

ESET Cyber Security Pro

Manual de usuario

[Haga clic aquí para ver la versión de la Ayuda de este documento](#)

Copyright ©2024 de ESET, spol. s r.o.

ESET Cyber Security Pro está desarrollado por ESET, spol. s r.o.

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

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación ni transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de aplicación descrito sin previo aviso.

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

REV. 12/04/2024

1 ESET Cyber Security Pro	1
1.1 Novedades de la versión 6	1
1.2 Requisitos del sistema	1
2 Instalación	2
2.1 Instalación típica	2
2.2 Instalación personalizada	4
2.3 Permitir las extensiones del sistema	5
2.4 Permitir acceso total al disco	6
3 Activación del producto	6
4 Desinstalación	7
5 Información general básica	7
5.1 Accesos directos del teclado	7
5.2 Comprobación del estado de protección	8
5.3 Qué hacer si el programa no funciona correctamente	8
6 Protección del ordenador	9
6.1 Protección antivirus y antispyware	9
6.1 General	9
6.1 Exclusiones	9
6.1 Protección del sistema	10
6.1 Protección del sistema de archivos en tiempo real	10
6.1 Opciones avanzadas	11
6.1 Modificación de la configuración de protección en tiempo real	11
6.1 Comprobación de la protección en tiempo real	11
6.1 ¿Qué debo hacer si la protección en tiempo real no funciona?	12
6.1 Análisis del ordenador a petición	12
6.1 Tipo de análisis	13
6.1 Análisis estándar	13
6.1 Análisis personalizado	13
6.1 Objetos de análisis	14
6.1 Perfiles de análisis	14
6.1 Configuración de parámetros del motor ThreatSense	15
6.1 Objetos	16
6.1 Opciones	16
6.1 Desinfección	16
6.1 Exclusiones	17
6.1 Límites	17
6.1 Otros	18
6.1 Detección de una amenaza	18
6.2 Análisis y bloqueo de medios extraíbles	19
7 Antiphishing	20
8 Cortafuegos	20
8.1 Modos de filtrado	21
8.2 Reglas del cortafuegos	21
8.2 Creación de reglas nuevas	22
8.3 Zonas del cortafuegos	22
8.4 Perfiles del cortafuegos	22
8.5 Registros del cortafuegos	23
9 Protección de web y correo electrónico	23
9.1 Protección web	24
9.1 Puertos	24

9.1 Listas de URL	24
9.2 Protección del correo electrónico	24
9.2 Comprobación del protocolo POP3	25
9.2 Comprobación del protocolo IMAP	25
10 Control parental	26
11 Actualización	26
11.1 Configuración de actualizaciones	27
11.1 Opciones avanzadas	27
11.2 Cómo crear tareas de actualización	28
11.3 Actualización de ESET Cyber Security Pro a una nueva versión	28
11.4 Actualizaciones del sistema	28
12 Herramientas	29
12.1 Archivos de registro	29
12.1 Mantenimiento de registros	30
12.1 Filtrado de registros	31
12.2 Planificador de tareas	31
12.2 Creación de nuevas tareas	32
12.2 Análisis como propietario de un directorio	33
12.2 Creación de tareas definidas por el usuario	34
12.3 Cuarentena	34
12.3 Puesta de archivos en cuarentena	35
12.3 Restauración de archivos de cuarentena	35
12.3 Envío de un archivo de cuarentena	35
12.4 Procesos en ejecución	35
12.5 Conexiones de red	36
12.6 Live Grid	36
12.6 Configuración de Live Grid	37
12.7 Enviar muestra para el análisis	37
13 Interfaz de usuario	38
13.1 Alertas y notificaciones	39
13.1 Mostrar alertas	39
13.1 Estados de protección	39
13.2 Privilegios	40
13.3 Menú contextual	40
13.4 Importar y exportar configuración	41
13.5 Servidor Proxy	42
14 Acuerdo de licencia para el usuario final	42
15 Política de privacidad	49

ESET Cyber Security Pro

ESET Cyber Security Pro representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense®, combinada con la protección del cliente de correo electrónico, el cortafuegos y el control parental, protege su ordenador con rapidez y precisión. Estas características lo convierten en un sistema inteligente que está constantemente en alerta defendiendo su ordenador frente a ataques y software malicioso.

ESET Cyber Security Pro es una solución de seguridad integral que nació tras un gran esfuerzo por combinar el nivel máximo de protección con un impacto mínimo en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial que componen ESET Cyber Security Pro son capaces de eliminar proactivamente la infiltración de virus, gusanos, troyanos, spyware, adware, rootkits y otros ataques que tienen su origen en Internet sin reducir el rendimiento del sistema.

Novedades de la versión 6

La versión 6 de ESET Cyber Security Pro introduce las siguientes actualizaciones y mejoras:

- **Compatibilidad con arquitecturas de 64 bits**
- **Anti-Phishing:** impide que los sitios web falsos disfrazados como sitios de confianza obtengan sus datos personales.
- **Actualizaciones del sistema:** la versión 6 de ESET Cyber Security Pro incorpora diversas correcciones y mejoras, incluidas las notificaciones de las actualizaciones del sistema operativo. Para obtener más información sobre este tema, consulte el apartado [Actualizaciones del sistema](#).
- **Estados de protección:** oculta las notificaciones de la pantalla Estado de protección (p. ej. *Protección del cliente de correo electrónico desactivada* o *Es necesario reiniciar el ordenador*).
- **Medios que se analizarán:** se pueden excluir determinados tipos de soportes del análisis en tiempo real (unidades locales, medios extraíbles, medios de red).
- **Conexiones de red:** muestra las conexiones de red de su ordenador y le permite crear reglas para ellas.

Para ver información detallada sobre las nuevas características de ESET Cyber Security Pro, lea el siguiente [artículo de la base de conocimientos de ESET](#):

Requisitos del sistema

Para disfrutar de un funcionamiento óptimo de ESET Cyber Security Pro, el sistema debería cumplir con los siguientes requisitos de hardware y software:

	Requisitos del sistema:
Arquitectura de procesador	Intel 64-bit, M1, M2
Sistema operativo	macOS 10.12 y posterior
Memoria	300 MB
Espacio libre en disco	200 MB



Además de la compatibilidad con Intel existente, las versiones 6.10.900.0 y posteriores de ESET Cyber Security Pro admiten los chips Apple M1 y M2 con Rosetta 2

Instalación

Antes de iniciar el proceso de instalación, cierre todos los programas que estén abiertos en el ordenador. ESET Cyber Security Pro contiene componentes que podrían entrar en conflicto con otros programas antivirus que ya estén instalados en el ordenador. ESET le recomienda encarecidamente que elimine los demás programas antivirus para evitar posibles problemas.

Para iniciar el asistente de instalación, realice una de estas acciones:

- Si va a realizar la instalación desde un archivo descargado del sitio web de ESET, abra el archivo y haga doble clic en el icono **Instalar**.
- Si va a realizar la instalación desde el CD o DVD, insértelo en el ordenador, ábralo desde el escritorio o la ventana del **Finder** y haga doble clic en el icono **Instalar**.



El asistente de instalación le guiará por el resto del proceso de configuración básica. En la fase inicial, el instalador comprueba automáticamente la existencia de una versión del producto más reciente en Internet. Si la encuentra, se le ofrecerá la opción de descargar la versión más reciente antes de proceder con la instalación.

Tras aceptar el acuerdo de licencia de usuario final, tendrá que seleccionar uno de los siguientes modos de instalación:

- [Instalación típica](#)
- [Instalación personalizada](#)

Instalación típica

El modo de instalación típica incluye opciones de configuración que son adecuadas para la mayoría de los usuarios. Esta configuración proporciona una seguridad máxima junto con un excelente rendimiento del sistema.

La instalación típica es la opción predeterminada y se recomienda cuando no es necesaria una configuración específica.

1. En la ventana de **ESET LiveGrid**, seleccione la opción que desee y haga clic en **Continuar**. Si más adelante decide que desea cambiar esta configuración, podrá hacerlo mediante la **Configuración de LiveGrid**. Si desea obtener más información sobre ESET LiveGrid, [visite nuestro glosario](#).
2. En la ventana **Aplicaciones potencialmente indeseables**, seleccione la opción que prefiera (consulte [¿Qué es una aplicación potencialmente indeseable?](#)) y haga clic en **Continuar**. Si más adelante decide que desea cambiar esta configuración, utilice **Configuración avanzada**.
3. Haga clic en **Instalar**. Si se le solicita que introduzca la contraseña de macOS, introdúzcala y haga clic en **Instalar software**.

Tras la instalación de ESET Cyber Security Pro:

macOS Big Sur (11)

1. [Permita las extensiones del sistema](#).
2. [Permitir acceso total al disco](#).
3. Permita que ESET añada configuraciones de proxy. Recibirá la siguiente notificación: "ESET Cyber Security Pro" **desea agregar configuraciones de proxy**. Cuando reciba esta notificación, haga clic en **Permitir**. Si hace clic en **No permitir**, la Protección de acceso a la web no funcionará.

[macOS 10.15 y versiones anteriores](#)

1. En macOS 10.13 y posteriores, el sistema mostrará la notificación **Extensión del sistema bloqueada** y la notificación **Su ordenador no está protegido** de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro tendrá que permitir las extensiones del kernel en el dispositivo. Para permitir las extensiones del kernel en su dispositivo, diríjase a **Preferencias del Sistema > Seguridad y privacidad** y haga clic en **Permitir** para permitir el software del sistema del desarrollador **ESET, spol. s.r.o.** Para obtener información más detallada, visite este [artículo de la Base de conocimiento](#).
2. En macOS 10.14 y posteriores recibirá la notificación **Su ordenador está protegido parcialmente** de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro, tendrá que permitir **Acceso total al disco** a ESET Cyber Security Pro. Haga clic en **Abrir Preferencias del Sistema > Seguridad y privacidad**. Diríjase a la ficha **Privacidad** y marque la opción **Acceso total al disco**. Haga clic en el icono para activar la edición. Haga clic en el signo más y seleccione la aplicación ESET Cyber Security Pro. Su ordenador mostrará una notificación de reinicio del ordenador. Haga clic en **Más tarde**. No reinicie el ordenador ahora. Haga clic en **Iniciar de nuevo** en la ventana de notificación de ESET Cyber Security Pro o reinicie el ordenador. Para obtener información más detallada, visite este [artículo de la Base de conocimiento](#).

Después de instalar ESET Cyber Security Pro, debe realizar un análisis del ordenador para comprobar si existe código malicioso. En la ventana principal del programa, haga clic en **Análisis inteligente > Análisis estándar**. Para obtener más información sobre los análisis del ordenador a petición, consulte el apartado [Análisis del ordenador a petición](#).

Instalación personalizada

El modo de instalación personalizada está diseñado para usuarios con experiencia que quieran modificar la configuración avanzada durante el proceso de instalación.

- **Servidor Proxy**

Si utiliza un servidor proxy, puede definir ahora sus parámetros tras seleccionar **Uso un servidor proxy**. En la ventana siguiente, introduzca la dirección IP o la URL de su servidor proxy en el campo **Dirección**. En el campo **Puerto**, especifique el puerto donde el servidor proxy acepta conexiones (3128 de forma predeterminada). En el caso de que el servidor proxy requiera autenticación, escriba los datos válidos de **Nombre de usuario** y **Contraseña** que permitan acceder al servidor proxy. Si no utiliza un servidor proxy, seleccione **No se utiliza un servidor proxy**. Si no está seguro de si utiliza un servidor proxy o no, seleccione **Usar configuración del sistema (recomendado)** para usar la configuración actual de su sistema.

- **Privilegios**

Puede definir los usuarios o grupos con privilegios a los que se concederá permiso para editar la configuración del programa. Seleccione los usuarios en la lista de usuarios disponible a la izquierda, y **agréguelos** a la lista **Usuarios con privilegios**. Para ver todos los usuarios del sistema, seleccione **Mostrar todos los usuarios**. Si la lista Usuarios con privilegios se deja vacía, se considerará que todos los usuarios tienen privilegios.

- **ESET LiveGrid®**

Si desea obtener más información sobre ESET LiveGrid, [visite nuestro glosario](#).

- **Aplicaciones potencialmente indeseables**

Si desea obtener más información sobre las aplicaciones potencialmente indeseables, [visite nuestro glosario](#).

- **Cortafuegos**

Puede seleccionar un modo de filtrado para el cortafuegos. Para obtener más información, consulte el tema [Modos de filtrado](#). Tras la instalación de ESET Cyber Security Pro:

macOS Big Sur (11)

1. [Permita las extensiones del sistema](#).

2. [Permitir acceso total al disco](#).

3. Permita que ESET añada configuraciones de proxy. Recibirá la siguiente notificación: "ESET Cyber Security Pro" **desea agregar configuraciones de proxy**. Cuando reciba esta notificación, haga clic en **Permitir**. Si hace clic en **No permitir**, la Protección de acceso a la web no funcionará.

[macOS 10.15 y versiones anteriores](#)

1. En macOS 10.13 y posteriores, el sistema mostrará la notificación **Extensión del sistema bloqueada** y la notificación **Su ordenador no está protegido** de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro tendrá que permitir las extensiones del kernel en el dispositivo. Para permitir las extensiones del kernel en su dispositivo, diríjase a **Preferencias del Sistema > Seguridad y privacidad** y haga clic en **Permitir** para permitir el software del sistema del desarrollador **ESET, spol. s.r.o.** Para obtener información más detallada, visite este [artículo de la Base de conocimiento](#).

2. En macOS 10.14 y posteriores recibirá la notificación **Su ordenador está protegido parcialmente** de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro, tendrá que permitir

Acceso total al disco a ESET Cyber Security Pro. Haga clic en **Abrir Preferencias del Sistema > Seguridad y privacidad**. Diríjase a la ficha **Privacidad** y marque la opción **Acceso total al disco**. Haga clic en el icono para activar la edición. Haga clic en el signo más y seleccione la aplicación ESET Cyber Security Pro. Su ordenador mostrará una notificación de reinicio del ordenador. Haga clic en **Más tarde**. No reinicie el ordenador ahora. Haga clic en **Iniciar de nuevo** en la ventana de notificación de ESET Cyber Security Pro o reinicie el ordenador. Para obtener información más detallada, visite este [artículo de la Base de conocimiento](#).

Después de instalar ESET Cyber Security Pro, realizar un análisis del ordenador para comprobar si existe código malicioso. En la ventana principal del programa, haga clic en **Análisis inteligente > Análisis estándar**. Para obtener más información sobre los análisis del ordenador a petición, consulte el apartado [Análisis del ordenador a petición](#).

Permitir las extensiones del sistema

En macOS 11 (Big Sur), las extensiones del kernel se reemplazaron por extensiones del sistema. Requieren la aprobación del usuario antes de cargar nuevas extensiones del sistema de terceros.

Tras la instalación de ESET Cyber Security Pro en macOS 11 y posteriores, el sistema mostrará la notificación Extensión del sistema bloqueada y la notificación Su ordenador no está protegido de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro tendrá que permitir las extensiones del sistema en el dispositivo.



