Tareas programadas

Esta sección contiene información sobre las tareas programadas.

Ejemplo:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:
\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 Ejecución de scripts de servicio

Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de ESET SysInspector, con la opción **Ejecutar script de servicio** del menú Archivo. Cuando abra un script, el programa mostrará el mensaje siguiente: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

Una ventana de diálogo confirmará que el script se ha ejecutado correctamente.

Si el script no se puede procesar por completo, se mostrará una ventana de diálogo con el mensaje siguiente: **El script de servicio se ejecutó parcialmente. ¿Desea ver el informe de errores?** Seleccione **Sí** para ver un informe de errores completo con todas las operaciones que no se ejecutaron.

Si no se reconoce el script, aparece una ventana de diálogo con el mensaje siguiente: **No se ha firmado el script de servicio seleccionado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del ordenador. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta inconsistencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.). Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nuevo.

5.5.5 Preguntas frecuentes

¿Es necesario contar con privilegios de administrador para ejecutar ESET SysInspector?

Aunque ESET SysInspector no requiere privilegios de administrador para su ejecución, sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario normal o restringido, se recopilará menor cantidad de información acerca de su entorno operativo.

¿ESET SysInspector crea archivos de registro?

ESET SysInspector puede crear un archivo de registro de la configuración de su ordenador. Para guardar uno, haga clic en **Archivo** > **Guardar registro** en la ventana principal del programa. Los registros se guardan con formato XML. De forma predeterminada, los archivos se guardan en el directorio *%USERPROFILE%**Mis documentos*\, con una convención de nomenclatura del tipo "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Si lo desea, puede modificar tanto la ubicación como el nombre del archivo de registro antes de guardarlo.

¿Cómo puedo ver el contenido del archivo de registro de ESET SysInspector?

Para visualizar un archivo de registro creado por ESET SysInspector, ejecute la aplicación y haga clic en **Archivo** > **Abrir registro** en la ventana principal del programa. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, le recomendamos que cree un acceso directo al archivo SYSINSPECTOR.EXE en su escritorio. Para ver los archivos de registro, arrástrelos y suéltelos en ese acceso directo. Por razones de seguridad, es posible que Windows Vista/7 no permita la acción de arrastrar y soltar entre ventanas que cuentan con permisos de seguridad diferentes.

¿Existe alguna especificación disponible para el formato del archivo de registro? ¿Y algún conjunto de herramientas para el desarrollo de aplicaciones (SDK)?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas para el desarrollo de aplicaciones, ya que el programa se encuentra aún en fase de desarrollo. Una vez que se haya lanzado, podremos proporcionar estos elementos en función de la demanda y los comentarios por parte de los clientes.

¿Cómo evalúa ESET SysInspector el riesgo que plantea un objeto en particular?

Generalmente, ESET SysInspector asigna un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para esto, utiliza una serie de reglas heurísticas que examinan las características de cada uno de ellos y después estima el 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). En el panel de navegación que se encuentra a la izquierda, las secciones estarán coloreadas según el nivel máximo de peligrosidad que presente un objeto en su interior.

El nivel de riesgo "6: desconocido (en color rojo)", ¿significa que un objeto es peligroso?

Las evaluaciones de ESET SysInspector no garantizan que un objeto sea malicioso. Esta determinación deberá confirmarla un experto en seguridad informática. ESET SysInspector está diseñado para proporcionar una guía rápida a estos expertos, con la finalidad de que conozcan los objetos que deberían examinar en un sistema en busca de algún comportamiento inusual.

¿Por qué ESET SysInspector se conecta a Internet cuando se ejecuta?

Como muchas otras aplicaciones, ESET SysInspector contiene una firma digital que actúa a modo de "certificado". Esta firma sirve para garantizar que ESET ha desarrollado la aplicación y que no se ha alterado. Para comprobar la autenticidad del certificado, el sistema operativo debe contactar con la autoridad certificadora, que verificará la identidad del desarrollador de la aplicación. Este es un comportamiento normal para todos los programas firmados digitalmente que se ejecutan en Microsoft Windows.