Actualice de la versión anterior de macOS a Big Sur.

Si ya tiene instalado ESET Cyber Security Pro y va a actualizar a macOS Big Sur, tendrá que permitir las extensiones del kernel de ESET manualmente tras la actualización. Se necesita acceso físico al equipo cliente: cuando se accede a ella de forma remota, el botón Permitir está desactivado.

Cuando instala el producto de ESET en macOS Big Sur o posterior, debe permitir manualmente las extensiones del sistema de ESET. Se necesita acceso físico al equipo cliente: al acceder a de forma remota, esta opción está desactivada.

Permitir las extensiones del sistema de forma manual

1. Haga clic en **Abrir Preferencias del Sistema** o **Abrir Preferencias de seguridad** en uno de los cuadros de diálogo de alerta.
2. Haga clic en el icono del candado situado en la parte inferior izquierda para permitir cambios en la ventana de configuración.
3. Utilice su Touch ID o haga clic en **Usar contraseña**, escriba su nombre de usuario y contraseña y, a continuación, haga clic en **Desbloquear**.
4. Haga clic en **Detalles**.
5. Seleccione las dos opciones de ESET Cyber Security Pro.app.
6. Haga clic en **Aceptar**.

Si desea consultar una guía detallada paso a paso, visite [el artículo de nuestra base de conocimiento](#) (los artículos de la base de conocimiento no están disponibles en todos los idiomas).

Permitir acceso total al disco

En macOS 10.14 recibirá la notificación **Su ordenador está parcialmente protegido** de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro, debe permitir el **Acceso total al disco** a ESET Cyber Security Pro.

1. Haga clic en **Abrir Preferencias del Sistema** en la ventana del cuadro de diálogo de alerta.
2. Haga clic en el icono del candado situado en la parte inferior izquierda para permitir cambios en la ventana de configuración.
3. Utilice su Touch ID o haga clic en **Usar contraseña**, escriba su nombre de usuario y contraseña y, a continuación, haga clic en **Desbloquear**.
4. Seleccione ESET Cyber Security Pro.app en la lista.
5. Se mostrará una notificación de reinicio de ESET Cyber Security Pro. Haga clic en **Ms tarde**.
6. Seleccione **Protección del sistema de archivos en tiempo real** de ESET en la lista.




No está presente la opción Protección del sistema de archivos en tiempo real de ESET

Si la opción de **Protección del sistema de archivos en tiempo real** no está en la lista, tiene que [permitir las extensiones del sistema para su producto de ESET](#).

7. Haga clic en **Iniciar de nuevo** en la ventana del cuadro de diálogo de la alerta de ESET Cyber Security Pro o reinicie el ordenador. Para obtener información más detallada, consulte el [artículo de nuestra base de conocimiento](#).

Activación del producto

Tras la instalación se muestra automáticamente la ventana Activación del producto. Para acceder al cuadro de diálogo Activación del producto en cualquier momento, haga clic en el icono de ESET Cyber Security Pro , disponible en la barra de menús de macOS (parte superior de la pantalla) y, a continuación, en **Activación del producto...**

- **Clave de licencia:** es una cadena única con el formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX que se usa para la identificación del propietario de la licencia y la activación de la misma. Si ha comprado una versión en caja del producto, active su producto con una clave de licencia. Normalmente se encuentra en el interior o en la parte posterior del paquete del producto.
- **Nombre de usuario y contraseña:** si tiene un nombre de usuario y una contraseña y no sabe cómo activar ESET Cyber Security Pro, haga clic en **Tengo un nombre de usuario y una contraseña, ¿qué tengo que hacer?**. Se le redirigirá a my.eset.com, donde puede convertir sus credenciales en una clave de licencia.
- **Licencia de prueba gratuita:** seleccione esta opción si desea evaluar ESET Cyber Security Pro antes de comprar el producto. Escriba su dirección de correo electrónico para activar ESET Cyber Security Pro durante un periodo de tiempo limitado. Recibirá la licencia de prueba por correo electrónico. Las licencias de prueba solo se pueden activar una vez por cliente.

- **Comprar licencia:** si no dispone de una licencia y quiere comprarla, haga clic en Comprar licencia. Se le redirigirá al sitio web del distribuidor local de ESET.
- **Activar más tarde:** haga clic en esta opción si no desea realizar la activación en este momento.

Desinstalación

Para desinstalar ESET Cyber Security Pro, realice una de las siguientes tareas:

- Inserte el CD o DVD de instalación de ESET Cyber Security Pro en el ordenador, ábralo desde el escritorio o la ventana del **Finder** y haga doble clic en **Desinstalar**.
- Abra el archivo de instalación de ESET Cyber Security Pro (.dmg) y haga doble clic en **Desinstalar**.
- Inicie **Finder**, abra la carpeta **Aplicaciones** de la unidad de disco duro, pulse Ctrl y haga clic en el icono de **ESET Cyber Security Pro** y seleccione **Mostrar contenido del paquete**. Abra la carpeta **Contents > Helpers** y haga doble clic en el icono **Uninstaller**.

Información general básica

La ventana principal de ESET Cyber Security Pro 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.

Desde el menú principal puede acceder a las siguientes secciones:

- **Inicio:** contiene información sobre el control parental y sobre el estado de protección del ordenador, el cortafuegos, la protección de la web y del correo electrónico.
- **Análisis del ordenador:** este apartado le permite configurar e iniciar el [análisis del ordenador a petición](#).
- **Actualización:** muestra información sobre las actualizaciones de los módulos de detección.
- **Configuración:** seleccione esta opción para ajustar el nivel de seguridad del ordenador.
- **Herramientas:** proporciona acceso a [Archivos de registro](#), [Planificador de tareas](#), [Cuarentena](#), [Procesos en ejecución](#) y otras características del programa.
- **Ayuda:** proporciona acceso a los archivos de ayuda, la base de conocimientos en Internet, el formulario de solicitud del servicio de atención al cliente e información adicional del programa.

Accesos directos del teclado

ESET Cyber Security Pro es compatible con los siguientes accesos directos del teclado:

- cmd+, : muestra las preferencias de ESET Cyber Security Pro.
- cmd+O : restaura el tamaño predeterminado de la ventana principal de la GUI de ESET Cyber Security Pro y la mueve al centro de la pantalla.
- cmd+Q : oculta la ventana principal de la GUI de ESET Cyber Security Pro. Se puede abrir haciendo clic en el icono de ESET Cyber Security Pro de la barra de menús de macOS (parte superior de la pantalla).
- cmd+W : cierra la ventana principal de la GUI de ESET Cyber Security Pro.

Los siguientes accesos directos del teclado solo funcionan si está activada la opción **Utilizar menú estándar** en

Configuración > Introducir preferencias de aplicación... > Interfaz:

- cmd+alt+L: abre la sección Archivos de registro.
- cmd+alt+S: abre la sección Planificador de tareas.
- cmd+alt+Q: abre la sección Cuarentena.

Comprobación del estado de protección

Para consultar el estado de la protección, haga clic en **Inicio** en el menú principal. En la ventana principal, se mostrará un resumen del estado de funcionamiento de los módulos de ESET Cyber Security Pro.



Qué hacer si el programa no funciona correctamente

Cuando un módulo funciona correctamente se muestra un icono de color verde. Cuando un módulo no funciona correctamente, se muestra un signo de exclamación de color rojo o un icono de notificación de color naranja. También se muestra información adicional acerca del módulo y una sugerencia para resolver el problema. Para cambiar el estado de los módulos individuales, haga clic en el vínculo azul disponible debajo de cada mensaje de notificación.

Si no consigue solucionar el problema con estas sugerencias, puede buscar una solución en la [base de conocimiento de ESET](#) o ponerse en contacto con el [Servicio de atención al cliente de ESET](#). El Servicio de atención al cliente responderá sus preguntas rápidamente y le ayudará a resolver los problemas que tenga con ESET Cyber Security Pro.

Protección del ordenador

Puede consultar la configuración del ordenador en **Configuración > Ordenador**. En esta sección se muestra el estado de **Protección del sistema de archivos en tiempo real** y **Bloqueo de medios extraíbles**. Para desactivar módulos individuales, establezca el botón del módulo deseado en **DESACTIVADO**. Tenga en cuenta que esto puede disminuir el nivel de protección del ordenador. Para acceder a la configuración detallada de cada módulo, haga clic en el botón **Configuración....**

Protección antivirus y antispyware

La protección antivirus protege el sistema contra ataques maliciosos mediante la modificación de archivos que presenten amenazas potenciales. Si se detecta una amenaza con código malicioso, el módulo antivirus puede bloquearlo y, a continuación, desinfectarlo, eliminarlo o ponerlo en cuarentena.

General

En la sección **General (Configuración > Introducir preferencias de aplicación... > General)**, puede activar la detección de los siguientes tipos de aplicaciones:



- **Aplicaciones potencialmente indeseables:** el grayware, o aplicaciones potencialmente indeseables (PUA), es una amplia categoría de software no inequívocamente malicioso, al contrario de lo que sucede con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar software adicional indeseable, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas o esperadas por el usuario. Puede obtener más información sobre estos tipos de aplicaciones en el [Glosario](#).
- **Aplicaciones potencialmente peligrosas:** estas aplicaciones son software comercial y legítimo que podría ser utilizado por atacantes si se instala sin consentimiento del usuario. En esta clasificación se incluyen programas como, por ejemplo, las herramientas de acceso remoto, de ahí que esta opción esté desactivada de forma predeterminada.
- **Aplicaciones sospechosas:** estas aplicaciones incluyen programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia aprovechan estos tipos de protectores para evitar que se detecte. Los empaquetadores son ejecutables de autoextracción en tiempo real que incluyen varios tipos de códigos maliciosos en un solo paquete. Los empaquetadores más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo código malicioso se puede detectar de diferente manera cuando se comprime con un empaquetador diferente. Los empaquetadores también tienen la capacidad de hacer que sus "firmas" muten con el tiempo, dificultando su detección y eliminación.

Para configurar [las exclusiones del sistema de archivos, web y correo electrónico](#), haga clic en el botón **Configuración....**

Exclusiones

En el apartado **Exclusiones** puede excluir del análisis determinados archivos y carpetas, aplicaciones o direcciones IP/IPv6.

Los archivos y carpetas incluidos en la pestaña **Sistema de archivos** se excluirán de todos los análisis: en el inicio, en tiempo real y a petición (análisis del ordenador).

- **Ruta:** ruta de acceso de los archivos y las 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, pero no por completo. Si más adelante este archivo se infecta con otro código malicioso, el módulo antivirus lo detectará.
- : crea una exclusión nueva. Introduzca la ruta de un objeto (también puede utilizar los comodines * y ?) o seleccione la carpeta o el archivo en la estructura de árbol.
- : elimina las entradas seleccionadas.
- **Predeterminado:** cancela todas las exclusiones.


En la ficha **Web y correo electrónico** puede excluir determinadas **Aplicaciones** o **Direcciones IP/IPv6** del análisis de protocolos.

Protección del sistema

La verificación de archivos en el inicio analiza los archivos al iniciar el sistema. De forma predeterminada, este análisis se ejecuta periódicamente como una tarea programada después del inicio de sesión del usuario o de una actualización correcta de los módulos de detección. Para modificar la configuración de los parámetros del motor de ThreatSense aplicable al análisis del inicio, haga clic en el botón **Configuración**. Encontrará más información sobre la configuración del motor ThreatSense en [esta sección](#).

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y activa un análisis en función de varios sucesos. Cuando se utiliza la tecnología ThreatSense (descrita en el apartado [Configuración de parámetros del motor ThreatSense](#)), la protección del sistema de archivos en tiempo real puede ser diferente para los archivos recién creados y los archivos existentes. Los archivos recién creados se pueden controlar de una forma más precisa.

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. La protección en tiempo real comienza cuando se inicia el sistema y proporciona un análisis ininterrumpido. En algunos casos especiales (por ejemplo, en caso de conflicto con otro programa de análisis en tiempo real), la protección en tiempo real se puede desactivar. Para desactivarla, haga clic en el icono de ESET Cyber Security Pro , situado en la barra de menús (parte superior de la pantalla) y, a continuación, seleccione **Desactivar la protección del sistema de archivos en tiempo real**. La protección en tiempo real también se puede desactivar en la ventana principal del programa (haga clic en **Configuración > Ordenador** y establezca **Protección del sistema de archivos en tiempo real** en **DESACTIVADO**).

Los siguientes tipos de soporte se pueden excluir del análisis en Real-time:

- **Unidades locales:** discos duros del sistema.
- **Medios extraíbles:** CD, DVD, soportes USB, dispositivos Bluetooth, etc.
- **Medios de red:** todas las unidades asignadas.

Se recomienda utilizar la configuración predeterminada y únicamente modificar las exclusiones del análisis en casos concretos como, cuando al analizar determinados soportes, la transferencia de datos se ralentiza

considerablemente.

Para modificar la configuración avanzada de la protección del sistema en tiempo real, vaya a **Configuración > Introducir preferencias de aplicación** (o pulse *cmd+,*) > **Protección en tiempo real** y haga clic en **Configuración...** junto a **Opciones avanzadas** (descritas en [Opciones avanzadas de análisis](#)).

Opciones avanzadas

En esta ventana puede definir los tipos de objeto que analiza el motor ThreatSense. Para obtener más información sobre los **Archivos comprimidos autoextraíbles**, los **Empaquetadores de tiempo de ejecución** y la **Heurística avanzada**, consulte [Configuración de parámetros del motor ThreatSense](#).

No recomendamos realizar cambios en la sección **Configuración predeterminada de archivos comprimidos** a menos que sea necesario para resolver un problema específico, ya que un valor superior de anidamiento de archivos comprimidos podría afectar al rendimiento del sistema.

Parámetros de ThreatSense para archivos ejecutados: de forma predeterminada se utiliza la **Heurística avanzada** al ejecutar los archivos. Se recomienda encarecidamente mantener activadas la optimización inteligente y ESET Live Grid para paliar la repercusión en el rendimiento del sistema.

Aumentar compatibilidad con volúmenes de red: esta opción aumenta el rendimiento al acceder a archivos a través de la red. Si experimenta ralentización al acceder a las unidades de red, debería activarla. Esta función utiliza el coordinador de archivos del sistema en macOS 10.10 y versiones posteriores. Tenga en cuenta que no todas las aplicaciones son compatibles con el coordinador de archivos; por ejemplo, Microsoft Word 2011 no es compatible con él, mientras que Word 2016 sí.

Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más importante para mantener un sistema seguro con ESET Cyber Security Pro. Tenga cuidado cuando modifique los parámetros de protección en tiempo real. Le recomendamos que los modifique únicamente en casos concretos, Por ejemplo, una situación en la que existe un conflicto con una aplicación determinada.

Una vez instalado ESET Cyber Security Pro, se optimizará toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en la opción **Predeterminado** situada en la parte inferior izquierda de la ventana **Protección en tiempo real (Configuración > Introducir preferencias de aplicación...)**. > **Protección en tiempo real**).

Comprobación de la protección en tiempo real

Para asegurarse de que la protección en tiempo real está funcionando y detectando virus, descargue el archivo de prueba de eicar.com y asegúrese de que ESET Cyber Security Pro lo identifica como una amenaza. Se trata de un archivo inofensivo especial detectable por todos los programas antivirus. El archivo fue creado por el instituto EICAR (European Institute for Computer Antivirus Research: 'Instituto Europeo para la Investigación de Antivirus') con el fin de comprobar la funcionalidad de los programas antivirus.

¿Qué debo hacer si la protección en tiempo real no funciona?

En este capítulo se describen las situaciones en las que puede surgir un problema cuando se utiliza la protección en tiempo real y cómo resolverlas.

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 > Ordenador** en el menú principal y establezca **Protección del sistema de archivos en tiempo real** en **ACTIVADO**. También puede activar la protección del sistema de archivos en tiempo real en la ventana de preferencias de la aplicación, con la opción **Activar la protección del sistema de archivos en tiempo real** de **Protección en tiempo real**.

La protección en tiempo real no detecta ni desinfecta las amenazas

Asegúrese de que no tenga instalados otros programas antivirus en el ordenador. Si hay dos protecciones en tiempo real activas a la vez, pueden entrar en conflicto. Le recomendamos que desinstale uno de los programas antivirus del sistema.

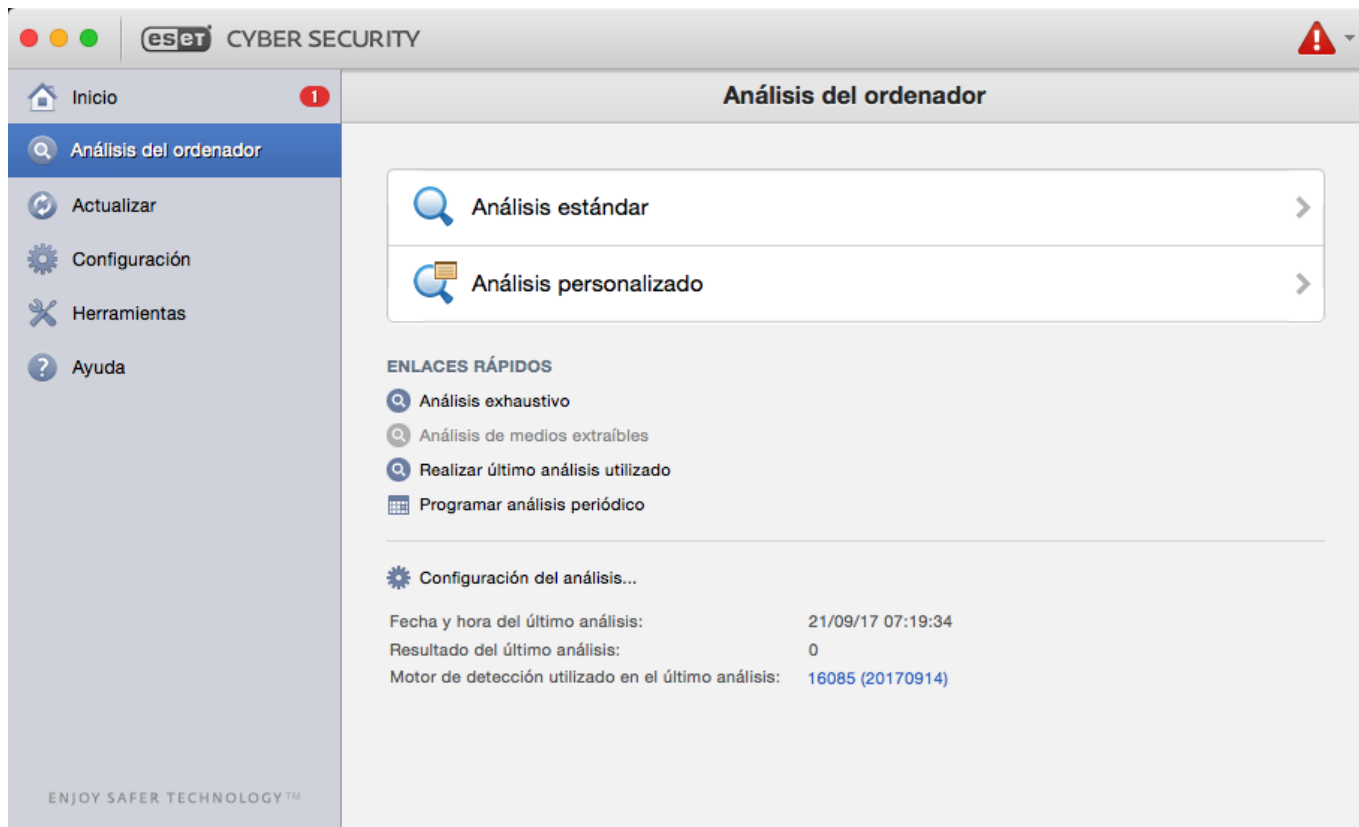
La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema, es posible que se deba a que entre en conflicto con otros programas. En caso de ser así, consulte al servicio de atención al cliente de ESET.

Análisis del ordenador a petición

Si sospecha que su ordenador está infectado (se comporta de manera anormal), ejecute un **Análisis estándar** para analizar el equipo en busca de infecciones. Para una mayor protección, el ordenador debe analizarse de forma periódica, como parte de las medidas de seguridad rutinarias, no únicamente cuando se crea que hay alguna amenaza. Los análisis regulares ayudan a detectar amenazas que no se detectaron durante el análisis en tiempo real, cuando se guardaron en el disco. Esto puede ocurrir si se ha desactivado el análisis en tiempo real en el momento de la infección o los módulos de detección no estaban actualizados.

Le recomendamos que ejecute un análisis a petición una o dos veces al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas > Tareas programadas**.



Tipo de análisis

Están disponibles dos tipos de análisis del ordenador a petición. **Análisis estándar** analiza el sistema rápidamente, sin necesidad de realizar ninguna configuración adicional de los parámetros de análisis. **Análisis personalizado** le permite seleccionar perfiles de análisis predefinidos y elegir objetos del análisis específicos.

Análisis estándar

El análisis estándar le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin necesidad de que intervenga el usuario. La principal ventaja es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis estándar comprueba todos los archivos de todas las carpetas y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece de forma automática en el valor predeterminado. Para obtener más información acerca de los tipos de desinfección, consulte el apartado [Desinfección](#).

Análisis personalizado

El **Análisis personalizado** es la solución ideal para especificar parámetros de análisis como, por ejemplo, los objetos y métodos del análisis. El análisis personalizado tiene la ventaja de que permite 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 reiteradamente con los mismos parámetros.

Para seleccionar objetos de análisis, seleccione **Análisis del ordenador > Análisis personalizado** y, a continuación, seleccione los **Objetos de análisis** específicos que desee en la estructura de árbol. Los objetos de análisis también se pueden especificar con más precisión al introducir la ruta a la carpeta o los archivos que se deseen incluir en el análisis. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione

Analizar sin desinfectar. Además, puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración > Desinfección**.



Análisis personalizado

Los análisis del ordenador en el modo personalizado están recomendados para usuarios avanzados con experiencia previa en la utilización de programas antivirus.

Objetos de análisis

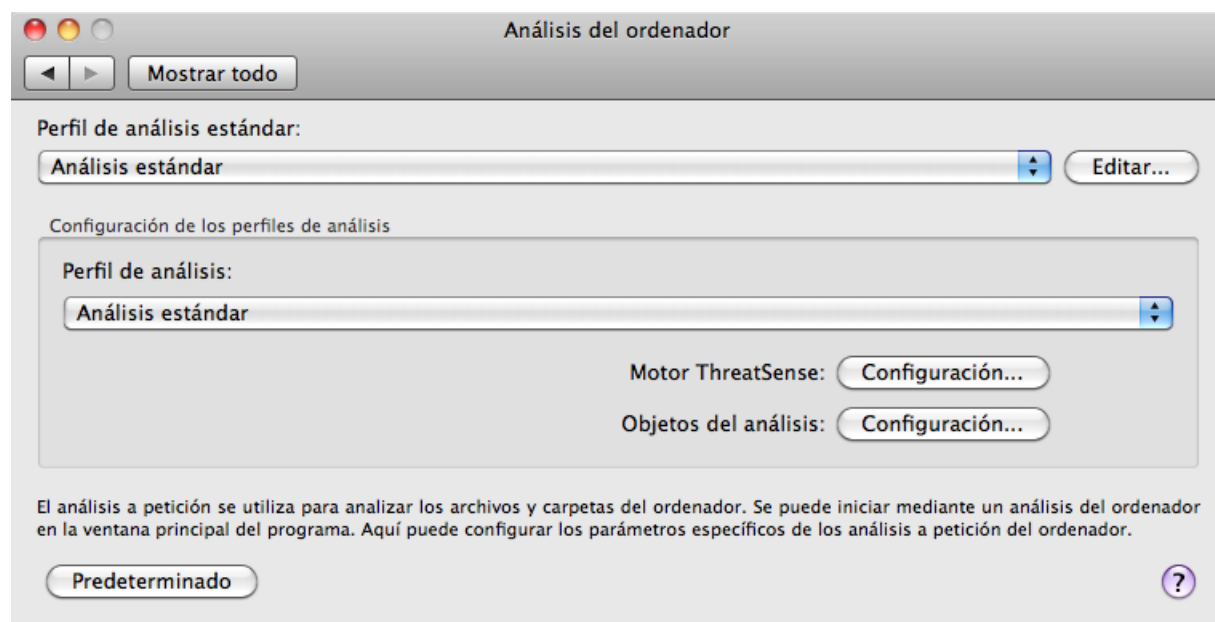
La estructura de árbol de objetos de análisis le permite seleccionar los archivos y carpetas que se analizarán en busca de virus. Las carpetas también se pueden seleccionar según la configuración de un perfil.

Los objetos de análisis se pueden especificar con más precisión al introducir la ruta a la carpeta o los archivos que se deseen incluir en el análisis. Seleccione los objetos en la estructura de árbol que muestra todas las carpetas disponibles en el ordenador activando la casilla de verificación correspondiente a un archivo o carpeta determinados.

Perfiles de análisis

Puede guardar sus perfiles 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, diríjase a **Configuración > Introducir preferencias de aplicación...** en el menú principal (o pulse *cmd+,*) > **Análisis del ordenador** y haga clic en **Editar** junto a la lista de perfiles actuales.



Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte el apartado [Configuración de parámetros del motor ThreatSense](#) para ver una descripción de los diferentes parámetros de la configuración del análisis.

Ejemplo: supongamos que desea crear su propio perfil de análisis y parte de la configuración del análisis estándar es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones

potencialmente peligrosas y, además, quiere aplicar una desinfección estricta. En la ventana **Lista de perfiles del análisis a petición**, escriba el nombre del perfil, haga clic en el botón **Agregar** y en **Aceptar** para, de este modo, confirmar la operación. A continuación, ajuste los parámetros **Motor ThreatSense** y **Objetos de análisis** en función de sus requisitos.

Si desea cerrar el sistema operativo y apagar el ordenador una vez finalizado el análisis a petición, utilice la opción **Apagar tras analizar**.

Configuración de parámetros del motor ThreatSense

ThreatSense es una tecnología patentada de ESET que se compone de una combinación de métodos complejos de detección de amenazas. Se trata de una tecnología proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de diferentes métodos (análisis de código, emulación de código, firmas genéricas, etc.) que funcionan de forma conjunta para mejorar de forma significativa 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. La tecnología ThreatSense también elimina eficazmente los rootkits.

Las opciones de configuración de la tecnología ThreatSense permiten que el usuario especifique 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 abrir la ventana de configuración, haga clic en **Configuración > Introducir preferencias de aplicación** (o pulse *cmd+,*) y, a continuación, haga clic en el botón **Configuración** del motor ThreatSense situado en los módulos **Protección del inicio**, **Protección en tiempo real** y **Análisis del ordenador**; todos ellos utilizan la tecnología ThreatSense (ver a continuación). Es posible que cada situación de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar de forma individual para los siguientes módulos de protección:

- **Protección del sistema:** verificación automática de archivos en el inicio.
- **Protección en tiempo real:** protección del sistema de archivos en tiempo real.
- **Análisis del ordenador:** análisis del ordenador a petición.
- **Protección de acceso a la Web**
- **Protección del correo electrónico**

Los parámetros de ThreatSense están optimizados específicamente para cada módulo, por lo que su modificación puede afectar considerablemente al funcionamiento del sistema. Por ejemplo, si cambia la configuración para analizar siempre los empaquetadores en tiempo real o activa la tecnología heurística avanzada en el módulo de protección del sistema de archivos en tiempo real, el sistema podría ralentizarse. Por este motivo, se recomienda que no modifique los parámetros predeterminados de ThreatSense en todos los módulos, a excepción de Análisis del ordenador.

Objetos

En la sección **Objetos** se pueden definir los archivos que se analizarán en busca de amenazas.

- **Enlaces simbólicos:** (solo análisis a petición) analiza los archivos que contengan una cadena de texto que el sistema operativo interprete y siga como una ruta a otro archivo o directorio.
- **Archivos de correo electrónico:** (no disponible en Protección en tiempo real) analiza los archivos de correo.
- **Buzones de correo:** (no disponible en la Protección en tiempo real) analiza los buzones de usuarios que haya en el sistema. El uso incorrecto de esta opción podría tener como resultado un conflicto con el cliente de correo electrónico. Para obtener más información acerca de las ventajas y desventajas de esta opción, lea el siguiente [artículo de la base de conocimientos](#).
- **Archivos comprimidos:** (no disponible en la Protección en tiempo real) analiza los archivos incluidos en los archivos comprimidos (.rar, .zip, .arj, .tar, etc.).
- **Archivos comprimidos de autoextracción:** (no disponible en la Protección en tiempo real) analiza los archivos incluidos en los archivos comprimidos de autoextracción.
- **Empaquetadores en tiempo real:** a diferencia de los archivos comprimidos estándares, los empaquetadores en tiempo real se descomprimen en la memoria. Cuando se selecciona, también se analizan los empaquetadores estáticos estándares (como UPX, yoda, ASPack, FGS).

Opciones

En la sección **Opciones**, se pueden seleccionar los métodos utilizados durante un análisis del sistema. Están disponibles estas opciones:

- **Heurística:** la tecnología heurística emplea un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de la detección heurística es la capacidad para detectar nuevo software malicioso que anteriormente no existía.
- **Heurística avanzada:** la heurística avanzada consiste en un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. La capacidad de detección del programa es muy superior gracias a esta tecnología heurística avanzada.

Desinfección

La configuración de desinfección determina el comportamiento del análisis durante la desinfección de los archivos infectados. Hay 3 niveles de 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.
- **Desinfección estándar** el programa intenta desinfectar o eliminar de manera automática un archivo infectado. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrecerá una selección de acciones que seguir. La selección de acciones que seguir también aparecerá si no se puede completar una acción predefinida.
- **Desinfección estricta:** el programa desinfectará o eliminará todos los archivos infectados (incluidos los archivos comprimidos). Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un

archivo, se mostrará una notificación y se pedirá al usuario que seleccione el tipo de acción que desea realizar.