¿En qué consiste la tecnología AntiStealth?

La tecnología AntiStealth proporciona un método efectivo de detección de rootkits.

Si el código malicioso que se comporta como un rootkit ataca al sistema, el usuario se expone a pérdidas o robo de información. Si no se dispone de una herramienta antirootkit especial, es prácticamente imposible detectar los rootkits.

¿Por qué a veces hay archivos con la marca "Firmado por MS" que, al mismo tiempo, tienen una entrada de "Nombre de compañía" diferente?

Al intentar identificar la firma digital de un archivo ejecutable, ESET SysInspector comprueba en primer lugar si el archivo contiene una firma digital integrada. Si se encuentra una firma digital, el archivo se validará utilizando dicha información. Si no se encuentra una firma digital, ESI comienza a buscar el archivo CAT correspondiente (Catálogo de seguridad: *%systemroot%\system32\catroot*) que contiene información sobre el archivo ejecutable procesado. Si se encuentra el archivo CAT relevante, la firma digital de dicho archivo CAT será la que se aplique en el proceso de validación del archivo ejecutable.

Esa es la razón por la cual a veces hay archivos marcados como "Firmado por MS", pero que tienen una entrada "Nombre de compañía" diferente.

Ejemplo:

Windows 2000 incluye la aplicación HyperTerminal, que se encuentra en *C:\Archivos de programa\Windows NT*. El archivo ejecutable de la aplicación principal no está firmado digitalmente; sin embargo, ESET SysInspector lo marca como archivo firmado por Microsoft. La razón es la referencia que aparece en *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que lleva a *C:\Archivos de programa\Windows NT\hypertrm.exe* (archivo ejecutable principal de la aplicación HyperTerminal), y *sp4.cat* está digitalmente firmado por Microsoft.

5.6 Línea de comandos

El módulo antivirus de ESET Internet Security se puede iniciar manualmente a través de la línea de comandos, con el comando "ecls" o con un archivo por lotes ("bat"). Uso del análisis de línea de comandos ESET:

```
ecls [OPTIONS..] FILES..
```

Los siguientes parámetros y modificadores se pueden utilizar al ejecutar el análisis a petición desde la línea de comandos:

Opciones

/base-dir=CARPETA	cargar módulos desde una CARPETA
/quar-dir=CARPETA	CARPETA de cuarentena
/exclude=MÁSCARA	excluir del análisis los archivos que cumplan MÁSCARA
/subdir	analizar subcarpetas (predeterminado)
/no-subdir	no analizar subcarpetas
/max-subdir-level=NIVEL	máximo nivel de anidamiento para subcarpetas a analizar
/symlink	seguir enlaces simbólicos (predeterminado)
/no-symlink	omitir enlaces simbólicos
/ads	analizar ADS (predeterminado)
/no-ads	no analizar ADS
/log-file=ARCHIVO	registrar salida en ARCHIVO
/log-rewrite	sobrescribir el archivo de salida (predeterminado – agregar)
/log-console	enviar registro a la consola (predeterminado)
/no-log-console	no enviar registro a la consola
/log-all	registrar también los archivos sin infectar
/no-log-all	no registrar archivos sin infectar (predeterminado)
/aind	mostrar indicador de actividad
/auto	analizar y desinfectar automáticamente todos los discos locales