Archivos comprimidos

en el modo predeterminado (Desinfección estándar) solamente se eliminan los archivos comprimidos en su totalidad si todos los archivos que contiene están infectados. Si un archivo comprimido contiene tanto archivos legítimos como archivos infectados, no se eliminará. Si se detecta un archivo infectado en el modo Desinfección estricta, se eliminará todo el archivo comprimido aunque contenga archivos no infectados.



Análisis de archivos comprimidos

En el modo predeterminado de Desinfección estándar solamente se eliminan los archivos comprimidos en su totalidad si todos los archivos que contiene están infectados. Si un archivo comprimido contiene tanto archivos legítimos como archivos infectados, no se eliminará. Si se detecta un archivo infectado en el modo Desinfección estricta, se eliminará todo el archivo comprimido aunque contenga archivos no infectados.

Exclusiones

Las extensiones son la parte del nombre de archivo delimitada por un punto, que define el tipo y el contenido de un archivo. En esta sección de la configuración de parámetros de ThreatSense, puede definir los tipos de archivos que desea excluir del análisis.

De forma predeterminada, se analizan todos los archivos independientemente de cuál sea su extensión. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis. Los botones y le permiten activar o prohibir el análisis de extensiones concretas.

A veces es necesario excluir archivos del análisis, como sucede cuando el análisis de ciertos tipos de archivos impide que el programa funcione correctamente. Por ejemplo, podría ser recomendable excluir los archivos *log*, *cfg* y *tmp*. El formato correcto para introducir las extensiones del archivo es:

log

cfg

tmp

Límites

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

- **Tamaño máximo:** define el tamaño máximo de los objetos que se analizarán. Cuando se define el tamaño máximo, el módulo antivirus solamente analizará los objetos cuyo tamaño sea inferior al especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos de mayor tamaño.
- **Tiempo máximo de análisis:** define el tiempo máximo asignado para analizar un objeto. Si se introduce aquí un valor definido por el usuario, el módulo antivirus detendrá el análisis de los objetos cuando se haya agotado el tiempo, tanto si ha finalizado el análisis como si no.

- **Nivel máximo de anidamiento:** especifica la profundidad máxima del análisis de archivos comprimidos. Le recomendamos que no cambie el valor predeterminado de 10: en circunstancias normales, no debería haber motivos para hacerlo. Si el análisis finaliza antes de tiempo debido al número de archivos anidados, el archivo comprimido quedará sin analizar.
- **Tamaño máximo del archivo:** esta opción le permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se vayan a analizar. Si el análisis finaliza antes de tiempo debido a este límite, el archivo comprimido quedará sin analizar.

Otros

Activar optimización inteligente

Si la opción Optimización inteligente está activada, la configuración se optimiza para garantizar el nivel de análisis más eficaz sin que la velocidad de análisis se vea afectada. Los diferentes módulos de protección analizan de forma inteligente y con distintos métodos de análisis. La optimización inteligente no se ha definido de forma estricta en el producto. El equipo de desarrollo de ESET implementa constantemente cambios nuevos que, posteriormente, se integran en ESET Cyber Security Pro mediante actualizaciones periódicas. Si la opción Optimización inteligente está desactivada, durante el análisis solamente se aplica la configuración definida por el usuario en el módulo ThreatSense.

Analizar flujo de datos alternativo (solo análisis a petición)

Los flujos de datos alternativos utilizados por el sistema de archivos son asociaciones de carpetas y archivos invisibles para técnicas de análisis ordinario. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Detección de una amenaza

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

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

1. Haga clic en **Análisis del ordenador**.
2. Haga clic en **Análisis estándar** (para obtener más información, consulte el apartado [Análisis estándar](#)).
3. Una vez 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 desee incluir en el análisis de virus.

A modo de ejemplo general de cómo se gestionan las amenazas en ESET Cyber Security Pro, suponga que el supervisor del sistema de archivos en tiempo real, que utiliza el nivel de desinfección predeterminado, detecta una amenaza. La protección en tiempo real intentará desinfectar o eliminar el archivo. Si no se dispone de ninguna tarea predefinida para el módulo de protección en tiempo real, una ventana de alerta le pedirá que seleccione una opción. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados permanecerían infectados. Esta opción está

pensada para situaciones en las que esté seguro de que el archivo sea inofensivo y se haya detectado por error.

Desinfección y eliminación

Inicie la desinfección si un archivo ha sido infectado por un virus que le haya añadido código malicioso. Si es el caso, primero intente desinfectar el archivo infectado para devolverlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.



Eliminación de amenazas en archivos comprimidos

En el modo de desinfección predeterminado, solamente se eliminará el archivo comprimido en su totalidad si todos los archivos que contiene están infectados. En otras palabras, no se eliminan los archivos comprimidos si también contienen archivos no infectados e inofensivos. Sin embargo, tenga cuidado cuando realice un análisis con **Desinfección estricta**, ya que el archivo comprimido se eliminará si contiene, como mínimo, un archivo infectado, sin tener en cuenta el estado de los demás.

Análisis y bloqueo de medios extraíbles

ESET Cyber Security Pro puede ejecutar un análisis a petición de dispositivos de memoria extraíble insertados (CD, DVD, USB, etc.). En macOS 10.15, también puede analizar otros ESET Cyber Security Pro dispositivos de medios externos.



Análisis de medios extraíbles en macOS 11 y versiones posteriores

ESET Cyber Security Pro instalado en macOS 11 y versiones posteriores analiza solo los dispositivos de memoria.



Los medios extraíbles pueden contener código malicioso y poner en peligro su ordenador. Para bloquear los medios extraíbles, haga clic en **Configuración de bloqueo de medios** (véase la imagen anterior) o en el menú principal, **Configuración > Introducir preferencias de aplicación... > Medios** en la ventana principal del programa y seleccione la opción **Activar bloqueo de medios extraíbles**. Si desea permitir el acceso a determinados tipos de unidades, anule la selección de los volúmenes de medios que desee.



Acceso a CD-ROM

Si desea permitir el acceso a la unidad de CD-ROM externa conectada al ordenador mediante un cable USB, anule la selección de la opción **CD-ROM**.

Anti-Phishing

El término phishing hace referencia a una actividad delictiva que utiliza la ingeniería social (la manipulación de usuarios con el fin de obtener información confidencial). El phishing suele utilizarse para acceder a datos confidenciales, como números de cuentas bancarias, números de tarjetas de crédito, números PIN o nombres de usuario y contraseñas.

Le recomendamos que mantenga la función Anti-Phishing activada (**Configuración > Introducir las preferencias de la aplicación... > Protección Anti-Phishing**). Se bloquearán todos los posibles ataques de phishing que provengan de sitios web o dominios peligrosos y se mostrará una notificación que le informa del ataque.

Cortafuegos

El cortafuegos controla todo el tráfico de red que tiene como origen o destino el sistema al permitir o denegar conexiones de red concretas basándose en las reglas de filtrado especificadas. Proporciona protección frente a ataques procedentes de ordenadores remotos y activa el bloqueo de determinados servicios. También ofrece protección antivirus para los protocolos HTTP, POP3 e IMAP.



Excepciones de análisis

ESET Cyber Security Pro no analiza los protocolos cifrados HTTPS, POP3S e IMAPS.

Puede consultar la configuración del cortafuegos en **Configuración > Cortafuegos**. Aquí puede ajustar el modo de filtrado, las reglas y la configuración detallada, así como acceder a la configuración detallada del programa.

Si establece **Bloquear todo el tráfico de red: desconectar la red** en **ACTIVADO**, el cortafuegos bloqueará toda la comunicación entrante y saliente. Utilice esta opción únicamente si considera que existen riesgos de seguridad

que requieren la desconexión del sistema de la red.

Modos de filtrado

El cortafuegos de ESET Cyber Security Pro ofrece tres modos de filtrado. Los ajustes de los modos de filtrado se encuentran en las preferencias de ESET Cyber Security Pro (pulse *cmd+*) > **Cortafuegos**. El comportamiento del cortafuegos cambia en función del modo seleccionado. Los modos de filtrado influyen también en el nivel necesario de interacción del usuario.

Todo el tráfico bloqueado: bloquea todas las conexiones entrantes y salientes.

Automático con excepciones: este es el modo predeterminado, y es aconsejable para aquellos usuarios que optan por un uso sencillo y cómodo del cortafuegos sin necesidad de definir reglas. El modo automático permite todo el tráfico saliente para el sistema en cuestión y bloquea todas las conexiones no iniciadas desde la ubicación remota. También le permite añadir reglas personalizadas definidas por el usuario.

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. En este cuadro de diálogo se 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 en este momento, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla.



Si desea registrar información detallada sobre todas las conexiones bloqueadas en un archivo de registro, seleccione **Registrar todas las conexiones bloqueadas**. Para revisar los archivos de registro del cortafuegos, en el menú principal haga clic en **Herramientas > Registros** y seleccione **Cortafuegos** en el menú desplegable **Registro**.

Reglas del cortafuegos

Las reglas del cortafuegos representan un conjunto de condiciones que se utilizan para probar todas las conexiones de red y decidir las acciones adecuadas para estas condiciones. Con las reglas del cortafuegos puede definir el tipo de acción que se debe realizar cuando se establezca una conexión definida por una regla.

Las conexiones entrantes se inician en ordenadores remotos que intentan establecer una conexión con el sistema local. Las conexiones salientes funcionan de la forma opuesta: el sistema local se pone en contacto con un ordenador remoto.

Si se detecta una comunicación desconocida, debe considerar detenidamente su admisión o denegación. Las conexiones no solicitadas, no seguras o desconocidas suponen un riesgo de seguridad para el sistema. Si se establece una conexión de este tipo, debe prestar especial atención al ordenador remoto y a la aplicación que intenta 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.

De manera predeterminada, las aplicaciones firmadas por Apple pueden acceder automáticamente a la red. Si quiere desactivar esta configuración, anule la selección de **Permitir que el software firmado por Apple acceda a la red automáticamente**.

Creación de reglas nuevas

La ficha **Reglas** contiene una lista de todas las reglas aplicadas al tráfico que genera cada aplicación. Las reglas se agregan automáticamente, de acuerdo con las respuestas de los usuarios ante una comunicación nueva.

1. Para crear una regla nueva, haga clic en **Agregar**, escriba el nombre de la regla y arrastre y coloque el icono de la aplicación en el campo en blanco, o haga clic en **Examinar** para buscar el programa en la carpeta */Aplicaciones*. Para aplicar la regla a todas las aplicaciones instaladas en el ordenador, seleccione la opción **Todas las aplicaciones**.
2. En la siguiente ventana, especifique la **Acción** (permitir o denegar la comunicación entre la aplicación seleccionada y la red) y la **Dirección** de la comunicación (entrante, saliente o ambas). Puede registrar todas las comunicaciones relacionadas con esta regla en un archivo de registro. Para ello, seleccione la opción **Regla de registro**. Para revisar los registros, haga clic en **Herramientas > Archivos de registro** en el menú principal de ESET Cyber Security Pro y seleccione **Cortafuegos** en el menú desplegable **Registro**.
3. En la sección **Protocolo/Puertos**, seleccione un protocolo para la comunicación de la aplicación y los números de puerto (si se selecciona el protocolo TCP o UDP). La capa del protocolo de transporte ofrece una transferencia de datos segura y eficiente.
4. Por último, especifique los criterios del **Destino** (dirección IP, rango, subred, Ethernet o Internet) para la regla.

Zonas del cortafuegos

Una zona es una recopilación de direcciones de red que conforman un grupo lógico. A cada dirección de un grupo se le asignan reglas similares definidas de manera centralizada para todo el grupo.

Haga clic en **Agregar...** para crear zonas de confianza. Introduzca un **Nombre** y una **Descripción** (opcional) para la zona, seleccione el perfil al que pertenecerá y agregue una dirección IPv4/IPv6, un rango de direcciones, una subred, una red Wi-Fi o una interfaz.

Perfiles del cortafuegos

La opción **Perfiles** permite controlar el comportamiento del cortafuegos de ESET Cyber Security Pro. Cuando cree o modifique una regla del cortafuegos, puede asignarla a un perfil específico. Al seleccionar un perfil solo se aplican las reglas globales (que no tienen un perfil especificado) y las reglas asignadas a dicho perfil. Es posible crear varios perfiles con diferentes reglas asignadas para modificar fácilmente el comportamiento del

cortafuegos.

Registros del cortafuegos

El cortafuegos de ESET Cyber Security Pro guarda todos los sucesos importantes en un archivo de registro. Para acceder a los registros del cortafuegos desde el menú principal, haga clic en **Herramientas > Registros** y seleccione **Cortafuegos** en el menú desplegable **Registro**.

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

- Fecha y hora del suceso
- Nombre del suceso
- Fuente
- Dirección de la red de destino
- Protocolo de comunicación de red
- Regla aplicada
- Aplicación implicada
- Usuario

Un análisis exhaustivo de estos datos puede ayudarle a detectar los intentos de poner en peligro la seguridad del sistema. Hay muchos otros factores que indican posibles riesgos para la seguridad de los que puede defenderse con el cortafuegos, como los siguientes: conexiones frecuentes desde ubicaciones desconocidas, intentos repetidos de establecer conexiones, comunicación de aplicaciones desconocidas o números de puertos poco comunes.

Protección de web y correo electrónico

Para acceder a Protección de web y correo electrónico desde el menú principal, haga clic en **Configuración > Web y correo electrónico**. Desde aquí también puede acceder a la configuración detallada de cada módulo haciendo clic en **Configuración**.

- **Protección del tráfico de Internet:** supervisa la comunicación HTTP entre los navegadores web y los servidores remotos.
- **Protección del cliente de correo electrónico:** proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing:** bloquea posibles ataques de phishing procedentes de sitios web o dominios.



Excepciones de análisis

ESET Cyber Security Pro no analiza los protocolos cifrados HTTPS, POP3S e IMAPS.

Protección web

La protección del acceso a la Web controla la comunicación entre los navegadores web y los servidores remotos para que se cumplan las reglas del protocolo HTTP (Protocolo de transferencia de hipertexto).

El filtrado web se puede realizar definiendo [los números de puerto de la comunicación HTTP](#) y/o las [direcciones URL](#).

Puertos

En la ficha **Puertos** puede definir el número de puertos utilizados para la comunicación HTTP. Los números de puerto predeterminados son 80, 8080 y 3128.

Listas de URL

En la sección **Listas de URL** puede especificar las direcciones HTTP que desea bloquear, permitir o excluir en el análisis. No será posible acceder a los sitios web incluidos en la lista de direcciones bloqueadas. El acceso a los sitios web de la lista de direcciones excluidas se realiza sin un análisis en busca de código malicioso.

Para solo permitir acceso a las direcciones URL incluidas en la lista **Dirección URL permitida**, seleccione la opción **Restringir direcciones URL**.

Para activar una lista, seleccione **Activada** junto al nombre de la lista. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione la opción **Notificada**.

Todas las listas admiten el uso de los símbolos especiales * (asterisco) y ? (signo de interrogación). 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.

Protección del correo electrónico

La protección de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Al examinar los mensajes entrantes, ESET Cyber Security Pro utiliza todos los métodos de análisis avanzados incluidos en el motor de análisis ThreatSense. El análisis de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

Motor ThreatSense: Configuración: la configuración avanzada del análisis le permite configurar objetos de análisis, métodos de detección, etc. Haga clic en **Configuración** para ver la ventana de configuración detallada del análisis.

Añadir mensajes de etiqueta a la nota al pie de los correos electrónicos: después de analizarse un correo electrónico, se puede añadir al mensaje una notificación que contenga los resultados del análisis. Los mensajes de etiqueta son una herramienta útil pero no pueden utilizarse como una decisión final con respecto a la seguridad, ya que se pueden omitir en mensajes HTML problemáticos y determinadas amenazas pueden falsificarlos. Están disponibles estas opciones:

- **Nunca:** no se agregará mensaje de etiqueta a ningún correo electrónico.
- **Solo al correo electrónico infectado:** únicamente se marcarán como analizados los correos electrónicos que contengan malware.
- **A todos los mensajes analizados:** se agregarán mensajes de etiqueta a todos los correos electrónicos analizados.

Agregar una advertencia en el asunto de los mensajes infectados recibidos y leídos: marque esta casilla de verificación si desea que la protección de correo electrónico incluya una alerta de amenaza en los mensajes infectados. Esta característica permite un filtrado sencillo de los correos electrónico infectados. Además, aumenta la credibilidad ante el destinatario y, si se detecta una amenaza, proporciona información valiosa sobre el nivel de amenaza de un correo electrónico o remitente determinado.

Plantilla añadida al asunto del correo electrónico infectado: modifique esta plantilla para modificar el formato de prefijo del asunto de un mensaje infectado.

- %avstatus%: añade el estado de infección del correo electrónico (por ejemplo: limpio, infectado...).
- %virus%: añade el nombre de la amenaza.
- %aspmstatus%: cambia el asunto en función del resultado del análisis antispam.
- %product%: añade el nombre de su producto ESET (en este caso, ESET Cyber Security Pro).
- %product_url%: añade el vínculo al sitio web de ESET (www.eset.com)

En la parte inferior de esta ventana también puede activar y desactivar la comprobación de las comunicaciones de correo electrónico recibidas a través de los protocolos POP3 e IMAP. Para obtener más información sobre este aspecto, consulte los siguientes temas:

- [Comprobación del protocolo POP3](#)
- [Comprobación del protocolo IMAP](#)

Comprobación del protocolo POP3

El protocolo POP3 es el más ampliamente utilizado para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. ESET Cyber Security Pro 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. Asegúrese de que el módulo esté activado para que el filtrado de protocolos funcione correctamente; el control del protocolo POP3 se realiza automáticamente, sin que sea necesario volver a configurar su cliente de correo electrónico. De forma predeterminada, se analizan todas las comunicaciones realizadas en el puerto 110, pero se pueden agregar otros puertos de comunicación si es necesario. Los números de puerto deben delimitarse con una coma.

Si está seleccionada la opción **Activar la comprobación del protocolo POP3**, se supervisa todo el tráfico POP3 en busca de software malicioso.

Comprobación del protocolo IMAP

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 mantiene la información de estado (por ejemplo, si el mensaje se ha leído, contestado o eliminado). ESET Cyber Security Pro ofrece 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. Asegúrese de que la verificación del protocolo IMAP esté habilitada para que el módulo funcione correctamente; el control del protocolo IMAP se realiza automáticamente, sin que sea necesario volver a configurar su 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. Los números de puerto deben delimitarse con una coma.

Si está seleccionada la opción **Activar la comprobación del protocolo IMAP**, se comprueba la presencia de software malicioso en todo el tráfico a través de IMAP.

Control parental

En la sección **Control parental** puede definir la configuración del Control parental, que proporciona a los padres herramientas automáticas que les ayudan a proteger a sus hijos. El objetivo de esta función es impedir que los niños y adolescentes tengan acceso a páginas que contienen contenido inapropiado o perjudicial. El Control parental le permite bloquear las páginas web que pueden contener material que podría resultar ofensivo. Además, los padres pueden prohibir el acceso a un total de 27 categorías de sitios web predefinidas.

En la ventana **Control parental (Configuración > Introducir las preferencias de la aplicación > Control parental)** se muestra una lista de sus cuentas de usuario. Seleccione la cuenta que desea utilizar para el control parental. Para especificar un nivel de protección para la cuenta seleccionada, haga clic en el botón **Configuración...**. Para crear una cuenta nueva, haga clic en **Agregar...**. Este botón le redirigirá a la ventana de cuentas del sistema de macOS.

En la ventana **Configuración del control parental**, seleccione uno de los perfiles predefinidos en el menú desplegable **Perfil de configuración** o copie la configuración de control parental de otra cuenta de usuario. Cada perfil contiene una lista modificada de las categorías permitidas. Si una categoría está seleccionada, significa que se permite. Al mover el ratón sobre una categoría se muestra una lista de las páginas web incluidas en dicha categoría.

Para modificar la lista de **Páginas web bloqueadas y permitidas**, haga clic en **Configuración** en la parte inferior de una ventana y agregue un nombre de dominio a la lista deseada. No escriba *http://*. No es necesario utilizar comodines (*). Si escribe un nombre de dominio, se incluirán todos los subdominios. Por ejemplo, si agrega *google.com* a la **Lista de páginas web permitidas**, se permitirán todos los subdominios (*mail.google.com*, *news.google.com*, *maps.google.com* etc.).



Reglas

La acción de bloquear o permitir una página web específica puede ser más precisa que su aplicación a toda una categoría de páginas web.

Actualización

Es necesario actualizar ESET Cyber Security Pro de forma periódica para mantener el máximo nivel de seguridad. El módulo de actualización descarga la base de firmas de virus más reciente para, de este modo, garantizar que los módulos de detección estén siempre al día.

Haga clic en **Actualizar** en el menú principal para comprobar el estado de la actualización de ESET Cyber Security Pro, así como la fecha y la hora de la última actualización y si es necesario actualizar el programa. Haga clic en

Actualizar módulos para iniciar el proceso de actualización manualmente.

En circunstancias normales, cuando las actualizaciones se descargan correctamente, se mostrará el mensaje **No es necesario actualizar los módulos, ya están actualizados.** en la ventana Actualización. Si no es posible actualizar los módulos, recomendamos que revise la [configuración de actualización](#): el motivo más típico de este error es haber introducido datos de autenticación incorrectos (nombre de usuario y contraseña) o una incorrecta [configuración de la conexión](#).

La ventana de actualización también contiene el número de versión del motor de detección. El número de versión está vinculado a la página web de ESET, en la que se muestra la información de actualización del motor de detección.

Configuración de actualizaciones

Para eliminar todos los datos de actualización almacenados temporalmente, haga clic en **Eliminar** situado junto a **Eliminar la caché de actualización**. Utilice esta opción si tiene dificultades para realizar la actualización.

Opciones avanzadas

Para desactivar las notificaciones mostradas tras una actualización correcta, seleccione **No mostrar notificación sobre la actualización correcta**.

Para descargar los módulos en desarrollo que están en las fases de prueba finales, active **Actualización previa a su lanzamiento**. Las actualizaciones previas a su lanzamiento suelen contener correcciones de problemas del producto. La **Actualización retrasada** descarga las actualizaciones horas después de su publicación, con el fin de garantizar que los clientes no recibirán las actualizaciones hasta que esté confirmado que no contienen problemas de estado salvaje.

ESET Cyber Security Pro registra instantáneas del motor de detección y los módulos del programa para usarlas con la función de **Reversión de actualización**. Mantenga activada la opción **Crear instantáneas de archivos actualizados** para que ESET Cyber Security Pro registre estas instantáneas de forma automática. Si sospecha que una nueva actualización del módulo de detección o de los módulos del programa puede ser inestable o estar dañada, puede usar la función de reversión para volver a una versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido. Para devolver las actualizaciones a una versión más antigua del historial, haga clic en **Revertir**. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente. Al volver a una actualización anterior, utilice el menú desplegable **Definir periodo de suspensión en** para especificar el periodo de tiempo durante el que desea suspender las actualizaciones. Si selecciona la opción **hasta que se revoque**, las actualizaciones no se reanudarán hasta que las restaure manualmente. Para restaurar las actualizaciones manualmente, haga clic en **Permitir**. Tenga cuidado al establecer el periodo de tiempo durante el que desea suspender las actualizaciones.

Establecer una antigüedad máxima para la base de datos automáticamente: permite establecer el tiempo máximo (en días) tras el que los módulos de detección se considerarán desactualizados. El valor predeterminado es siete días.

Cómo crear tareas de actualización

Las actualizaciones pueden desencadenarse manualmente haciendo clic en la opción **Actualizar** del menú principal y, posteriormente, en **Actualizar módulos**.

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 Cyber Security Pro:

- **Actualización automática periódica**
- **Actualización automática tras inicio de sesión 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](#).

Actualización de ESET Cyber Security Pro a una nueva versión

Utilice la compilación más reciente de ESET Cyber Security Pro para disfrutar de la máxima protección posible. Para buscar una versión nueva, haga clic en **Inicio** en el menú principal. Si está disponible una nueva compilación, se mostrará un mensaje. Haga clic en **Más información...** para abrir una ventana nueva con el número de versión de la nueva compilación y el registro de cambios.

Haga clic en **Sí** para descargar la última compilación o en **Ahora no** para cerrar la ventana y descargar la actualización más adelante.

Al hacer clic en **Sí**, el archivo se guarda en la carpeta de descargas (o la carpeta predeterminada que indique el navegador). Cuando finalice la descarga, abra el archivo y siga las instrucciones de instalación. El nombre de usuario y la contraseña se transferirán automáticamente a la nueva instalación. Se recomienda comprobar periódicamente si hay actualizaciones disponibles, especialmente cuando ESET Cyber Security Pro se instala desde un CD o DVD.

Actualizaciones del sistema

La función de actualizaciones del sistema macOS es un componente importante que tiene como objetivo proteger a los usuarios frente al software malicioso. Para una mayor seguridad, le recomendamos que instale estas actualizaciones en cuanto estén disponibles. ESET Cyber Security Pro le informará de las actualizaciones que faltan en función del nivel que haya especificado. Puede ajustar la disponibilidad de las notificaciones de actualización en **Configuración > Introducir preferencias de aplicación** (o pulse `cmd +,`) > **Alertas y notificaciones > Configuración**, cambiando las opciones de **Mostrar condiciones** disponibles junto a **Actualizaciones del sistema operativo**.

- **Mostrar todas las actualizaciones:** se mostrará una notificación siempre que falte una actualización del sistema.

- **Mostrar solo las recomendadas:** solo recibirá una notificación para las actualizaciones recomendadas.

Si no desea recibir notificaciones relativas a las actualizaciones que faltan, anule la selección de la casilla de verificación disponible junto a **Actualizaciones del sistema operativo**.

La ventana de notificación contiene una visión general de las actualizaciones disponibles para el sistema operativo macOS y las aplicaciones que se actualizan a través de la herramienta nativa de macOS, Actualizaciones de Software. Puede ejecutar la actualización directamente desde la ventana de notificación o desde la sección **Inicio** de ESET Cyber Security Pro, haciendo clic en **Instalar actualizaciones inexistentes**.

En la ventana de notificación se muestra el nombre, la versión, el tamaño y las propiedades (marcadores) de la aplicación, así como información adicional sobre las actualizaciones disponibles. En la columna Marcadores se muestra la información siguiente:

- **[recomendado]:** el fabricante del sistema operativo le recomienda instalar esta actualización para aumentar la seguridad y la estabilidad del sistema.
- **[reiniciar]:** es necesario reiniciar el ordenador después de la instalación.
- **[apagar]:** es necesario apagar el ordenador y volver a encenderlo tras la instalación,

En la ventana de notificación se muestran las actualizaciones recuperadas mediante la herramienta de la línea de comandos "softwareupdate". Las actualizaciones recuperadas con esta herramienta varían en función de las actualizaciones que muestra la aplicación "Actualizaciones de Software". Si desea instalar todas las aplicaciones disponibles que se muestran en la ventana de actualizaciones de sistema pendientes, así como aquellas que no muestra la aplicación "Actualizaciones de Software", utilice la herramienta de la línea de comandos "softwareupdate". Para obtener más información sobre esta herramienta, lea el manual de "softwareupdate"; para ello, escriban softwareupdate en una ventana de Terminal. Esto solo se recomienda a usuarios avanzados.

Herramientas

El menú **Herramientas** incluye módulos que simplifican la administración del programa y ofrecen más opciones para usuarios avanzados.

Archivos de registro

Los archivos de registro contienen información relacionada con todos 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 la configuración actual del nivel de detalle de los registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno de ESET Cyber Security Pro, donde también se pueden archivar registros.

Para acceder a los archivos de registro desde el menú principal de ESET Cyber Security Pro, haga clic en **Herramientas > Registros**. Seleccione el tipo de registro que desee en el menú desplegable **Registro**, situado en la parte superior de la ventana. Están disponibles los siguientes registros:

1. **Amenazas detectadas:** utilice esta opción para ver toda la información de los sucesos relacionados con la detección de amenazas.

2.**Sucesos:** esta opción se ha diseñado para ayudar a los administradores del sistema y los usuarios con la solución de problemas. Todas las acciones importantes que realice ESET Cyber Security Pro se registran en los registros de sucesos.

3.**Análisis del ordenador:** en este registro se muestran los resultados de todos los análisis completados. Haga doble clic en cualquier entrada para ver los detalles del correspondiente análisis del ordenador a petición.

4.**Control parental:** aquí se proporciona una lista de todas las páginas web bloqueadas por el control parental.

5.**Cortafuegos:** este registro contiene los resultados de todos los sucesos relacionados con la red.

6.**Sitios web filtrados:** esta lista resulta útil si desea ver una lista de los sitios web que la Protección del acceso a la Web ha bloqueado. En estos registros puede ver la hora, la URL, el estado, la dirección IP, el usuario y la aplicación que han establecido conexión con el sitio web en cuestión.

La información que se muestra en las diferentes secciones se puede copiar directamente en el portapapeles; para ello, seleccione la entrada y haga clic en el botón **Copiar**.

Mantenimiento de registros

Puede acceder a la configuración de registros de ESET Cyber Security Pro desde la ventana principal del programa. Haga clic en **Configuración > Introducir las preferencias de la aplicación** (o pulse *cmd+,*) > **Archivos de registro**. Puede especificar las siguientes opciones para los archivos de registro:

- **Eliminar los registros antiguos automáticamente:** las entradas de registro anteriores al número de días especificado se eliminarán de forma automática (90 días de forma predeterminada).
- **Optimizar los archivos de registro automáticamente:** los archivos de registro se desfragmentan automáticamente si se supera el porcentaje especificado de registros no utilizados (25 % de forma predeterminada).