Opciones de análisis

/files	analizar archivos (predeterminado)
/no-files	no analizar archivos
/memory	analizar memoria
/boots	analizar sectores de inicio
/no-boots	no analizar sectores de inicio (predeterminado)
/arch	analizar archivos comprimidos (predeterminado)
/no-arch	no analizar archivos
/max-obj-size=TAMAÑO	analizar solo archivos menores de TAMAÑO megabytes (predeterminado 0 = ilimitado)
/max-arch-level=NIVEL	máxima profundidad de anidamiento para archivos comprimidos (archivos anidados) a analizar
/scan-timeout=LÍMITE	analizar archivos comprimidos durante LÍMITE segundos como máximo
/max-arch-size=TAMAÑO	analizar los archivos dentro de un archivo comprimido solo si su tamaño es inferior a TAMAÑO (predeterminado 0 = ilimitado)
/max-sfx-size=TAMAÑO	analizar solo los archivos en un archivo comprimido de autoextracción si su tamaño es inferior a TAMAÑO megabytes (predeterminado 0 = ilimitado)
/mail	analizar archivos de correo (predeterminado)
/no-mail	no analizar archivos de correo
/mailbox	analizar buzones de correo (predeterminado)
/no-mailbox	no analizar buzones de correo
/sfx	analizar archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no analizar archivos comprimidos de autoextracción
/rtp	analizar empaquetadores en tiempo real (predeterminado)
/no-rtp	no analizar empaquetadores en tiempo real
/unsafe	analizar en busca de aplicaciones potencialmente peligrosas

/no-unsafe	no analizar en busca de aplicaciones potencialmente peligrosas
/unwanted	analizar en busca de aplicaciones potencialmente indeseables
/no-unwanted	no analizar en busca de aplicaciones potencialmente indeseables (predeterminado)
/suspicious	analizar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no analizar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	activar heurística (predeterminado)
/no-heur	desactivar heurística
/adv-heur	activar heurística avanzada (predeterminado)
/no-adv-heur	desactivar heurística avanzada
/ext=EXTENSIONES	analizar solo EXTENSIONES separadas por dos puntos
/ext-exclude=EXTENSIONES	excluir EXTENSIONES del análisis, separándolas por el signo ":" (dos puntos)
/clean-mode=MODO	utilizar el MODO desinfección para objetos infectados Están disponibles las opciones siguientes: • **none** (ninguno): no se realiza la desinfección automática. • **standard** (estándar, predeterminado): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados. • **strict** (estricto): ecls.exe intenta desinfectar o eliminar automáticamente los archivos infectados sin la intervención del usuario (no verá una notificación antes de que se eliminen los archivos). • **rigorous** (riguroso): ecls.exe elimina los archivos sin intentar desinfectarlos, sea cual sea el archivo. • **delete** (eliminar): ecls.exe elimina los archivos sin intentar desinfectarlos, pero no elimina archivos delicados como los archivos del sistema de Windows.
/quarantine	copiar archivos infectados (si se han desinfectado) a la carpeta Cuarentena (complementa la acción realizada durante la desinfección)
/no-quarantine	no copiar archivos infectados a cuarentena

Opciones generales

/help	mostrar ayuda y salir
/version	mostrar información sobre la versión y salir
/preserve-time	conservar hora del último acceso

Códigos de salida

0	no se ha detectado ninguna amenaza
1	amenaza detectada y eliminada
10	no se han podido analizar todos los archivos (podrían ser amenazas)
50	amenaza detectada
100	error

NOTA

Los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por lo tanto, puede estar infectado.

6. Preguntas habituales

Este capítulo abarca algunas de las preguntas más frecuentes y los problemas encontrados. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

- Cómo actualizar ESET Internet Security
- Cómo eliminar un virus de mi PC
- Cómo permitir la comunicación para una aplicación determinada
- Cómo activar el control parental para una cuenta
- Cómo crear una tarea nueva en el Planificador de tareas

Cómo programar una tarea de análisis (cada 24 horas)

Si su problema no aparece en las páginas de ayuda anteriores, pruebe a buscar en las páginas de ayuda de ESET Internet Security.