Toda la información relevante que se muestra en los mensajes de la interfaz gráfica de usuario, de amenazas y de sucesos se puede almacenar en formato de texto legible, como texto sin formato o CSV (Comma-separated values). Si desea que estos archivos estén disponibles para el procesamiento con herramientas de terceros, seleccione la casilla de verificación situada junto a **Activar registro en archivos de texto**.

Para definir la carpeta de destino donde se guardarán los archivos de registro, haga clic en **Configuración**, junto a **Opciones avanzadas**.

En función de las opciones que seleccione en **Archivos de registro de texto: Editar** puede guardar registros con la siguiente información:

o Los sucesos como *Nombre de usuario y contraseña no válidos, No se pueden actualizar los módulos*, etc. se registran en el archivo *eventslog.txt*.

o Las amenazas detectadas por Análisis en el inicio, Protección en tiempo real o Análisis del ordenador se guardan en el archivo *threatslog.txt*.

o Los resultados de todos los análisis completados se guardan en formato *scanlog.NÚMERO.txt*

o Todos los sucesos relacionados con la comunicación a través del cortafuegos se escriben en *firewalllog.txt*

Para configurar los filtros de **Historiales de registro de análisis del ordenador predeterminados**, haga clic en **Editar** y seleccione o anule la selección de los tipos de registro que desee. Encontrará una explicación más

detallada de estos tipos de registro en [Filtrado de registros](#).

Filtrado de registros

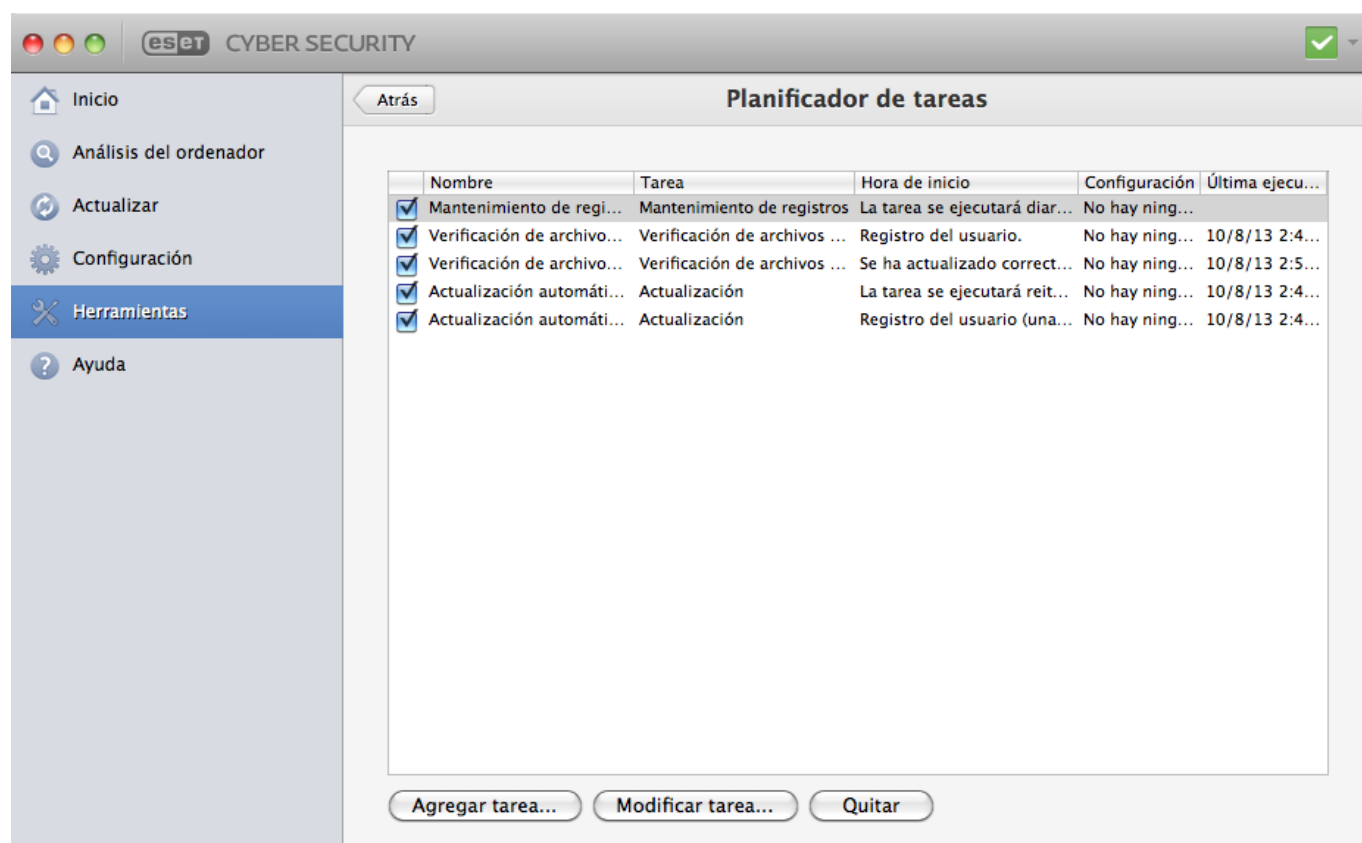
Registra información acerca de sucesos importantes del sistema. La característica de filtrado de registros permite ver los registros de un tipo específico de suceso.

A continuación se enumeran los tipos de registro más utilizados:

- **Alertas críticas:** errores graves del sistema (por ejemplo, «No se ha podido iniciar la protección del antivirus»).
- **Errores:** mensajes de error, como «*Error al descargar el archivo*», y errores graves.
- **Alertas:** mensajes de alerta.
- **Registros informativos:** mensajes informativos, como los de actualizaciones realizadas con éxito, alertas, etc.
- **Registros de diagnóstico:** información necesaria para ajustar el programa y todos los registros descritos anteriormente.

Planificador de tareas

El **Planificador de tareas** se puede encontrar en el menú principal de ESET Cyber Security Pro, en **Herramientas**. 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 que se hayan utilizado.



El Planificador de tareas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas. La configuración y las propiedades contienen información como la fecha y la hora, así como los

perfiles especificados que se van a utilizar durante la ejecución de la tarea.

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

- Mantenimiento de registros (después de activar la opción **Mostrar tareas de sistema** en la configuración del planificador de tareas)
- Verificación de archivos en el inicio tras el inicio de sesión del usuario
- Verificación de archivos en el inicio tras actualizar correctamente los módulos de detección
- Actualización automática de rutina
- Actualización automática tras inicio de sesión del usuario

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), pulse Ctrl y haga clic en la tarea que desee modificar y, a continuación, haga clic en **Editar** o seleccione la tarea y haga clic en **Modificar tarea....**

Creación de tareas nuevas

Para crear una nueva tarea en Tareas programadas, haga clic en **Agregar tarea** o haga clic con la tecla Ctrl pulsada en el espacio en blanco y seleccione **Agregar** en el menú contextual. Hay cinco tipos de tareas programadas disponibles:

- **Ejecutar aplicación**
- **Actualización**
- **Mantenimiento de registros**
- **Análisis del ordenador a petición**
- **Verificación de archivos en el inicio del sistema**



Ejecutar aplicación

Si selecciona **Ejecutar aplicación**, puede ejecutar programas como un usuario del sistema llamado "nadie". Los permisos para la ejecución de aplicaciones a través de Tareas programadas vienen definidos por macOS. Si desea cambiar el valor predeterminado del usuario, escriba el nombre de usuario seguido de dos puntos (:) delante del comando. Con esta característica también puede utilizar el usuario **root**.



Ejemplo: Ejecutar tarea como usuario

En este ejemplo vamos a programar la aplicación de calculadora para que se inicie a la hora seleccionada con el nombre de usuario **Usuario1**:

1. Seleccione **Agregar tarea** en **Tareas programadas**.
2. Escriba el nombre de la tarea. Seleccione **Ejecutar aplicación** como una **Tarea programada**. Seleccione **Una vez** en la ventana **Ejecutar tarea** para ejecutar esta tarea una sola vez. Haga clic en **Siguiente**.
3. Haga clic en Examinar y seleccione la aplicación Calculadora.
4. Escriba **Usuario1**: antes de la ruta de acceso de la aplicación (Usuario1: '/Applications/Calculator.app/Contents/MacOs/Calculator') y haga clic en **Siguiente**.
5. Seleccione la hora a la que desea ejecutar la tarea y haga clic en **Siguiente**.
6. Si la tarea no se puede ejecutar, seleccione una opción alternativa y haga clic en **Siguiente**.
7. Haga clic en **Finalizar**.
8. La función Tareas programadas de ESET iniciará la aplicación Calculadora a la hora que haya seleccionado.



Ejemplo: Tarea de actualización

En este ejemplo vamos a crear una tarea de actualización que se ejecutará a una hora concreta.

1. En el menú desplegable **Tarea programada**, seleccione **Actualización**.
2. Introduzca el nombre de la tarea en el campo **Nombre de la tarea**.
3. Seleccione la frecuencia de la tarea en el menú desplegable **Ejecutar tarea**. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización. Si selecciona **Definido por el usuario**, se le pedirá que especifique la fecha/hora en formato cron (para obtener más información, consulte el apartado [Creación de tareas definidas por el usuario](#)).
4. En el siguiente paso, defina la acción que deberá llevarse a cabo si la tarea no se puede realizar o completar a la hora programada.
5. En el último paso se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar**. La nueva tarea programada se agregará a la lista de tareas programadas actualmente.

De forma predeterminada, ESET Cyber Security Pro contiene tareas programadas predefinidas para garantizar el correcto funcionamiento del producto. Estas tareas no se deben modificar, por lo que están ocultas de forma predeterminada. Para ver estas tareas, vaya a **Configuración > Introducir preferencias de aplicación** en el menú principal (o pulse *cmd+,*) > **Planificador de tareas** y seleccione **Mostrar tareas de sistema**.

Análisis como propietario de un directorio

Puede analizar directorios como propietario del directorio:

```
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -  
f %u "$VOLUME" ` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -  
f /tmp/scan_log "$VOLUME"; done
```

También puede analizar la carpeta /tmp como el usuario que ha iniciado sesión:

```
root:sudo -u \#`stat -  
f %u /dev/console ` '/Applications/ESET Cyber Security.app/Contents/MacOS/esets_scan' -  
/tmp
```

Creación de tareas definidas por el usuario

La fecha y la hora de la tarea **Definida por el usuario** se deben introducir en formato cron ampliado por años (una cadena compuesta de 6 campos separados por un espacio en blanco):

minuto(0-59) hora(0-23) día del mes(1-31) mes(1-12) año(1970-2099) día de la semana(0-7) (Domingo = 0 o 7)

Ejemplo:

30 6 22 3 2012 4

Caracteres especiales admitidos en las expresiones cron:

- Asterisco (*): la expresión coincidirá con todos los valores del campo; por ejemplo, un asterisco en el tercer campo (día del mes) significa todos los días.
- Guion (-): define los rangos, por ejemplo 3-9.
- Coma (,): separa los elementos de una lista; por ejemplo, 1,3,7,8.
- Barra (/): define incrementos de rangos: p. ej., 3-28/5 en el tercer campo (día del mes) significa tercer día del mes y, luego, cada 5 días.

No se admiten nombres de días (Monday-Sunday) ni de meses (January-December).



Ejecución de comandos

si define el día del mes y el día de la semana, el comando solo se ejecutará cuando ambos campos coincidan.

Cuarentena

El objetivo principal de la cuarentena es almacenar de forma segura los archivos infectados. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Cyber Security Pro los detecta incorrectamente como infectados.

Puede poner en cuarentena cualquier archivo. Es aconsejable si el comportamiento de un archivo es sospechoso y no lo ha detectado el análisis. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de amenazas de ESET.

Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en las que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, etc.) y el número de amenazas (por ejemplo, si se trata de un archivo que contenga varias amenazas). La carpeta de cuarentena con archivos en cuarentena () permanece en el sistema incluso tras desinstalar ESET Cyber Security Pro. Los archivos en cuarentena se guardan en un formato cifrado seguro y se pueden restaurar tras la instalación de ESET Cyber Security Pro.

Puesta de archivos en cuarentena

ESET Cyber Security Pro copia en cuarentena automáticamente los archivos eliminados (si no ha cancelado esta opción en la ventana de alerta). Puede poner manualmente en cuarentena cualquier archivo sospechoso haciendo clic en **Cuarentena...**. El menú contextual también se puede utilizar con este fin: pulse la tecla Control, haga clic en el espacio en blanco, seleccione **Cuarentena**, elija el archivo que desee poner en cuarentena y haga clic en **Abrir**.

Restauración de archivos de cuarentena

Los archivos en cuarentena también se pueden devolver a su ubicación original; para ello, elija un archivo en cuarentena y haga clic en **Restaurar**. La opción de restauración también está disponible en el menú contextual; pulse la tecla Control y haga clic en un archivo de la ventana Cuarentena y, a continuación, haga clic en **Restaurar**. 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.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o se ha evaluado incorrectamente un archivo como infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, se ha copiado a cuarentena, envíe el archivo al laboratorio de amenazas de ESET. Para enviar un archivo de cuarentena, pulse la tecla Control y haga clic en el archivo y seleccione **Enviar archivo para su análisis** en el menú contextual.

Procesos en ejecución

En la lista **Procesos en ejecución** se muestran los procesos que se están ejecutando en el ordenador. ESET Cyber Security Pro contiene información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET Live Grid.

- **Proceso:** nombre del proceso que se está ejecutando actualmente en el ordenador. En el Monitor de Actividad (disponible en */Aplicaciones/Utilidades*) también se muestran todos los procesos en ejecución.
- **Nivel de riesgo:** en la mayoría de los casos, ESET Cyber Security Pro y la tecnología ESET Live Grid asignan un nivel de riesgo a los objetos (archivos, procesos, etc.) mediante una serie de reglas heurísticas que examinan las características de cada uno de ellos y, después, estiman el potencial de actividad maliciosa. De acuerdo con esta heurística, se asigna un nivel de riesgo a los diferentes objetos. Las aplicaciones conocidas marcadas en verde son totalmente seguras (incluidas en lista blanca) y no se analizarán. Esto aumenta la velocidad de los análisis a petición y en tiempo real. El hecho de que una aplicación esté marcada como desconocida (amarillo), no implica necesariamente que se trate de software malicioso. Normalmente se trata de una aplicación reciente. Si no está seguro de la clasificación de un archivo, puede enviarlo al laboratorio de amenazas de ESET para su análisis. Si resulta que el archivo es una aplicación maliciosa, su firma se agregará a una de las siguientes actualizaciones.
- **Número de usuarios:** número de usuarios que utilizan una aplicación determinada. La tecnología ESET Live Grid se encarga de recopilar esta información.
- **Hora de la detección:** periodo de tiempo transcurrido desde que la tecnología ESET LiveGrid® detectó la aplicación.