Si no encuentra la solución a su problema o consulta en las páginas de ayuda, puede visitar nuestra base de conocimientos en línea de ESET, que se actualiza periódicamente. A continuación se incluyen vínculos a nuestros artículos de la base de conocimientos más populares para ayudarle a solucionar problemas comunes:

- He recibido un error de activación al instalar mi producto ESET. ¿Qué significa?
- Activar mi producto doméstico ESET para Windows con mi nombre de usuario, contraseña o clave de licencia
- Desinstalar o reinstalar mi producto doméstico ESET
- He recibido el mensaje de que mi instalación de ESET ha finalizado prematuramente
- ¿Qué debo hacer después de renovar mi licencia? (usuarios domésticos)
- ¿Qué sucede si cambio mi dirección de correo electrónico?

Cómo iniciar Windows en Modo seguro o en Modo seguro con funciones de red

Si lo necesita, puede ponerse en contacto con el Servicio de atención al cliente para hacerle llegar sus preguntas o problemas. Puede encontrar el formulario de contacto en la ficha **Ayuda y asistencia técnica** de ESET Internet Security.

6.1 Cómo actualizar ESET Internet Security

ESET Internet Security se puede actualizar de forma manual o automática. Para activar la actualización, haga clic en **Actualización** en la ventana principal del programa y, a continuación, haga clic en **Buscar actualizaciones**.

Los parámetros de instalación predeterminados crean una tarea de actualización automática que se lleva a cabo cada hora. Si es necesario cambiar el intervalo, vaya a **Herramientas** > **Planificador de tareas** (para obtener más información sobre el Planificador de tareas, haga clic aquí).

6.2 Cómo eliminar un virus de mi PC

Si su ordenador muestra señales de una infección por código malicioso, por ejemplo, es más lento, se bloquea a menudo, etc., se recomienda que haga lo siguiente:

1. En la ventana principal del programa, haga clic en **Análisis del ordenador**.
2. Haga clic en **Análisis del ordenador** para iniciar el análisis del sistema.
3. Una vez finalizado el análisis, revise el registro con el número de archivos analizados, infectados y desinfectados.
4. Si solo desea analizar determinadas partes del disco, haga clic en **Análisis personalizado** y especifique los objetos que desee analizar en busca de virus.

Si desea información adicional, visite nuestro artículo de la base de conocimientos de ESET que se actualiza periódicamente.

6.3 Cómo permitir la comunicación para una aplicación determinada

Si se detecta una nueva conexión en el modo interactivo y no hay ninguna regla que coincida, se le solicitará que confirme o rechace la conexión. Si desea que ESET Internet Security lleve a cabo la misma acción cada vez que la aplicación intente establecer una conexión, active la casilla de verificación **Recordar acción (crear regla)**.

En la ventana de configuración del cortafuegos situada en **Red** > **Cortafuegos** > **Reglas y zonas** > **Configuración**, puede crear reglas del cortafuegos para aplicaciones antes de que ESET Internet Security las detecte. Para que la ficha **Reglas** esté disponible en **Configuración de reglas y zonas**, el modo de filtrado del cortafuegos debe estar establecido en el modo interactivo.

En la pestaña **General**, escriba el nombre, la dirección y el protocolo de comunicación de la regla. Esta ventana le permite definir la acción que se debe realizar cuando se aplica la regla.

Inserte la ruta al archivo ejecutable de la aplicación y al puerto de comunicación local en la pestaña **Local**. Haga clic en la pestaña **Remoto** para introducir la dirección y el puerto remotos (si corresponde). La regla que se acaba de crear se aplicará en cuanto la aplicación intente comunicarse de nuevo.

6.4 Cómo activar el control parental para una cuenta

Para activar el control parental para una cuenta de usuario específica, siga los pasos que se indican a continuación:

1. El control parental está desactivado de forma predeterminada en ESET Internet Security. Hay dos métodos para activar el control parental:
   - Haga clic en  en **Configuración** > **Herramientas de seguridad** > **Control parental** en la ventana principal del programa y cambie el estado del control parental a activado.
   - Pulse F5 para acceder al árbol **Configuración avanzada**, desplácese hasta **Web y correo electrónico** > **Control parental** y, a continuación, active el interruptor junto a **Integrar en el sistema**.
2. Haga clic en **Configuración** > **Herramientas de seguridad** > **Control parental** en la ventana principal del programa. Aunque aparezca **Activado** junto a **Control parental**, debe configurarlo para la cuenta deseada haciendo clic en **Proteger cuenta infantil** o **Cuenta paterna**. En la siguiente ventana, seleccione la fecha de nacimiento para determinar el nivel de acceso y las páginas web recomendadas según la edad. El control parental ahora estará activado en esa cuenta de 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 ficha Categorías. Para permitir o bloquear páginas web personalizadas que no concuerdan con ninguna categoría, haga clic en la ficha Excepciones.

6.5 Cómo crear una tarea nueva en el Planificador de tareas

Para crear una tarea nueva en **Herramientas** > **Más herramientas** > **Tareas programadas**, haga clic en **Agregar** o haga clic con el botón derecho y seleccione **Agregar...** en el menú contextual. Están disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear una instantánea de estado del equipo**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Actualización**: programa una tarea de actualización mediante la actualización de los módulos.

La **actualización** es una de las tareas programadas más frecuentes, por lo que a continuación explicaremos cómo se agrega una nueva tarea de actualización:

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Introduzca el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Están disponibles las opciones siguientes: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición.** Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las opciones siguientes:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución (horas)**)

En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. Aquí puede definir los perfiles principal y alternativo. El perfil alternativo se utiliza cuando la tarea no se puede completar con el perfil principal. Haga clic en **Finalizar** para confirmar la operación; la nueva tarea se agregará a la lista de tareas programadas actualmente.

6.6 Cómo programar un análisis del ordenador semanal

Para programar una tarea periódica, abra la ventana principal del programa y haga clic en **Herramientas** > **Más herramientas** > **Tareas programadas**. A continuación, se proporcionan las instrucciones básicas para programar una tarea que analice los discos locales cada 24 horas. Consulte el artículo de nuestra Base de conocimiento para ver instrucciones más detalladas.

Para programar una tarea:

1. Haga clic en **Agregar** en la pantalla principal del Planificador de tareas.
2. Seleccione **Análisis de estado inactivo** en el menú desplegable.
3. Escriba un nombre para la tarea y seleccione **Semanalmente** para la frecuencia de la tarea.
4. Establezca el día y la hora de ejecución de la tarea.
5. Seleccione **Ejecutar la tarea lo antes posible** para realizar la tarea más tarde si no se ejecuta a la hora programada por cualquier motivo (por ejemplo, si el ordenador estaba apagado).
6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.
7. En el menú desplegable **Objetos**, seleccione **Discos locales**.
8. Haga clic en **Finalizar** para aplicar la tarea.

6.7 Cómo desbloquear la Configuración avanzada

Cuando intenta acceder a la Configuración avanzada protegida, se muestra la ventana de introducción de contraseña. Si olvida o pierde la contraseña, haga clic en la opción **Restaurar contraseña** que aparece a continuación e introduzca la dirección de correo electrónico que utilizó para registrar la licencia. ESET le enviará un mensaje de correo electrónico con el código de verificación. Introduzca el código de verificación y, a continuación, escriba y confirme la nueva contraseña. El código de verificación tiene una validez de 7 días.

También puede **restaurar la contraseña desde su cuenta de my.eset.com**. Utilice esta opción si la licencia está asociada a su Administrador de licencias de ESET.

Si no recuerda su dirección de correo electrónico, haga clic en **No sé cuál es mi dirección de correo electrónico** y se le redirigirá al sitio web de ESET para que pueda ponerse en contacto rápidamente con el departamento de Atención al cliente.

Generar código para atención al cliente: esta opción generará el código que se debe proporcionar a Atención al cliente. Copie el código proporcionado por Atención al cliente y haga clic en **Tengo un código de verificación**. Escriba el código de verificación y, a continuación, escriba la nueva contraseña y su confirmación. El código de verificación tiene una validez de 7 días.

Para obtener más información detallada, lea la Base de conocimiento ESET.