- **Id. de paquete de aplicaciones:** nombre del proveedor o el proceso de la aplicación.

Al hacer clic en un proceso, se muestra la información siguiente en la parte inferior de la ventana:

- **Archivo:** ubicación de una aplicación en el ordenador.
- **Tamaño del archivo:** tamaño físico del archivo en el disco.
- **Descripción del archivo:** características del archivo en función de su descripción del sistema operativo.
- **Id. de paquete de aplicaciones:** nombre del proveedor o el proceso de la aplicación.
- **Versión del archivo:** información sobre el editor de la aplicación.
- **Nombre del producto:** nombre de la aplicación o nombre comercial.

Conexiones de red

Conexiones de red presenta una lista de las conexiones de red activas en su ordenador. ESET Cyber Security Pro aporta información detallada de cada conexión y le permite crear una regla con la que bloquear dichas conexiones.

Crear una regla de bloqueo para esta conexión

ESET Cyber Security Pro le permite crear una regla de bloqueo para cada conexión en el administrador de **Conexiones de red**. Para crear una regla de bloqueo, haga clic con el botón derecho del ratón en la conexión y seleccione **Crear una regla de bloqueo para esta conexión**.

1. Seleccione el **Perfil** de conexión para el que desea crear la regla, y escriba el nombre de la regla. Seleccione la aplicación a la que se debe aplicar la regla o marque la casilla de verificación para aplicar la regla a todas las aplicaciones.
2. Seleccione una acción para la conexión, ya sea denegarla (bloquearla) o permitirla. Seleccione la dirección de comunicación a la que se debe aplicar la regla. Si desea crear un archivo de registro para la regla, haga clic en **Regla de registro**.
3. Seleccione el protocolo de conexión y los tipos de puerto. Seleccione el puerto para el servicio o especifique un intervalo de puertos con el formato: desde-hasta.
4. Seleccione el destino e introduzca la información en el campo correspondiente, en función de su destino.

Live Grid

El sistema de alerta temprana Live Grid informa a ESET de las nuevas amenazas de forma inmediata y continua. El sistema de alerta temprana Live Grid bidireccional tiene un único objetivo: mejorar la protección que le ofrecemos. La mejor manera de garantizar la detección de nuevas amenazas en cuanto aparecen es un "enlace" al mayor número posible de clientes que funcionen como exploradores de amenazas. Existen dos opciones:

1. Puede optar por no activar el sistema de alerta temprana Live Grid. El software no perderá funcionalidad y seguirá recibiendo la mejor protección que ofrecemos.
2. Puede configurar el sistema de alerta temprana Live Grid para que envíe información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso. Esta información se puede enviar a ESET para que realice un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar su motor de

detección y a mejorar las funciones de detección de amenazas del programa.

El sistema de alerta temprana Live Grid recopilará información acerca de su ordenador que esté relacionada con amenazas detectadas recientemente. Esta información puede incluir una muestra o una copia del archivo en el que haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la fecha y la hora, el proceso mediante el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

Aunque existe la posibilidad de que este proceso revele cierta información acerca del usuario o su ordenador (nombres de usuario en una ruta al directorio, etc.) al laboratorio de amenazas de ESET, esta información no se utilizará con NINGÚN propósito que no esté relacionado con la ayuda necesaria para responder inmediatamente a nuevas amenazas.

Para acceder a la configuración de Live Grid desde el menú principal, haga clic en **Configuración > Introducir preferencias de la aplicación....** (o pulse *cmd+,*) > **Live Grid**. Seleccione **Activar el sistema de alerta temprana Live Grid** para activar Live Grid y, a continuación, haga clic en **Configuración**, junto a **Opciones avanzadas**.

Configuración de Live Grid

ESET Cyber Security Pro está configurado de forma predeterminada para enviar los archivos sospechosos para su análisis detallado en el laboratorio de amenazas de ESET. Si no desea que estos archivos se envíen automáticamente, anule la selección de la opción **Enviar archivos**.

Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio para su análisis. Para ello, haga clic en **Herramientas > Enviar muestra para su análisis** en la ventana principal del programa. Si es una aplicación maliciosa, su detección se agregará a una próxima actualización.

Enviar estadísticas anónimas: el sistema de alerta temprana ESET Live Grid recopila información anónima acerca del ordenador relacionada con las amenazas detectadas recientemente. Esta información incluye el nombre de la amenaza, la fecha y la hora en que se detectó, la versión del producto de seguridad de ESET, la versión del sistema operativo de su ordenador y la configuración regional. Normalmente, estas estadísticas se envían a los servidores de ESET una o dos veces al día.

Filtro de exclusión: esta opción le permite excluir del envío determinados tipos de archivo. y 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, .rtf, etc.). Si lo desea, puede añadir tipos de archivo a la lista de archivos excluidos.

Correo electrónico de contacto (opcional): es posible utilizar su dirección de correo electrónico para comunicarnos con usted cuando se requiera más información para poder realizar el análisis. Tenga en cuenta que no recibirá una respuesta de ESET a menos que sea necesaria más información.

Enviar muestra para el análisis

Si encuentra un archivo sospechoso en su ordenador, puede enviarlo al laboratorio de investigación de ESET para que lo analicen.



Antes de enviar muestras a ESET

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

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

Para enviar una muestra para su análisis, utilice el formulario de envío de muestras de su producto. Se encuentra en **Herramientas > Enviar muestra para su análisis**.

En el formulario **Enviar muestra para su análisis**, rellene los siguientes datos:

Archivo: la ruta de acceso del archivo que quiere enviar.

Comentario: describa el motivo por el que envía el archivo.

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



Puede que no reciba ninguna respuesta de ESET.

No obtendrá ninguna respuesta de ESET a menos que sea necesario que envíe información adicional. Cada día, nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.


Si la muestra resulta ser una aplicación o un sitio web maliciosos, su detección se agregará a una actualización futura de ESET.

Interfaz de usuario

Las opciones de configuración de la interfaz de usuario le permiten ajustar el entorno de trabajo según sus necesidades. Para acceder a estas opciones desde el menú principal, haga clic en **Configuración > Introducir preferencias de aplicación** (o pulse `cmd+,`) > **Interfaz**.

- Si desea ver la pantalla de inicio de ESET Cyber Security Pro al iniciar el sistema, seleccione **Mostrar pantalla inicial con la carga del sistema**.
- **Aplicación presente en el Dock** le permite visualizar el icono de ESET Cyber Security Pro ® en el Dock de macOS, así como alternar ESET Cyber Security Pro y otras aplicaciones en ejecución pulsando `cmd + tabulador`. Los cambios se aplican tras reiniciar ESET Cyber Security Pro (normalmente se activa con el reinicio del sistema).
- La opción **Utilizar menú estándar** le permite utilizar determinados accesos directos del teclado (consulte [Accesos directos del teclado](#)) y ver los elementos del menú estándar (Interfaz de usuario, Configuración y Herramientas) en la barra de menús de macOS (parte superior de la pantalla).
- Para activar el uso de las sugerencias para determinadas opciones de ESET Cyber Security Pro, seleccione **Mostrar sugerencias y consejos útiles**.
- **Mostrar archivos ocultos** le permite ver y seleccionar los archivos ocultos en la configuración de **Objetos de**

análisis de un Análisis del ordenador.

- De manera predeterminada, el icono de ESET Cyber Security Pro  se muestra en los extras de la barra de menús que aparecen en la parte derecha de la barra de menús de macOS (parte superior de la pantalla). Para desactivar esta configuración, anule la selección de **Mostrar icono en los extras de la barra de menús**. Este cambio se aplica tras reiniciar ESET Cyber Security Pro (normalmente se activa con el reinicio del sistema).

Alertas y notificaciones

La sección **Alertas y notificaciones** le permite configurar la gestión de las alertas de amenazas y las notificaciones del sistema por parte de ESET Cyber Security Pro.

Si desactiva **Mostrar alertas**, se cancelarán todas las ventanas de alertas; esta opción solo se recomienda en situaciones específicas. Para la mayoría de los usuarios, se recomienda mantener la opción predeterminada (activada). Las opciones avanzadas se describen [en este capítulo](#).

Si selecciona **Mostrar notificaciones en el escritorio**, las ventanas de alertas que no requieran la interacción del usuario se mostrarán en el escritorio (de forma predeterminada, en la esquina superior derecha de la ventana). Si desea definir el periodo durante el que se mostrará una notificación, ajuste el valor de **Cerrar automáticamente las notificaciones después de X segundos** (5 segundos de manera predeterminada).

Desde la versión 6.2 de ESET Cyber Security Pro también puede evitar que **Estados de protección** determinados se muestren en la pantalla principal del programa (ventana **Estado de protección**). Para obtener más información sobre este aspecto, consulte los [Estados de protección](#).

Mostrar alertas

ESET Cyber Security Pro muestra cuadros de diálogo de alerta para informarle sobre nuevas versiones del programa, actualizaciones del sistema operativo, la desactivación de determinados componentes del programa, la eliminación de registros, etc. Seleccione **No volver a mostrar este cuadro de diálogo** para suprimir cada notificación.

En **Lista de cuadros de diálogo** (**Configuración** > **Introducir preferencias de aplicación** > **Alertas y notificaciones** > **Configuración**) se muestra la lista de todos los cuadros de diálogo de alerta que activa ESET Cyber Security Pro. Para activar o suprimir cada notificación, active la casilla de verificación que aparece a la izquierda de **Nombre del cuadro de diálogo**. También puede definir las **Condiciones de visualización** bajo las que se mostrarán las notificaciones sobre nuevas versiones del programa y actualizaciones del sistema operativo.

Estados de protección

El estado de protección actual de ESET Cyber Security Pro se puede modificar activando o desactivando los estados en **Configuración** > **Introducir las preferencias de la aplicación...** > **Alertas y notificaciones** > **Mostrar en la pantalla Estado de protección: Configuración**. El estado de diversas características del programa se mostrará u ocultará de la pantalla principal de ESET Cyber Security Pro (ventana **Estado de protección**).

Puede ocultar el estado de protección de las siguientes características del programa:

- Cortafuegos

- Anti-Phishing
- Protección del acceso a la Web
- Protección de clientes de correo electrónico
- Actualizaciones del sistema operativo
- Caducidad de la licencia
- Es necesario reiniciar el ordenador

Privilegios

La configuración de ESET Cyber Security Pro puede ser muy importante para la política de seguridad de la empresa. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Por este motivo, puede definir qué usuarios tienen permiso para editar la configuración del programa.

Para especificar los usuarios con privilegios, haga clic en **Configuración > Introducir las preferencias de la aplicación** (o pulse *cmd+,*) > **Privilegios**. Seleccione los usuarios o grupos en la lista de la izquierda y haga clic en **Agregar**. Para ver todos los usuarios o grupos del sistema, seleccione **Mostrar todos los usuarios o grupos**. Para quitar un usuario, seleccione su nombre en la lista **Usuarios seleccionados** de la derecha y haga clic en **Quitar**.



Acerca de la actualización

Si la lista Usuarios seleccionados se deja vacía, se considerará que todos los usuarios tienen privilegios.

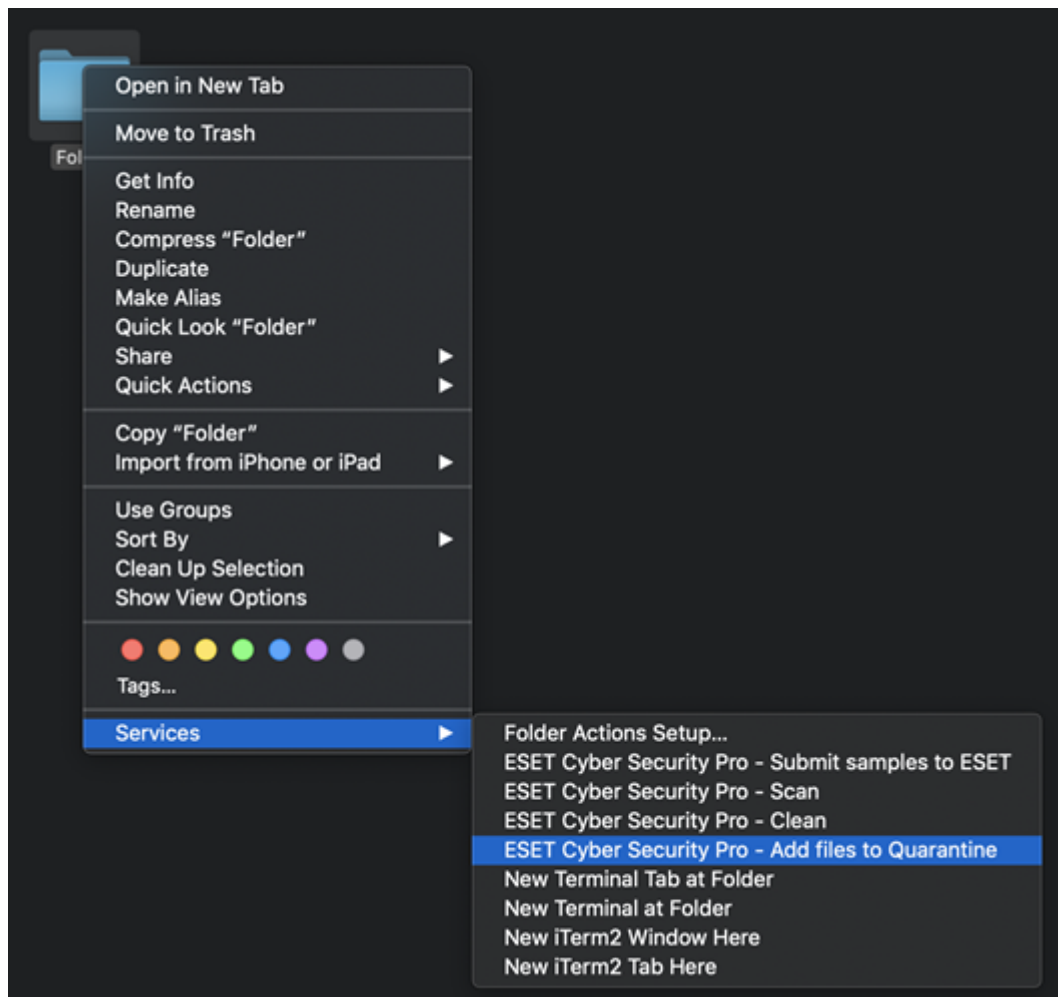
Menú contextual

La integración del menú contextual se puede activar haciendo clic en **Configuración > Introducir las preferencias de la aplicación** (o pulse *cmd+,*) > **Menú contextual** mediante la selección de la opción **Integrar en el menú contextual**. Es necesario cerrar sesión o reiniciar el ordenador para que se apliquen los cambios. Las opciones del menú contextual estarán disponibles en la ventana **Finder** al hacer CTRL + clic en cualquier archivo.

Puede seleccionar las opciones que se mostrarán en el menú contextual. Puede mostrar la opción **Solo analizar**, que le permitirá analizar el archivo seleccionado; la opción **Solo desinfectar** le permitirá desinfectar el archivo seleccionado desde el menú contextual. Inicie la desinfección si un archivo ha sido infectado por un virus que le haya añadido código malicioso. Si es el caso, primero intente desinfectar el archivo infectado para devolverlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.

Si selecciona la opción **Todo**, puede realizar las siguientes tareas desde el menú contextual:

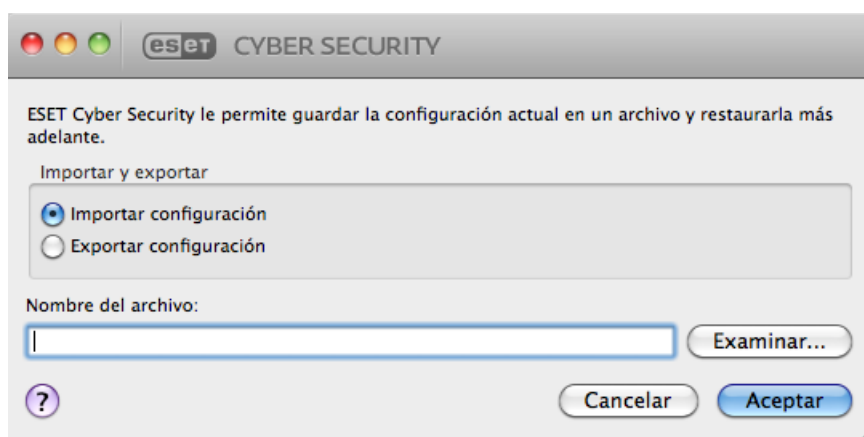
- Enviar muestras a ESET
- Analizar
- Limpio
- [Agregar archivos a la cuarentena](#)



Importar y exportar configuración

Para importar una configuración existente o exportar su configuración de ESET Cyber Security Pro, haga clic en **Configuración > Importar o exportar configuración**.

La importación y la exportación son útiles para realizar copias de seguridad de la configuración actual de ESET Cyber Security Pro y utilizarla más adelante. La exportación de la configuración también es útil para los usuarios que desean utilizar su configuración preferida de ESET Cyber Security Pro en diferentes sistemas. De esta forma puede importar fácilmente el archivo de configuración para transferir los ajustes deseados.



Para importar una configuración, seleccione **Importar configuración** y haga clic en **Examinar** para desplazarse

hasta el archivo de configuración que quiera importar. Para exportar, seleccione **Exportar configuración** y utilice el navegador para seleccionar la ubicación del ordenador en la que desea guardar el archivo de configuración.

Configuración del servidor Proxy

Los ajustes del servidor Proxy se pueden configurar en **Configuración > Introducir preferencias de aplicación** (o pulse *cmd +,*) > **Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se define la configuración global del servidor Proxy para todas las funciones de ESET Cyber Security Pro. Los parámetros definidos aquí los utilizarán todos los módulos que necesiten conexión a Internet. ESET Cyber Security Pro es compatible con los tipos de autenticación de acceso básico y NTLM (administrador de LAN NT).

Para especificar la configuración del servidor Proxy en este nivel, seleccione **Conexión mediante servidor Proxy** y, a continuación, introduzca la dirección IP o la URL del servidor Proxy en el campo **Servidor Proxy**. En el campo Puerto, especifique el puerto en el que el servidor proxy recibe conexiones (el 3128, de forma predeterminada). También puede hacer clic en **Detectar** para que el programa cumpla los dos campos.

Si la comunicación con el servidor proxy requiere autenticación, introduzca un **Nombre de usuario** y una **Contraseña** válidos en los campos correspondientes.

Acuerdo de licencia para el usuario final

IMPORTANTE: Lea los términos y condiciones de la aplicación del producto que se detallan a continuación antes de descargarlo, instalarlo, copiarlo o utilizarlo. **LA DESCARGA, LA INSTALACIÓN, LA COPIA O LA UTILIZACIÓN DEL SOFTWARE IMPLICAN SU ACEPTACIÓN DE ESTOS TÉRMINOS Y CONDICIONES Y DE LA [POLÍTICA DE PRIVACIDAD](#).**

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final (en adelante, "Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 (en adelante, "ESET" o "Proveedor") y usted, una persona física o jurídica (en adelante, "Usted" o "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, la descarga, la copia o la utilización del Software, expresa su aceptación de los términos y condiciones de este Acuerdo. Si no acepta todos los términos y condiciones de este Acuerdo, haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE SU UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE ACEPTA SU SUJECCIÓN A LOS TÉRMINOS Y CONDICIONES.

1. **Software.** En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este

Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo (de aquí en adelante, la "Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. Instalación, Ordenador y una Clave de licencia. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. Licencia. Siempre que haya aceptado los términos de este Acuerdo y cumpla todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (en adelante denominados "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (de aquí en adelante, "un AUC") cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíquesele inmediatamente al Proveedor.

c) **Business Edition.** Debe obtener una versión Business Edition del Software para poder utilizarlo en servidores, relays abiertos y puertas de enlace de correo, así como en puertas de enlace a Internet.

d) **Vigencia de la licencia.** Tiene derecho a utilizar el Software durante un período de tiempo limitado.

e) **Software OEM.** El software OEM solo se puede utilizar en el ordenador con el que se le proporcionó. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR.** El Software cuya venta esté prohibida o de prueba no se puede pagar, y únicamente se debe utilizar para demostraciones o para probar las características del Software.

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la licencia, el usuario debe eliminar, destruir o devolver (a sus expensas) el software y todas las copias de seguridad del mismo a ESET o al lugar donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El Proveedor podrá publicar ocasionalmente actualizaciones del Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para suministrar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

b) **Envío de amenazas e información al proveedor.** El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet (de aquí en adelante "amenazas") y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el ordenador o la plataforma en la que el Software está instalado o información sobre las operaciones y las funciones del Software e información sobre dispositivos de la red local como tipo, proveedor, modelo o nombre del dispositivo (de aquí en adelante "información"). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las Amenazas junto con los metadatos asociados.

La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La función del sistema de reputación LiveGrid incluye la recopilación y el envío al proveedor de algoritmos hash unidireccionales relacionados con las amenazas. Esta función se activa en la sección de configuración estándar del software.

ii. La función del Sistema de Respuesta LiveGrid incluye la recopilación y el envío al Proveedor de las Amenazas con los metadatos y la Información asociados. Esta función la puede activar el Usuario final durante el proceso de instalación del Software.

El Proveedor solo podrá utilizar la Información y las Amenazas recibidas con fines de análisis e investigación de las Amenazas y mejora de la verificación de la autenticidad del Software y de la Licencia, y deberá tomar las medidas pertinentes para garantizar la seguridad de las Amenazas y la Información recibidas. Si se activa esta función del Software, el Proveedor podrá recopilar y procesar las Amenazas y la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. Estas funciones se pueden desactivar en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

Tras la terminación de este Acuerdo, el Proveedor y sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, estarán autorizados a transferir, procesar y almacenar sus datos identificativos fundamentales para fines relacionados con la facturación, la ejecución del Acuerdo y la transmisión de notificaciones en su Ordenador. Por la presente acepta recibir notificaciones y mensajes, lo que incluye, entre otros elementos, información de marketing.

En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos como persona interesada. También puede visitarla desde la sección de ayuda del Software.

5. Ejercicio de los derechos de usuario final. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los Ordenadores o los sistemas informáticos para los que ha obtenido una Licencia.

6. Restricciones de los derechos. No puede copiar, distribuir, extraer componentes ni crear versiones derivadas del software. El uso del software está sujeto a las siguientes restricciones:

- a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.
- b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.
- c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.
- d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.
- e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.
- f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.
- g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no

autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. Copyright. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

8. Reserva de derechos. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. Versiones en varios idiomas, software en soporte dual, varias copias. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. Comienzo y rescisión del Acuerdo. Este acuerdo es efectivo a partir de la fecha en que acepte sus términos. Puede terminar este acuerdo en cualquier momento mediante la desinstalación, destrucción o devolución (a sus expensas) del software, todas las copias de seguridad y todo el material relacionado que le hayan suministrado el proveedor o sus socios comerciales. Independientemente del modo de terminación de este acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán en vigor de forma ilimitada.

11. DECLARACIONES DEL USUARIO FINAL. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA "TAL CUAL", SIN GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y DENTRO DEL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, SUS PROVEEDORES DE LICENCIAS O SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, EXPRESA O IMPLÍCITA; EN PARTICULAR, NINGUNA GARANTÍA DE VENTAS O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJA UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE SATISFAGAN SUS REQUISITOS O QUE EL SOFTWARE FUNCIONE SIN INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN DEL SOFTWARE PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LA INSTALACIÓN, EL USO Y LOS RESULTADOS OBTENIDOS.

12. Ninguna obligación adicional. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. LIMITACIÓN DE RESPONSABILIDAD. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE LAS PÉRDIDAS DE BENEFICIOS, INGRESOS, VENTAS, DATOS O COSTES SOPORTADOS PARA OBTENER PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS CAUSADOS DE

CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, CONDUCTA INADECUADA INTENCIONADA, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO A LA UTILIZACIÓN O LA INCAPACIDAD DE UTILIZACIÓN DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR O SUS PROVEEDORES DE LICENCIAS HAYAN SIDO NOTIFICADOS DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Ninguna de las disposiciones de este acuerdo se establece en perjuicio de los derechos estatutarios de una parte que actúe como consumidor en contra de lo aquí dispuesto.

15. Soporte técnico. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin ningún tipo de garantía o declaración. El usuario final debe realizar una copia de seguridad de todos los datos, aplicaciones de software y programas almacenados en el ordenador antes de recibir soporte técnico. ESET y/o los terceros contratados por ESET no se hacen responsables de los daños, las pérdidas de datos, elementos en propiedad, software o hardware ni las pérdidas de ingresos a causa de la prestación del servicio de soporte técnico. ESET y/o los terceros contratados por ESET se reservan el derecho de determinar que la solución de un problema no entra dentro del ámbito de soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

16. Transferencia de la licencia. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal como se especifica en el artículo 17.

17. Verificación de la autenticidad del Software. El Usuario final puede demostrar su derecho a utilizar el Software de las siguientes maneras: (i) mediante un certificado de licencia emitido por el Proveedor o un tercero designado por el Proveedor; (ii) mediante un acuerdo de licencia por escrito, si se ha celebrado dicho acuerdo; (iii) mediante el envío de un mensaje de correo electrónico enviado por el Proveedor con la información de la licencia (nombre de usuario y contraseña). Pueden ser necesarios los datos de Licencia y de identificación del Usuario final de acuerdo con la Política de Privacidad para verificar la autenticidad del Software.

18. Licencia para organismos públicos y gubernamentales de EE.UU.. El software se proporcionará a los organismos públicos, incluido el gobierno de Estados Unidos, con los derechos y las restricciones de licencia descritos en este acuerdo.

19. Cumplimiento de las normas de control comercial.

a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo (en adelante, las "Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino

Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen (en adelante, las "Leyes de control de las exportaciones") y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen (en adelante, las "Leyes sancionadoras").

b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es probable que incumpla lo dispuesto en el Artículo 19.a del Acuerdo; o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud del Acuerdo podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

c) Ninguna disposición del Acuerdo tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe interpretarse en ese sentido.

20. Avisos. Los avisos y el Software y la Documentación devueltos deben enviarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. Legislación aplicable. Este acuerdo se registrará e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. Disposiciones generales. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. En caso de discrepancia entre las versiones de este acuerdo en diferentes idiomas, prevalecerá la versión en inglés. Este acuerdo solo se puede modificar por escrito y con la firma de un representante autorizado del proveedor o una persona autorizada expresamente para este fin mediante un poder notarial.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

EULA ID: HOM-ECS-20-01

Política de privacidad

ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, República Eslovaca, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, número de registro de la empresa 31333532, como controlador de datos («ESET» o «Nosotros»), quiere ser transparente en cuanto al procesamiento de datos personales y la privacidad de sus clientes. Para alcanzar este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes («Usuario final» o «Usted») sobre los siguientes temas:

- Procesamiento de datos personales
- Confidencialidad de los datos
- Derechos del titular de los datos

Procesamiento de datos personales

Los servicios prestados por ESET implementados en el producto se prestan de acuerdo con los términos del Acuerdo de licencia para el usuario final ("EULA"), pero algunos pueden requerir atención específica. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos diferentes servicios descritos en el EULA y en la documentación de producto, como el servicio de actualización, ESET LiveGrid®, protección contra mal uso de datos, soporte, etc. Para que todo funcione, debemos recopilar la siguiente información:

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Algoritmos hash unidireccionales relativos a infiltraciones que forman parte del sistema de reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones contra malware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.
- Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe

Oinfiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;

Oinformación sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;

Oinformación relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;

Oarchivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o

formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

- La información de licencia, como el ID de licencia, y los datos personales como el nombre, los apellidos, la dirección y la dirección de correo electrónico son necesarios para la facturación, la verificación de la autenticidad de la licencia y la prestación de nuestros servicios.
- La información de contacto y los datos contenidos en sus solicitudes de soporte pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Es posible que le pidamos que nos facilite otra información para prestar el servicio de asistencia técnica.

Confidencialidad de los datos

ESET es una empresa que opera en todo el mundo a través de filiales o socios que forman parte de su red de distribución, servicio y asistencia. La información procesada por ESET puede transferirse a y de filiales o socios para cumplir el CLUF en aspectos como la prestación de servicios, la asistencia o la facturación. Según su ubicación y el servicio que decida utilizar, podemos vernos obligados a transferir sus datos a un país para el que no exista una decisión de adecuación de la Comisión Europea. Incluso en este caso, todas las transferencias de información cumplen la legislación sobre protección de datos y solo se realizan si es necesario. Deben implementarse sin excepción las cláusulas contractuales tipo, las reglas corporativas vinculantes u otra medida de seguridad adecuada.

Hacemos todo lo posible para evitar que los datos se almacenen más tiempo del necesario durante la prestación de servicios de acuerdo con el EULA. Nuestro período de retención puede ser mayor que el período de validez de su licencia para que tenga tiempo de renovarla de forma sencilla y cómoda. Pueden continuar tratándose estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar en todo momento la confidencialidad, la integridad, la disponibilidad y la resiliencia de los sistemas y los servicios de tratamiento. Sin embargo, en caso de filtración de información que ponga en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora y a los interesados. Como titular de los datos, tiene derecho a presentar una reclamación ante una autoridad supervisora.

Derechos del titular de los datos.

ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. Sin perjuicio de las condiciones establecidas por las leyes de protección de datos aplicables, en su calidad de interesado, tiene los siguientes derechos:

- derecho a solicitar a ESET acceso a sus datos personales;
- derecho de rectificación de sus datos personales en caso de que sean incorrectos (también tiene derecho a completarlos en caso de que estén incompletos);
- derecho a solicitar la eliminación de sus datos personales;
- derecho a solicitar la restricción del procesamiento de sus datos personales;
- derecho a oponerse al procesamiento;

- derecho a presentar una reclamación y
- derecho a la portabilidad de datos.

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk