

# ESET Cyber Security Pro

Guía para el usuario

[Haga clic aquí para mostrar la versión de ayuda de este documento](#)

Copyright ©2023 de ESET, spol. s r.o.

ESET Cyber Security Pro ha sido 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 o 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 la aplicación sin previo aviso.

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

REV. 19/03/2023

1 ESET Cyber Security Pro .....	1
<b>1.1 Novedades de la versión 6</b> .....	1
<b>1.2 Requisitos del sistema</b> .....	1
2 Instalación .....	2
<b>2.1 Instalación típica</b> .....	2
<b>2.2 Instalación personalizada</b> .....	4
<b>2.3 Permitir extensiones del sistema</b> .....	5
<b>2.4 Permitir acceso completo al disco</b> .....	6
3 Activación del producto .....	6
4 Desinstalación .....	7
5 Resumen general básico .....	7
<b>5.1 Accesos directos del teclado</b> .....	7
<b>5.2 Comprobación del estado de protección</b> .....	8
<b>5.3 Qué hacer si el programa no funciona correctamente</b> .....	8
6 Protección del equipo .....	9
<b>6.1 Protección antivirus y antispyware</b> .....	9
6.1 General .....	9
6.1 Exclusiones .....	9
6.1 Protección de inicio .....	10
6.1 Protección del sistema de archivos en tiempo real .....	10
6.1 Opciones avanzadas .....	11
6.1 Cuándo modificar la configuración de la protección en tiempo real .....	11
6.1 Verificación de la protección en tiempo real .....	11
6.1 Qué hacer si la protección en tiempo real no funciona .....	12
6.1 Exploración del equipo a petición .....	12
6.1 Tipo de exploración .....	13
6.1 Exploración inteligente .....	13
6.1 Exploración personalizada .....	13
6.1 Objetos para explorar .....	14
6.1 Perfiles de exploración .....	14
6.1 Configuración de los 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 Infiltración detectada .....	18
<b>6.2 Exploración y bloqueo de medios extraíbles</b> .....	19
7 Anti-Phishing .....	20
8 Firewall .....	20
<b>8.1 Modos de filtrado</b> .....	21
<b>8.2 Reglas de firewall</b> .....	21
8.2 Creación de reglas nuevas .....	22
<b>8.3 Zonas de firewall</b> .....	22
<b>8.4 Perfiles de firewall</b> .....	22
<b>8.5 Registros de firewall</b> .....	23
9 Protección web y de correo electrónico .....	23
<b>9.1 Protección web</b> .....	24
9.1 Puertos .....	24

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

# ESET Cyber Security Pro

ESET Cyber Security Pro representa un nuevo enfoque de la seguridad del equipo verdaderamente integrada. La versión más reciente del motor de exploración ThreatSense®, combinado con la protección del cliente de correo electrónico, firewall y control parental, utilizan velocidad y precisión para mantener su equipo seguro. Esto resulta en un sistema inteligente constantemente en alerta para defender su equipo de ataques y software maliciosos.

ESET Cyber Security Pro es una solución de seguridad completa producida mediante un esfuerzo de largo plazo con el fin de combinar la protección máxima con un tamaño mínimo en el sistema. Basadas en inteligencia artificial, las tecnologías avanzadas que comprende ESET Cyber Security Pro son capaces de eliminar proactivamente la infiltración a través de virus, gusanos, troyanos, spyware, adware, rootkits y otros ataques transmitidos por Internet sin afectar el rendimiento del sistema.

## Novedades de la versión 6

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

- **Soporte de arquitectura de 64 bits**
- **Anti-Phishing:** evita que los sitios web disfrazados de confiables adquieran su información personal
- **Actualizaciones del sistema:** ESET Cyber Security Pro la versión 6 cuenta con diferentes arreglos y mejoras que incluyen notificaciones para actualizaciones del sistema operativo. Para obtener más información, consulte la sección [Actualizaciones del sistema](#).
- **Estados de protección:** oculta las notificaciones de la pantalla Estado de protección (por ejemplo, *Protección de correo electrónico deshabilitada* o *Debe reiniciar el equipo*)
- **Medios que se analizarán:** determinados tipos de medios se pueden excluir del explorador en tiempo real (unidades locales, medios extraíbles, medios de red)
- **Conexiones de red:** muestra las conexiones de red en su equipo y le permite crear reglas para estas conexiones.

Para obtener más detalles sobre las nuevas características de ESET Cyber Security Pro, lea el [siguiente artículo de la Base de conocimiento de ESET](#):

## Requisitos del sistema

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

	Requisitos del sistema:
Arquitectura del 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 existente con Intel, la versión 6.10.900.0 de ESET Cyber Security Pro y posteriores son compatibles con los chips Apple M1 y M2 que usan Rosetta 2

## Instalación

Antes de comenzar el proceso de instalación, cierre todos los programas abiertos en el equipo. ESET Cyber Security Pro contiene componentes que pueden entrar en conflicto con otros programas antivirus instalados en su equipo. ESET recomienda firmemente eliminar cualquier otro programa antivirus para evitar problemas potenciales.

Para iniciar el asistente de instalación, realice una de las siguientes acciones:

- Si realiza la instalación desde un archivo descargado del sitio web de ESET, abra el archivo y haga doble clic en el ícono **Instalar**.
- Si realiza la instalación desde un CD/DVD, inserte el disco en su equipo, ábralo desde el Escritorio o la ventana **Finder** haga doble clic en el ícono **Instalar**.



El asistente de instalación lo guiará durante la configuración básica. Durante la etapa inicial de la instalación, el programa de instalación buscará automáticamente en línea la versión más reciente del producto. Si se encuentra una versión más reciente, se le dará la opción de descargarla antes de continuar con el proceso de instalación.

Luego de aceptar el Acuerdo de licencia de usuario final, se le pedirá que seleccione uno de los siguientes modos:

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

## Instalación típica

El modo de instalación típica incluye las opciones de configuración apropiadas para la mayoría de los usuarios. Esta configuración proporciona la máxima seguridad combinada con un excelente rendimiento del sistema. La instalación típica es la opción predeterminada y la recomendada para aquellos que no tienen requisitos

particulares sobre una configuración específica.

1. En la ventana **ESET LiveGrid**, seleccione su opción preferida y haga clic en **Continuar**. Si más adelante decide que quiere cambiar esta configuración, podrá hacerlo mediante la **configuración de LiveGrid**. Para obtener más información sobre ESET Live Grid, [visite nuestro Glosario](#).
2. En la ventana **Aplicaciones potencialmente no deseadas**, seleccione su opción preferida (consulte [¿Qué es una aplicación potencialmente no deseada?](#)) y haga clic en **Continuar**. Si más adelante decide que quiere cambiar esta configuración, utilice la **Configuración avanzada**.
3. Haga clic en **Instalar**. Si se le pide que ingrese su contraseña de macOS, ingrésele y haga clic en **Instalar software**.

Después de la instalación de ESET Cyber Security Pro:

## macOS Big Sur (11)

1. [Permitir extensiones del sistema](#).
2. [Permitir acceso completo al disco](#).
3. Permitir que ESET agregue configuraciones de proxy. Recibirá la siguiente notificación: "ESET Cyber Security Pro" **Quisiera 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 versiones posteriores, verá la notificación **Extensión del sistema bloqueada** de su sistema y la notificación **Su equipo no está protegido** de ESET Cyber Security Pro. Para acceder a todas las funciones ESET Cyber Security Pro, deberá permitir las extensiones de kernel en su dispositivo. Para permitir las extensiones de kernel en su dispositivo, vaya a **Preferencias del sistema > Seguridad y privacidad** y haga clic en **Permitir** para permitir el software de sistema del desarrollador **ESET, spol. s.r.o.** Para obtener información más detallada, visite nuestro [artículo de la base de conocimiento](#).
2. En macOS 10.14 y posterior, verá la notificación **Su equipo está parcialmente protegido** de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro, deberá permitir el **Acceso completo al disco** para ESET Cyber Security Pro. Haga clic en **Abrir preferencias del sistema > Seguridad y privacidad**. Vaya a la pestaña **Privacidad** y seleccione la opción **Acceso completo al disco**. Haga clic en el icono del candado para permitir la edición. Haga clic en el icono del símbolo "más" y seleccione la aplicación ESET Cyber Security Pro. Su equipo mostrará una notificación para reiniciar el equipo. Haga clic en **Más tarde**. No reinicie el equipo ahora. Haga clic en **Comenzar nuevamente** en la ventana de notificación de ESET Cyber Security Pro o reinicie su equipo. Para obtener información más detallada, visite nuestro [artículo de la base de conocimiento](#).

Después de la instalación de ESET Cyber Security Pro, debe realizarse una exploración del equipo en busca de códigos maliciosos. Desde la ventana principal del programa haga clic en **Exploración del equipo > Exploración inteligente**. Para obtener más información sobre las exploraciones del equipo a petición, consulte la sección [Exploración del equipo a petición](#).

# Instalación personalizada

El modo de instalación personalizada está diseñado para usuarios experimentados que deseen modificar opciones avanzadas de configuración durante el proceso de instalación.

- **Servidor proxy**

Si usa un servidor proxy, defina sus parámetros seleccionando **Uso un servidor proxy**. En la siguiente ventana, introduzca la dirección IP o la dirección URL del servidor proxy en el campo **Dirección**. En el campo **Puerto**, especifique el puerto en el que el servidor proxy aceptará las conexiones (el predeterminado es 3128). En caso de que el servidor proxy requiera autenticación, escriba un **Nombre de usuario** y una **Contraseña** válidos para tener acceso al servidor proxy. Si no usa un servidor proxy, seleccione **No uso servidor proxy**. Si no está seguro si utiliza un servidor proxy, seleccione **Usar configuración del sistema (recomendado)** para usar la configuración del sistema actual.

- **Privilegios**

Tiene la opción de definir usuarios o grupos con privilegios, que tendrán permiso para editar la configuración del programa. Desde la lista de usuarios que aparece a la izquierda, seleccione los usuarios y presione **Agregar** para agregarlos a la lista de **Usuarios con privilegios**. Para mostrar todos los usuarios del sistema, seleccione la opción **Mostrar todos los usuarios**. Si deja la lista Usuarios con privilegios vacía, se considerará que todos son usuarios con privilegios.

- **ESET LiveGrid®**

Para obtener más información sobre ESET Live Grid, [visite nuestro Glosario](#).

- **Aplicaciones potencialmente no deseadas**

Para obtener más información sobre aplicaciones potencialmente no deseadas, [visite nuestro Glosario](#).

- **Firewall**

Tiene la opción de seleccionar un modo de filtrado de firewall. Para obtener más información, consulte el tema [Modos de filtrado](#). Después de la instalación de ESET Cyber Security Pro:

## macOS Big Sur (11)

1. [Permitir extensiones del sistema](#).

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

3. Permitir que ESET agregue configuraciones de proxy. Recibirá la siguiente notificación: "ESET Cyber Security Pro" **Quisiera 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 versiones posteriores, verá la notificación **Extensión del sistema bloqueada** de su sistema y la notificación **Su equipo no está protegido** de ESET Cyber Security Pro. Para acceder a todas las funciones ESET Cyber Security Pro, deberá permitir las extensiones de kernel en su dispositivo. Para permitir las extensiones de kernel en su dispositivo, vaya a **Preferencias del sistema > Seguridad y privacidad** y haga clic en **Permitir** para permitir el software de sistema del desarrollador **ESET, spol. s.r.o.** Para obtener información más detallada, visite nuestro [artículo de la base de conocimiento](#).

2. En macOS 10.14 y posterior, verá la notificación **Su equipo está parcialmente protegido** de ESET Cyber

Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro, deberá permitir el **Acceso completo al disco** para ESET Cyber Security Pro. Haga clic en **Abrir preferencias del sistema > Seguridad y privacidad**. Vaya a la pestaña **Privacidad** y seleccione la opción **Acceso completo al disco**. Haga clic en el icono del candado para permitir la edición. Haga clic en el icono del símbolo “más” y seleccione la aplicación ESET Cyber Security Pro. Su equipo mostrará una notificación para reiniciar el equipo. Haga clic en **Más tarde**. No reinicie el equipo ahora. Haga clic en **Comenzar nuevamente** en la ventana de notificación de ESET Cyber Security Pro o reinicie su equipo. Para obtener información más detallada, visite nuestro [artículo de la base de conocimiento](#).

Después de la instalación de ESET Cyber Security Pro, realizarse una exploración del equipo en busca de códigos maliciosos. Desde la ventana principal del programa haga clic en **Exploración del equipo > Exploración inteligente**. Para obtener más información sobre las exploraciones del equipo a petición, consulte la sección [Exploración del equipo a petición](#).

## Permitir extensiones del sistema

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

Después de la instalación ESET Cyber Security Pro de macOS Big Sur (11) y versiones posteriores, recibirá la notificación Extensión del sistema bloqueada de su sistema y la notificación Su equipo no está protegido de ESET Cyber Security Pro. Para acceder a todas las funciones de ESET Cyber Security Pro, deberá permitir las extensiones del sistema en su dispositivo.



### Actualice desde versiones anteriores de macOS a Big Sur.

Si ya instaló ESET Cyber Security Pro y va a actualizar a macOS Big Sur, deberá permitir las extensiones de kernel de ESET de forma manual después de la actualización. Se necesita contar con acceso físico al equipo del cliente: cuando se accede de forma remota, el botón Permitir está deshabilitado.

Cuando instale el producto ESET en macOS Big Sur o versiones posteriores, deberá permitir las extensiones del sistema de ESET de forma manual. Se necesita contar con acceso físico al equipo del cliente: cuando se accede de forma remota, esta opción está deshabilitada.

## Permitir extensiones del sistema de forma manual

- 1.Haga clic en **Abrir preferencias del sistema** o **Abrir preferencias de seguridad** en uno de los diálogos de alerta.
- 2.Haga clic en el ícono del candado en la parte inferior izquierda para permitir cambios en la ventana de configuración.
- 3.Utilice su Touch ID o haga clic en **Usar contraseña** y escriba su nombre de usuario y contraseña; luego haga clic en **Desbloquear**.
- 4.Haga clic en **Detalles**.
- 5.Seleccione ambas opciones de ESET Cyber Security Pro.**app**.
- 6.Haga clic en **Aceptar**.

Para obtener una guía detallada, paso a paso, visite [nuestro artículo de la base de conocimiento](#). (Los artículos de la base de conocimiento no están disponibles en todos los idiomas).

## Permitir acceso completo al disco

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

1. Haga clic en **Abrir preferencias del sistema** en la ventana de diálogo de alertas.
2. Haga clic en el ícono del candado en la parte inferior izquierda para permitir cambios en la ventana de configuración.
3. Utilice su Touch ID o haga clic en **Usar contraseña** y escriba su nombre de usuario y contraseña; luego haga clic en **Desbloquear**.
4. Seleccione ESET Cyber Security Pro.app en la lista.
5. Aparecerá una notificación para reiniciar ESET Cyber Security Pro. Haga clic en Más tarde.
6. Seleccione **Protección del sistema de archivos en tiempo real** de ESET de la lista.



**La protección del sistema de archivos en tiempo real de ESET no figura**

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

7. Haga clic en Comenzar nuevamente en la ventana de diálogo de alertas de ESET Cyber Security Pro o reinicie el equipo. Para obtener información más detallada, visite nuestro [artículo de la base de conocimiento](#).

## Activación del producto

Luego de la instalación, se muestra automáticamente la pantalla de Activación del producto. Para acceder al diálogo de activación del producto en cualquier momento, haga clic en ESET Cyber Security Pro el ícono ubicado en la barra de menú de macOS (parte superior de la pantalla) y luego haga clic en **Activación del producto...**

- **Clave de licencia:** cadena única en el formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX que se utiliza para identificar el propietario de la licencia y para activar la licencia. Si compró una versión minorista en caja del producto, utilice una Clave de licencia para activar el producto. Por lo general aparece en el interior o al dorso del paquete del producto.
- **Nombre de usuario y contraseña:** si posee un nombre de usuario y contraseña y no sabe cómo activar ESET Cyber Security Pro, haga clic en **Tengo un nombre de usuario y contraseña, ¿qué hago?**. Será redirigido a my.eset.com, donde podrá convertir sus credenciales en una clave de licencia.
- **Licencia de prueba gratuita:** seleccione esta opción si le gustaría evaluar ESET Cyber Security Pro antes de realizar una compra. Ingrese su dirección de correo electrónico para activar ESET Cyber Security Pro por un período limitado. La licencia de prueba se enviará a su correo electrónico. Las licencias de prueba solo se pueden activar una vez por cliente.
- **Comprar licencia :** si no tiene licencia y desea comprar una, haga clic en Adquirir licencia. Será redirigido al

sitio Web de su distribuidor local de ESET.

- **Activar luego:** haga clic en esta opción si no desea activarlo en este momento.

## Desinstalación

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

- Inserte el CD/DVD de instalación de ESET Cyber Security Pro en su equipo, ábralo desde el escritorio o la ventana **Finder** y haga doble clic en **Desinstalar**.
- Abra el archivo de instalación de ESET Cyber Security Pro (.dmg) y haga doble clic en **Desinstalar**.
- Ejecute **Finder**, abra la carpeta **Aplicaciones** en su disco duro, CTRL+ clic en el ícono **ESET Cyber Security Pro** y seleccione **Mostrar contenidos del paquete**. Abra la carpeta **Contents** > **Helpers** y haga doble clic en el ícono **Uninstaller**.

## Resumen general básico

La ventana primaria de ESET Cyber Security Pro se encuentra dividida en dos secciones principales. La ventana primaria que está a la derecha muestra información correspondiente a la opción seleccionada en el menú principal de la izquierda.

Se puede acceder a las siguientes secciones desde el menú principal:

- **Inicio:** brinda información sobre el estado de protección de su Equipo, firewall, protección web y de correo electrónico y control parental.
- **Exploración del equipo:** esta sección permite configurar e iniciar la [Exploración bajo demanda del equipo](#).
- **Actualización:** muestra información sobre las actualizaciones de los módulos de detección.
- **Configuración:** seleccione esta sección para ajustar el nivel de seguridad de su equipo.
- **Herramientas:** proporciona acceso a [Archivos de registro](#), [Tareas programadas](#), [Cuarentena](#), [Procesos en ejecución](#) y otras funciones del programa.
- **Ayuda:** muestra el acceso a los archivos de ayuda, la base de conocimiento de Internet, el formulario de solicitud de soporte e información adicional del programa.

## Accesos directos del teclado

Algunos de los accesos directos del teclado que se pueden usar cuando se trabaja con ESET Cyber Security Pro son los siguientes:

- cmd+, : muestra las preferencias de ESET Cyber Security Pro,
- cmd+O: cambia el tamaño de la ventana principal de la interfaz gráfica de usuario de ESET Cyber Security Pro al tamaño predeterminado y la desplaza al centro de la pantalla,
- cmd+Q - esconde la ventana principal de la interfaz gráfica de usuario de ESET Cyber Security Pro. Puede abrirla haciendo clic en el icono ESET Cyber Security Pro  en la barra del menú macOS (en la parte superior de la pantalla).
- cmd+W : cierra la ventana principal de la interfaz gráfica de usuario de ESET Cyber Security Pro.

Los siguientes accesos directos del teclado funcionan solo si la opción **Usar el menú estándar** está habilitada debajo de **Configuración > Ingresar preferencias de aplicación... > Interfaz**:

- cmd+alt+L: abre la sección Archivos de registro,
- cmd+alt+S: abre la sección Tareas programadas,
- cmd+alt+Q: abre la sección Cuarentena.

## Comprobación del estado de protección

Para ver su estado de protección haga clic en **Inicio** en el menú principal. Se mostrará un resumen de estado del funcionamiento de los módulos de ESET Cyber Security Pro en la ventana principal.



## Qué hacer si el programa no funciona correctamente

Cuando un módulo está funcionando de manera adecuada, se muestra un ícono verde. Cuando un módulo no está funcionando de manera adecuada, se muestra un punto de exclamación rojo o un ícono de notificación naranja. Se muestra información adicional acerca del módulo y una solución sugerida para solucionar el problema. Para cambiar el estado de módulos individuales, haga clic en el vínculo azul que se encuentra debajo de cada mensaje de notificación.

Si no puede resolver un problema utilizando las soluciones sugeridas, puede buscar una solución en la [Base de conocimiento de ESET](#) o contactarse con el [Centro de atención al cliente de ESET](#). El servicio de Atención al cliente responderá rápidamente sus preguntas y lo ayudará a resolver el problema con ESET Cyber Security Pro.

# Protección del equipo

La configuración del equipo se encuentra en **Configuración > Equipo**. Muestra el estado de **Protección del sistema de archivos en tiempo real** y **Bloqueo de medios extraíbles**. Para desactivar módulos individuales, cambie el botón del módulo deseado a **DESHABILITADO**. Tenga en cuenta que esto puede disminuir el nivel de protección del equipo. Para acceder a la configuración detallada de cada módulo, haga clic en **Configuración...**

## Protección antivirus y antispyware

La protección antivirus defiende el sistema contra ataques maliciosos mediante la modificación de archivos que presentan amenazas potenciales. Si se detecta una amenaza con códigos maliciosos, el módulo Antivirus la puede eliminar mediante el bloqueo y la desinfección, la eliminación o la colocación en cuarentena.

## General

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

- **Aplicaciones potencialmente no deseadas:** Grayware o aplicación potencialmente no deseada (PUA, 'Potentially Unwanted Application') es una amplia categoría de software, cuya intención no es tan inequívocamente maliciosa como con otros tipos de malware, como virus o troyanos. Sin embargo, puede instalar otro software no deseado, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas o esperadas por el usuario. Obtenga más información sobre estos tipos de aplicaciones en el [Glosario](#).
- **Aplicaciones potencialmente no seguras:** estas aplicaciones hacen referencia a programas comerciales y legítimos de los cuales pueden aprovecharse los atacantes si son instalados sin el conocimiento del usuario. Esta clasificación incluye programas como herramientas de acceso remoto, razón por la cual esta opción se encuentra deshabilitada de forma predeterminada.
- **Aplicaciones sospechosas:** estas aplicaciones incluyen programas comprimidos con empaquetadores o protectores. Estos tipos de protectores por lo general son explotados por autores de malware para evadir su detección. El empaquetador es un programa autoejecutable que enrolla varios tipos de malware en un único paquete. Los empaquetadores más comunes son UPX, PE\_Compact, PKLite y ASPack. El mismo malware puede ser detectado de diferentes maneras cuando se comprime utilizando un empaquetador diferente. Los empaquetadores también tienen la habilidad de hacer que sus "firmas" muten a lo largo del tiempo, haciendo que los malware sean más difíciles de detectar y remover.

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

## Exclusiones

En la sección **Exclusiones** puede excluir de la exploración ciertos archivos/carpetas, aplicaciones o direcciones IP/IPv6.

Los archivos y las carpetas que se enumeran en la pestaña **Sistema de archivos** se excluirán de todos los módulos de exploración: Inicio, en tiempo real y bajo demanda (exploración en el equipo).

- **Ruta:** ruta a los archivos o las carpetas excluidos
- **Amenaza:** si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo solo se excluirá de la exploración en lo que respecta a esa amenaza, pero no se excluirá completamente. Si dicho archivo más tarde se infecta con otro código malicioso, el módulo antivirus lo detectará.
-  - crea una nueva exclusión. Ingrese la ruta al objeto (también puede usar los caracteres globales \* y ?) o seleccione la carpeta o el archivo desde la estructura con forma de árbol.
-  - elimina las entradas seleccionadas
- **Predeterminado:** cancela todas las exclusiones

En la ficha **Internet y correo electrónico** puede excluir ciertas **Aplicaciones** o **Direcciones IP/IPv6** de la exploración de protocolo.

## Protección de inicio

El archivo de inicio automáticamente explora archivos al inicio del sistema. Esta exploración se ejecuta regularmente de modo predeterminado como una tarea programada luego del inicio del usuario o luego de una actualización exitosa de los módulos de detección. Para modificar la configuración de los parámetros del motor ThreatSense aplicable a la exploración de inicio, haga clic en el botón **Configuración**. Puede obtener más información acerca de la configuración del motor ThreatSense leyendo [esta sección](#).

## Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real verifica todos los tipos de medios y acciona una exploración por diversos sucesos. Cuando usa la tecnología ThreatSense (descrita en la sección titulada [Configuración de los parámetros del motor ThreatSense](#)), la protección del sistema de archivos en tiempo real puede variar entre los nuevos archivos creados y los ya existentes. Los archivos recién creados se pueden controlar con mayor precisión.

En forma predeterminada, se exploran todos los archivos si hace clic en **Abrir archivo**, **Crear archivo** o **Ejecutar archivo**. Recomendamos mantener estas configuraciones predeterminadas, ya que brindan el máximo nivel de protección en tiempo real para su equipo. La protección en tiempo real se activa junto con el inicio del sistema y proporciona una exploración ininterrumpida. En casos especiales (por ejemplo, cuando existe un conflicto con otro programa de exploración en tiempo real), es posible detener la protección en tiempo real; para ello, haga clic en el ícono de ESET Cyber Security Pro<sup>®</sup> ubicado en la barra del menú (en la parte superior de la pantalla) y seleccione **Deshabilitar la protección del sistema de archivos en tiempo real**. También es posible detener la protección en tiempo real desde la ventana principal del programa (haga clic en **Configuración** > **Equipo** y cambie **Protección del sistema de archivos en tiempo real** a **DESHABILITADO**).

Se pueden excluir los siguientes tipos de medio del escáner Real-time:

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

Le recomendamos usar la configuración predeterminada y solo modificar las exclusiones de exploración en casos específicos, tales como cuando la exploración de determinados medios ralentiza significativamente las transferencias de datos.

Para modificar las opciones avanzadas de la protección del sistema de archivos en tiempo real, vaya a **Configuración > Ingresar preferencias de aplicación...** (o presione *cmd+,*) > **Protección en tiempo real** y haga clic en el botón **Configuración...** junto a **Opciones avanzadas** (se describe en la sección [Opciones avanzadas de exploración](#)).

## Opciones avanzadas

En esta ventana puede definir los tipos de objetos que el motor ThreatSense debe explorar. Para obtener más información acerca de los **Archivos de autoextracción**, los **Empaquetadores de tiempo de ejecución** y la **Heurística avanzada**, consulte la [Configuración de los parámetros del motor ThreatSense](#).

No se recomienda realizar cambios en la sección **Configuración predeterminada de archivos** a menos que sea necesario para solucionar un problema específico, dado que los valores más elevados de los archivos comprimidos anidados pueden afectar el rendimiento del sistema.

**Parámetros de ThreatSense para los archivos ejecutados:** en forma predeterminada, se usa la **Heurística avanzada** cuando se ejecutan los archivos. Recomendamos firmemente mantener la Optimización inteligente y ESET Live Grid habilitados para mitigar el impacto en el rendimiento del sistema.

**Aumentar la compatibilidad de los volúmenes de redes:** esta opción mejora el rendimiento cuando accede a los archivos por la red. Debería estar habilitada si experimenta lentitud durante el acceso a las unidades de red. Esta característica utiliza al coordinador de archivos del sistema en macOS 10.10 o posterior. Tenga en cuenta que no todas las aplicaciones admiten al coordinador de archivos, por ejemplo, Microsoft Word 2011 no lo admite, Word 2016, sí.

## Cuándo modificar la configuración de la protección en tiempo real

La protección en tiempo real es el componente más imprescindible para mantener un sistema seguro con ESET Cyber Security Pro. Modifique los parámetros de protección en tiempo real con precaución. Recomendamos modificar dichos parámetros únicamente en casos específicos. Por ejemplo, en una situación donde exista un conflicto con una aplicación en particular.

Después de la instalación de ESET Cyber Security Pro, todos los ajustes de configuración se optimizan para proporcionar el máximo nivel de seguridad del sistema para los usuarios. Para restaurar la configuración predeterminada, haga clic en **Predeterminado** que se encuentra en la parte inferior izquierda de la ventana **Protección en tiempo real (Configuración > Ingrese preferencias de aplicación... > Protección en tiempo real)**.

## Verificación de la protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta los virus, descargue el archivo de prueba de [eicar.com](http://eicar.com) controle que ESET Cyber Security Pro lo identifique como una amenaza. Este archivo de prueba es un archivo especial e inofensivo, que es detectado por todos los programas antivirus. El archivo fue creado por el instituto EICAR (Instituto Europeo para la Investigación de los Antivirus Informáticos, por sus siglas en inglés) para comprobar la eficacia de los programas antivirus.

# Qué hacer si la protección en tiempo real no funciona

En esta sección, se describirán situaciones que pueden presentar problemas al utilizar la protección en tiempo real, y se indicará cómo resolverlas.

## La protección en tiempo real está deshabilitada

Si un usuario ha deshabilitado la protección en tiempo real sin darse cuenta, será necesario volver a activarla. Para volver a activar la protección en tiempo real, en el menú principal haga clic en **Configuración > Equipo** y cambie **Protección del sistema de archivos en tiempo real** a **HABILITADO**. Otra alternativa es habilitar la protección del sistema de archivos en tiempo real en la ventana de preferencias de la aplicación en **Protección en tiempo real** seleccionando la opción **Habilitar protección del sistema de archivos en tiempo real**.

## La protección en tiempo real no detecta ni desinfecta infiltraciones

Asegúrese de que no haya otros programas antivirus instalados en el equipo. Si están habilitados dos escudos de protección en tiempo real al mismo tiempo, es posible que entren en conflicto. Se recomienda desinstalar cualquier otro programa antivirus que haya en el sistema.

## La protección en tiempo real no se activa

Si la protección en tiempo real no se activa durante el inicio del sistema, es posible que se deba a la existencia de conflictos con otros programas. En este caso, comuníquese con Atención al cliente de ESET.

# Exploración bajo demanda del equipo

Si sospecha que el equipo está infectado (se comporta en forma anormal), ejecute una **Exploración inteligente** para examinar el equipo en busca de infiltraciones. Para obtener la máxima protección, las exploraciones del equipo deben ejecutarse en forma habitual como parte de las medidas de seguridad de rutina, no solo cuando existe la sospecha de una infiltración. La exploración de rutina puede detectar infiltraciones que la exploración en tiempo real no detectó cuando se grabaron en el disco. Esta situación puede ocurrir si la exploración en tiempo real no estaba habilitada al momento de la infección o si los módulos de detección no están actualizados.

Recomendamos ejecutar una exploración del equipo bajo demanda al menos una vez al mes. La exploración se puede configurar como una tarea programada en **Herramientas > Tareas programadas**.



## Tipo de exploración

Se encuentran disponibles dos tipos de exploración del equipo bajo demanda. **Exploración inteligente** explora rápidamente el sistema sin necesidad de realizar ajustes de configuración adicionales de los parámetros de la exploración. **Exploración personalizada** permite seleccionar cualquiera de los perfiles de exploración predefinidos, así como elegir objetos específicos para la exploración.

## Exploración inteligente

La exploración inteligente permite iniciar rápidamente una exploración del equipo y desinfectar los archivos infectados sin necesidad de la intervención del usuario. La ventaja principal es su manejo sencillo, ya que no requiere una configuración detallada de la exploración. La exploración inteligente verifica todos los archivos de todas las carpetas y desinfecta o elimina de forma automática las infiltraciones detectadas. El nivel de desinfección está establecido automáticamente en el valor predeterminado. Para obtener información más detallada sobre los tipos de desinfección, consulte la sección [Desinfección](#).

## Exploración personalizada

La **exploración personalizada** es óptima si desea especificar los parámetros de exploración como objetos para explorar y métodos de exploración. La ventaja de ejecutar una Exploración personalizada es la capacidad para configurar los parámetros en detalle. Se pueden guardar configuraciones distintas como perfiles de exploración definidos por el usuario, que pueden ser útiles si la exploración se realiza varias veces con los mismos parámetros.

Para seleccionar objetos para explorar, seleccione **Exploración del equipo > Exploración personalizada** y a continuación seleccione **Objetos de exploración** específicos desde la estructura con forma de árbol. También se puede especificar con más precisión un objeto de exploración al indicar la ruta a las carpetas o archivos que desee

incluir. Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. Además, Puede elegir desde tres niveles de desinfección al hacer clic en **Configuración... > Desinfección**.



### Exploración personalizada

Se recomienda realizar exploraciones del equipo con la Exploración personalizada para usuarios avanzados con experiencia previa en el uso de programas antivirus.

## Objetos para explorar

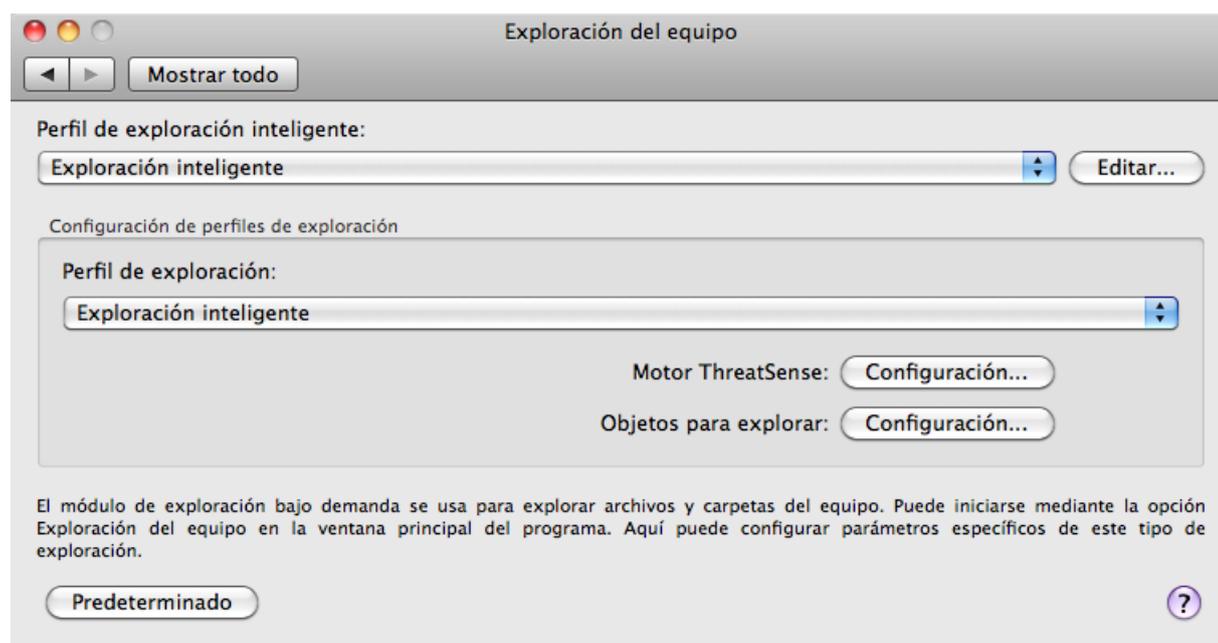
La estructura en forma de árbol que muestra los objetos para explorar permite seleccionar los archivos y las carpetas que desea explorar en busca de virus. También se pueden seleccionar carpetas de acuerdo con la configuración de un perfil determinado.

El objeto para explorar puede definirse con mayor precisión si se ingresa la ruta a las carpetas o los archivos que desea incluir en la exploración. Seleccione los objetos de la estructura en forma de árbol que enumera todas las carpetas disponibles en el equipo al seleccionar la casilla de verificación que corresponde a una carpeta o archivo determinado.

## Perfiles de exploración

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

Para crear un nuevo perfil, haga clic en **Configuración > Ingresar preferencias de aplicación...** del menú principal. (o presione *cmd+,*) > **Exploración del equipo** y haga clic en **Editar...** junto a la lista de perfiles actuales.



Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte la sección [Configuración de los parámetros del motor ThreatSense](#), donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

Ejemplo: Suponga que desea crear su propio perfil de exploración y la configuración de la exploración inteligente es parcialmente adecuada, pero no desea explorar empaquetadores en tiempo real o aplicaciones potencialmente no seguras y, además, desea aplicar una limpieza estricta. En la ventana **Lista de perfiles de la exploración bajo demanda**, escriba el nombre del perfil, haga clic en el botón **Agregar** y, para confirmar, haga clic en **Aceptar**. A continuación, ajuste los parámetros según sus requisitos mediante la configuración del **Motor ThreatSense** y de los **Objetos para explorar**.

Si desea desactivar el sistema operativo y apagar el equipo una vez finalizada la exploración bajo demanda, utilice la opción **Apagar el equipo después de la exploración**.

## Configuración de los parámetros del motor

### ThreatSense

ThreatSense es una tecnología perteneciente a ESET formada por varios métodos de detección de amenazas complejos. Esta tecnología es proactiva, lo que significa que también proporciona protección durante las primeras horas de propagación de una nueva amenaza. Utiliza una combinación de métodos distintos (exploración del código, emulación del código, firmas genéricas, etc.) que funcionan conjuntamente para mejorar de forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar varios flujos de datos simultáneamente, lo que maximiza la eficacia y la tasa de detección. La tecnología ThreatSense también elimina con éxito los rootkits.

Las opciones de configuración de la tecnología ThreatSense permiten especificar varios parámetros de exploración:

- Los tipos de archivos y las extensiones que se van a explorar.
- La combinación de diversos métodos de detección.
- Los niveles de desinfección, etc.

Para abrir la ventana de configuración haga clic en **Configuración > Ingrese las preferencias de aplicación** (o presione *cmd+*) y luego haga clic en el botón ThreatSense Motor **Configuración** en la **Protección de arranque**, **Protección en tiempo real** y módulos **Exploración del equipo**, que usan ThreatSense tecnología (ver a continuación). Diferentes escenarios de seguridad pueden requerir distintas configuraciones. Por ese motivo, ThreatSense se puede configurar de forma individual para cada uno de los siguientes módulos de protección:

- **Protección del inicio:** verificación automática de archivos de inicio del sistema.
- **Protección en tiempo real:** protección del sistema de archivos en tiempo real.
- **Exploración del equipo:** exploración del equipo bajo demanda
- **Protección del acceso a la Web**
- **Protección de correo electrónico**

Los parámetros de ThreatSense están específicamente optimizados para cada módulo y su modificación puede afectar considerablemente el funcionamiento del sistema. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema. En consecuencia, se recomienda mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos, excepto para Exploración del equipo.

# Objetos

La sección **Objetos** permite definir qué archivos del equipo se explorarán en busca de infiltraciones.

- **Vínculos simbólicos:** (solo para el módulo de exploración del equipo) explora archivos que contienen una cadena de texto interpretada y seguida por el sistema operativo como ruta a otro archivo o directorio.
- **Archivos de correo:** (no disponible en Protección en tiempo real) explora archivos de correo.
- **Buzones de correo:** (no disponible en la Protección en tiempo real) explora los buzones de correo del usuario en el sistema. El uso incorrecto de esta opción puede generar conflictos con la aplicación cliente de correo electrónico. Para obtener más información sobre las ventajas y desventajas de esta opción, consulte el siguiente [artículo de la base de conocimiento](#).
- **Archivos comprimidos:** (no disponible en la Protección en tiempo real) explora los archivos contenidos en archivos comprimidos (.rar, .zip, .arj, .tar, etc.).
- **Archivos comprimidos de autoextracción:** (no disponible en la Protección en tiempo real) explora los archivos que se encuentran contenidos en archivos comprimidos de autoextracción.
- **Empaquetadores ejecutables:** a diferencia de los tipos de archivos estándar, los empaquetadores ejecutables se descomprimen en la memoria. Cuando se selecciona esto, los empaquetadores estándar estáticos (por ej., UPX, yoda, ASPack, FGS) también se exploran.

# Opciones

En la sección **Opciones**, puede seleccionar los métodos que se usan durante el análisis del sistema. Están disponibles estas opciones:

- **Heurística:** la heurística usa un algoritmo que analiza la actividad de los programas (maliciosos). La ventaja principal de la detección heurística es la capacidad de detectar nuevo software malicioso que no existía con anterioridad.
- **Heurística avanzada:** la heurística avanzada está compuesta por un algoritmo heurístico único, desarrollado por ESET, optimizado para detectar troyanos y gusanos informáticos creados con lenguajes de programación de última generación. Como resultado de la heurística avanzada, la capacidad de detección del programa es significativamente mayor.

# Desinfección

La configuración de desinfección determina el comportamiento de la exploración durante la desinfección de los archivos infectados. Existen 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 intentará desinfectar o eliminar los archivos infectados de manera automática. 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 (incluyendo

comprimidos). La única excepción la constituyen los archivos del sistema. Si no es posible desinfectar un archivo, recibirá una notificación y se le pedirá que seleccione el tipo de acción a realizar.



### Archivos comprimidos

En el modo de desinfección predeterminado estándar, solamente se elimina 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 in archivo comprimido infectado en modo Desinfección exhaustiva, se eliminará todo el archivo comprimido aunque contenga archivos no infectados.



### Exploración de archivos comprimidos

En el modo de desinfección predeterminado estándar, solamente se elimina 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 in archivo comprimido infectado en modo Desinfección exhaustiva, se eliminará todo el archivo comprimido aunque contenga archivos no infectados.

## Exclusiones

Una extensión es la parte delimitada por un punto en el nombre de un archivo. La extensión define el tipo de archivo y su contenido. Esta sección de configuración de los parámetros de ThreatSense permite definir los tipos de archivos que se excluirán de la exploración.

De forma predeterminada, se exploran todos los archivos independientemente de su extensión. Se puede agregar cualquier extensión a la lista de archivos excluidos de la exploración. Mediante los botones + y - puede habilitar o prohibir la exploración de extensiones específicas.

A veces es necesario excluir archivos de la exploración si determinados tipos de archivos impiden que el programa funcione correctamente. Por ejemplo, podría ser recomendado excluir los archivos *log*, *cfg* y *tmp*. El formato correcto para ingresar una extensión de archivo es:

*log*

*cfg*

*tmp*

## Límites

La sección **Límites** permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

- **Tamaño máximo:** define el tamaño máximo de los objetos que se explorarán. Una vez que se definió el tamaño máximo, el módulo de antivirus explorará solo los objetos más pequeños que el tamaño especificado. Los únicos que deben modificar esta opción son los usuarios avanzados que tienen motivos específicos para excluir objetos de mayor tamaño de la exploración.
- **Duración máxima de la exploración:** define el valor máximo de tiempo permitido para explorar un objeto. Si en esta opción se ingresó un valor definido por el usuario, el módulo antivirus detendrá la exploración de un

objeto cuando haya transcurrido dicho tiempo, sin importar si la exploración ha finalizado.

- **Nivel máximo de anidado:** especifica la profundidad máxima de la exploración de los archivos comprimidos. No se recomienda cambiar el valor predeterminado de 10: en circunstancias normales, no existe ninguna razón para modificarlo. Si la exploración finaliza prematuramente debido a la cantidad de archivos comprimidos anidados, el archivo comprimido quedará sin verificar.

- **Tamaño máximo del archivo:** esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. Si la exploración finaliza prematuramente como consecuencia de este límite, el archivo comprimido quedará sin verificar.

## Otros

### Habilitar optimización inteligente

Cuando la opción Optimización inteligente está habilitada, se optimiza la configuración para garantizar el nivel de exploración más eficiente sin comprometer la velocidad de exploración. Los diversos módulos de protección realizan exploraciones de forma inteligente empleando distintos métodos de exploración. Optimización inteligente no está definida de manera inflexible en del producto. El Equipo de desarrollo de ESET implementa constantemente nuevos cambios, que luego se integran ESET Cyber Security Pro a través de las actualizaciones de rutina. Si la opción Optimización inteligente está deshabilitada, solo se aplica la configuración definida por el usuario en el núcleo de ThreatSense de ese módulo específico al efectuar la exploración.

### Explorar el flujo de datos alternativo (solo para exploración bajo demanda)

Los flujos de datos alternativos usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección camuflándose como flujos de datos alternativos.

## Infiltración detectada

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

Si su equipo muestra signos de infección por malware, por ej., funciona más lento, con frecuencia no responde, etc., se recomienda seguir los pasos que se detallan a continuación:

1. Haga clic en **Exploración del equipo**.
2. Haga clic en **Exploración inteligente** (para obtener más información, consulte la sección [Exploración inteligente](#)).
3. Una vez finalizada la exploración, consulte el registro para verificar la cantidad de archivos explorados, infectados y desinfectados.

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

Como ejemplo general de la forma en que ESET Cyber Security Pro maneja las infiltraciones, imagine que el monitor del sistema de archivos en tiempo real, que usa el nivel predeterminado de desinfección, detecta una infiltración. La protección en tiempo real intentará limpiar o eliminar el archivo. Si no hay ninguna acción predefinida disponible para el módulo de protección en tiempo real, el programa le pedirá que seleccione una

opción en una ventana de alerta. Por lo general, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acción**. No se recomienda seleccionar **Sin acción**, ya que los archivos infectados se dejan en estado infectado. Esta opción se utiliza en las situaciones en que usted está seguro de que el archivo es inofensivo y que se ha detectado por error.

#### Desinfección y eliminación:

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



#### Eliminación de archivos en archivos comprimidos

En el modo de desinfección predeterminado, se eliminará el archivo comprimido completo solo si todos los archivos que lo componen están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos inofensivos no infectados. No obstante, tenga precaución al realizar una exploración con **Desinfección estricta**: con Desinfección estricta, el archivo comprimido se eliminará si al menos contiene un archivo infectado, independientemente del estado de los demás archivos que lo componen.

## Exploración y bloqueo de medios extraíbles

ESET Cyber Security Pro puede ejecutar una exploración bajo demanda de los dispositivos de memoria extraíbles (CD, DVD, USB, etc.). En macOS 10.15, ESET Cyber Security Pro también puede explorar otros dispositivos de medios externos.



#### Exploración de medios extraíbles en macOS 11 y versiones posteriores

ESET Cyber Security Pro instalado en macOS 11 y versiones posteriores, explora únicamente dispositivos de memoria.



Los medios extraíbles pueden contener códigos maliciosos y poner su equipo en riesgo. Para bloquear los medios extraíbles, haga clic en **Configuración de bloqueo de medios** (consulte la imagen de arriba) o, en el menú principal, haga clic en **Configuración > Ingresar preferencias de aplicación... > Medios** en la ventana principal del programa y seleccione **Habilitar bloqueo de medios extraíbles**. Para permitir el acceso a ciertos tipos de medios, quite la selección de los volúmenes de dichos medios.



### Acceso de CD-ROM

Para permitir el acceso a unidades de CD-ROM conectadas a su equipo mediante un cable USB, quite la selección de la opción **CD-ROM**.

## Anti-Phishing

El término phishing define una actividad criminal que utiliza la ingeniería social (manipula a los usuarios para obtener información confidencial). Phishing se usa a menudo para obtener acceso a datos confidenciales tales como números de cuentas bancarias, números de tarjetas de crédito, números de PIN o nombres de usuarios y contraseñas.

Le recomendamos mantener habilitada la función Anti-Phishing (**Configuración > Ingresar las preferencias de la aplicación ... > Protección Anti-Phishing**). Todos los posibles ataques phishing que provengan de sitios web o dominios peligrosos se bloquearán, y se mostrará una notificación de advertencia que informa sobre el ataque.

## Firewall

El firewall controla todo el tráfico de la red desde y hacia el sistema al permitir o rechazar las conexiones individuales de red en base a las reglas de filtración especificadas. Proporciona protección contra ataques desde equipos remotos y permite el bloqueo de algunos servicios. También proporciona protección antivirus para protocolos HTTP, POP3 e IMAP.



### Excepciones de exploración

ESET Cyber Security Pro no explora los protocolos cifrados HTTPS, POP3S y IMAPS.

La configuración del firewall se puede encontrar en **Configuración > Firewall**. Permite ajustar el modo de filtrado, las reglas y los parámetros detallados de configuración. También puede acceder a parámetros de configuración más detallados del programa desde aquí.

Si cambia **Bloquear todo el tráfico de red: desconectar red** a **HABILITADO**, el firewall bloqueará todas las

comunicaciones de entrada y salida. Utilice esta opción solo si sospecha que existen riesgos críticos de seguridad que requieren desconectar el sistema de la red.

## Modos de filtrado

Están disponibles tres modos de filtrado para el firewall de ESET Cyber Security Pro. Los ajustes de modo de filtrado se pueden encontrar en ESET Cyber Security Pro preferencias (presiones *cmd+*) > **Firewall**. El comportamiento del firewall cambia según el modo seleccionado. Los modos de filtrado también tienen influencia sobre el nivel requerido de interacción del usuario.

**Todo el tráfico bloqueado:** se bloquearán todas las conexiones entrantes y salientes.

**Automático con excepciones:** modo predeterminado. Este modo es ideal para usuarios que prefieren un uso sencillo y conveniente del firewall sin necesidad de definir reglas. El modo automático permite el tráfico saliente estándar para un sistema determinado y bloquea todas las conexiones que no se inicien desde la red. También puede agregar reglas personalizadas, definidas por el usuario.

**Modo interactivo:** permite crear una configuración personalizada para su firewall. Cuando se detecta una comunicación y no se aplica ninguna regla existente a esa comunicación, se muestra una ventana de diálogo que informa que hay una conexión desconocida. La ventana de diálogo le da la opción de aceptar o rechazar la comunicación, y la decisión de aceptar o rechazar se puede recordar como una nueva regla para el firewall. Si elige crear una nueva regla en este momento, se permitirán o se bloquearán todas las conexiones futuras de este tipo, de acuerdo con la regla.



Para registrar información detallada acerca de todas las conexiones bloqueadas en un archivo de registro, seleccione la opción **Registrar todas las conexiones bloqueadas**. Para revisar los archivos de registros de firewall, desde el menú principal, haga clic en **Herramientas > Registros** y luego seleccione **Firewall** desde el menú desplegable **Registro**.

## Reglas de firewall

Las reglas de firewall representan un conjunto de condiciones usadas para evaluar todas las conexiones de red y determinar las acciones apropiadas para dichas condiciones. Con las reglas de firewall, puede definir el tipo de acción que desea tomar si se establece una conexión definida por una regla.

Las conexiones entrantes son iniciadas por un equipo remoto que intenta establecer una conexión con el sistema local. Las conexiones salientes funcionan de la forma opuesta: el sistema local Contacta a un equipo remoto.

Cada vez que se detecte una nueva comunicación, deberá analizar cuidadosamente si la permitirá o la rechazará. Las conexiones no solicitadas, no seguras o desconocidas suponen un riesgo de seguridad para el sistema. Si dicha conexión se establece, recomendamos que preste particular atención al equipo remoto y a la aplicación que intenta conectarse al equipo. Muchas infiltraciones intentan obtener y enviar datos privados o descargar otras aplicaciones maliciosas a las estaciones de trabajo de los hosts. El firewall le permite detectar y terminar tales conexiones.

De manera predeterminada, las aplicaciones firmadas por Apple pueden acceder a la red automáticamente. Si desea deshabilitar esta acción, desmarque **Permitir que el software firmado por Apple acceda a la red de manera automática**.

## Creación de reglas nuevas

La pestaña **Reglas** contiene una lista de todas las reglas aplicadas al tráfico generado por las aplicaciones individuales. Las reglas se agregan automáticamente de acuerdo con las respuestas del usuario a cada nueva comunicación.

1. Para crear una nueva regla, haga clic en **Agregar**, escriba un nombre para la regla y arrastre y suelte el ícono 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 equipo, seleccione la opción **Todas las aplicaciones**
2. En la ventana siguiente, especifique la **Acción** (permitir o rechazar 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 o este archivo de registro. Para ello, seleccione la opción **regla de registro**. Para renovar los registros, haga clic en **Herramientas > Registros** desde el menú principal de ESET Cyber Security Pro y seleccione **Firewall** desde el menú desplegable **Registro**.
3. En la sección **Protocolo/Puertos**, seleccione un protocolo mediante el cual la aplicación se comunicará y los números de puertos (si está seleccionado el protocolo TCP o UDP). La capa de transporte del protocolo proporciona una transferencia de datos segura y eficiente.
4. Por último, especifique los criterios de **Destino** (dirección IP, rango, subred, ethernet o Internet) para la regla.

## Zonas de firewall

Una zona representa una colección de direcciones de red que crean un grupo lógico. A cada dirección de un grupo dado se le asignan reglas similares, que se definieron en forma general para todo el grupo.

Estas zonas se pueden crear al hacer clic en **Agregar...** Introduzca un **Nombre** y **Descripción** (opcional) de la zona, seleccione un perfil al que pertenecerá esta zona y agregue una dirección IPv4/IPv6, un rango de direcciones, una subred, una red wifi o una interfaz.

## Perfiles de firewall

**Los perfiles** le permiten controlar el comportamiento del firewall de ESET Cyber Security Pro. Cuando crea o edita una regla de firewall, puede asignarla a un perfil específico. Al seleccionar un perfil, se aplicarán solamente las reglas globales (que no tienen perfiles especificados) y las reglas que han sido asignadas a ese perfil. Puede crear

diversos perfiles con diferentes reglas asignadas para modificar fácilmente el comportamiento del firewall.

## Registros de firewall

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

Los archivos de registro son una herramienta valiosa para detectar errores y revelar invasiones al sistema. Los registros del firewall ESET contienen los siguientes datos:

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

Un análisis completo de estos datos puede ayudar a detectar intentos de comprometer la seguridad del sistema. Existen muchos otros factores que indican riesgos de seguridad potenciales y que se pueden evitar con un firewall como: conexiones demasiado frecuentes desde ubicaciones remotas, intentos reiterados de establecer conexiones, comunicaciones de aplicaciones desconocidas o el uso de números de puerto inusuales.

## Protección web y de correo electrónico

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

- **Protección de acceso web:** controla la comunicación HTTP/HTTPS entre los navegadores y los servidores remotos.
- **Protección del correo electrónico del cliente:** proporciona el control de las comunicaciones por correo electrónico recibido a través de los protocolos POP3 e IMAP.
- **Protección anti-Phishing:** bloquea los posibles ataques de phishing de sitios web o dominios.



### Excepciones de exploración

ESET Cyber Security Pro no explora los protocolos cifrados HTTPS, POP3S y IMAPS.

# Protección web

La protección del acceso a la Web monitorea las comunicaciones entre los navegadores web y los servidores remotos, y cumple con las reglas de HTTP (Protocolo de transferencia de hipertexto).

El filtrado de web se puede lograr a través de la definición de [los números de puerto para la comunicación HTTP](#) y/o [direcciones URL](#).

## Puertos

En la pestaña **Puertos** puede definir los números de puerto usados para la comunicación HTTP. De forma predeterminada, están predefinidos los números de puerto 80, 8080 y 3128.

## Listas de URL

La sección **Listas de URL** permite especificar direcciones HTTP para bloquear, permitir o excluir de la verificación. No es posible acceder a los sitios web de la lista de direcciones bloqueadas. Es posible acceder a los sitios web de la lista de direcciones excluidas sin explorarlos en búsqueda de códigos maliciosos.

Para permitir el acceso solo a las direcciones URL dentro de la lista **URL permitidas**, seleccione la opción **Restringir direcciones URL**.

Para activar una lista, seleccione **Habilitada** junto a su nombre. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione **Notificado**.

En todas las listas, pueden usarse los símbolos especiales \* (asterisco) y ? (signo de interrogación). El asterisco sustituye cualquier cadena de caracteres y el signo de interrogación sustituye cualquier símbolo. Se debe tener especial cuidado al especificar las direcciones excluidas, ya que la lista debe contener solamente direcciones seguras y de confianza. De forma similar, es necesario garantizar que los símbolos \* y ? se usen correctamente en la lista.

## Protección de correo electrónico

La protección del correo electrónico proporciona el 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 avanzado incluidos en el motor de exploración de ThreatSense. La exploración de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

**ThreatSense Motor: Configuración:** la configuración avanzada del módulo de exploración de virus permite configurar los objetos para explorar, los métodos de detección, etc. Haga clic en **Configurar** para mostrar la ventana de configuración detallada del módulo de exploración de virus.

**Añadir mensajes de etiqueta al pie de página del correo electrónico:** una vez explorado un correo electrónico, se puede añadir una notificación con los resultados de la exploración al mensaje. Los mensajes de etiqueta son una herramienta útil, pero no se deben utilizar como determinación final de la seguridad del mensaje, dado que se pueden omitir en mensajes HTML problemáticos y determinadas amenazas pueden falsificarlos. Están disponibles

estas opciones:

- **Nunca:** no se agregarán mensajes de etiqueta a ningún mensaje de correo electrónico
- **Solamente al correo electrónico infectado:** solo el correo electrónico con contenido de malware se etiquetará como analizado
- **A todos los mensajes de correo electrónico explorados:** todos los mensajes de correo electrónico explorados se añadirán con mensajes de etiqueta

**Anexar nota al asunto del correo electrónico recibido y leído:** seleccione esta casilla de verificación si desea que la protección de correo electrónico incluya una advertencia de amenaza en el correo electrónico infectado. Esta función permite filtrar de manera sencilla los correos electrónicos infectados. También aumenta el nivel de credibilidad del destinatario y, si se detecta una infiltración, proporciona información valiosa acerca del nivel de amenaza de un determinado correo electrónico o remitente.

**Plantilla agregada al asunto del correo electrónico infectado:** puede editar esta plantilla para modificar el formato de prefijo del asunto de un correo electrónico infectado.

- %avstatus% - Agrega el estado la infección del correo electrónico (por ejemplo: limpio, infectado...)
- %virus% - Agrega el nombre de la amenaza
- %aspmstatus% - Cambia el asunto basado en el resultado de la exploración antispam
- %product% - Agrega el nombre de su producto de ESET (en este caso - ESET Cyber Security Pro)
- %product\_url% - Agrega el enlace del sitio web de ESET ([www.eset.com](http://www.eset.com))

En la parte inferior de esta ventana, también puede habilitar/deshabilitar la verificación de la comunicación por correo electrónico recibida mediante protocolos POP3 e IMAP. Para obtener más información, consulte los siguientes temas:

- [Verificación de protocolo POP3](#)
- [Verificación de protocolo IMAP](#)

## Verificación de protocolo POP3

El protocolo POP3 es el protocolo más popular usado para recibir comunicaciones por correo electrónico en una aplicación cliente de correo electrónico. ESET Cyber Security Pro proporciona protección para este protocolo independientemente del cliente de correo electrónico utilizado.

El módulo de protección que proporciona este control se inicia automáticamente cuando se inicia el sistema y, luego, permanece activo en la memoria. Asegúrese de que se habilite el módulo para que el filtrado de protocolos funcione correctamente; la verificación del protocolo POP3 se realiza automáticamente sin necesidad de volver a configurar su cliente de correo electrónico. De forma predeterminada, se exploran todas las comunicaciones en el puerto 110, pero, si es necesario, se pueden agregar otros puertos de comunicación. Los números de los puertos se deben delimitar mediante comas.

Si se selecciona la opción **Habilitar verificación del protocolo POP3**, se monitorea todo el tráfico de POP3 en búsqueda de programas de software malicioso.

## Verificación de protocolo IMAP

El Protocolo de acceso a mensajes de Internet (IMAP, Internet Message Access Protocol) es otro protocolo de Internet para recuperación de correo electrónico. El protocolo IMAP tiene algunas ventajas sobre el de POP3, por ejemplo, se pueden conectar simultáneamente varios clientes al mismo buzón de correo y mantener información

del estado de los mensajes, como si se leyó, respondió o eliminó el mensaje, etc. ESET Cyber Security Pro brinda protección para este protocolo independientemente del cliente de correo utilizado.

El módulo de protección que proporciona este control se inicia automáticamente cuando se inicia el sistema y, luego, permanece activo en la memoria. Asegúrese de que la verificación del protocolo IMAP se habilite para que el módulo funcione correctamente; el control del protocolo IMAP se realiza automáticamente sin necesidad de volver a configurar su cliente de correo electrónico. De forma predeterminada, se exploran todas las comunicaciones en el puerto 143, pero, si es necesario, se pueden agregar otros puertos de comunicación. Los números de los puertos se deben delimitar mediante comas.

Si se encuentra seleccionar **Habilitar verificación del protocolo IMAP**, todo el tráfico a través de IMAP se controla en busca de software malicioso.

## Control parental

La selección de **Control parental** le permite configurar el Control parental, lo que proporciona a los padres las herramientas automatizadas para ayudar a proteger a sus hijos. El objetivo es impedir que los niños y jóvenes tengan acceso a páginas con contenido inapropiado o nocivo. El control parental le permite bloquear las páginas web que puedan contener material potencialmente ofensivo. Además, los padres pueden prohibir el acceso de hasta 27 categorías de sitios web predefinidos.

Sus cuentas de usuario figuran en la ventana de **Control parental (Configuración > Ingresar preferencias de aplicación... > Control parental)**. Selecciona la que desea usar para control parental. Para especificar el nivel de protección para la cuenta seleccionada, haga clic en **Configuración...**. Para crear una cuenta nueva, haga clic en **Agregar...**. Esto lo redireccionará a la ventana de cuentas del sistema macOS.

En la ventana de **Configuración de 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, entonces está permitida. Si pasa el mouse por una categoría, podrá ver una lista de las páginas web que entran en esa categoría.

Para modificar la lista de **Páginas web permitidas y bloqueadas**, 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 el uso de comodines (\*). Si escribe simplemente un nombre de dominio, se incluirán todos los subdominios. Por ejemplo, si agrega *google.com* en la **Lista de páginas web permitidas**, todos los subdominios (*mail.google.com*, *news.google.com*, *maps.google.com* etc.) estarán permitidos.



### Reglas

Bloquear o permitir una página web específica puede ser más preciso que bloquear o permitir una categoría completa de páginas web.

## Actualización

Las actualizaciones de rutina de ESET Cyber Security Pro son necesarias para mantener el máximo nivel de seguridad. El módulo de actualización garantiza que el programa se mantenga siempre actualizado mediante la descarga de los módulos de detección más recientes.

Al hacer clic en **Actualización** en el menú principal, encontrará el estado actual de la actualización de ESET Cyber Security Pro, incluidas la fecha y hora de la última actualización correcta, y se indicará si se necesita una nueva

actualización. Para iniciar el proceso de actualización de forma manual, haga clic en **Actualizar ahora**.

En circunstancias normales, cuando las actualizaciones se descargan de manera apropiada, el mensaje **No es necesario actualizar: los módulos instalados son actuales** aparecerá en la ventana de actualizaciones. Si no se pueden actualizar los módulos, se recomienda verificar la [configuración de la actualización](#). El motivo más común de este error es el ingreso incorrecto de los datos de autenticación (el nombre de usuario y la contraseña) o de la [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 que lista la información de actualización del motor de detección.

## Configuración de la actualización

Para eliminar todos los datos de la actualización guardados temporalmente, haga clic en el botón **Borrar** junto a **Borrar el caché de la actualización**. Use esta opción si tiene dificultades durante la actualización.

## Opciones avanzadas

Para deshabilitar las notificaciones luego de cada actualización exitosa, seleccione **No mostrar notificaciones sobre actualizaciones exitosas**.

Para descargar módulos de desarrollo que estén en etapas de pruebas finales, habilite **Actualización previa a su lanzamiento**. En muchos casos, las actualizaciones previas al lanzamiento solucionan problemas del producto. **Actualización demorada** descarga la actualización unas horas después de su lanzamiento, para asegurar que los clientes no reciban actualizaciones hasta que esté confirmado que no tienen errores.

ESET Cyber Security Pro registra instantáneas del motor de detección y de los módulos de programa para usar con la característica de **reversión de la actualización**. Mantenga **Crear instantáneas de archivos de actualización** habilitado para que ESET Cyber Security Pro registre las instantáneas automáticamente. Si sospecha que la nueva actualización del módulo de detección o de los módulos de programas puede ser inestable o estar corrupta, puede hacer una reversión a la versión anterior y deshabilitar cualquier actualización para un período determinado. Para revertir las actualizaciones a una versión anterior en el historial, haga clic en **Reversión**. Como alternativa, puede habilitar actualizaciones antes deshabilitadas si las había pospuesto indefinidamente. Cuando utilice la reversión de la actualización para volver a una actualización anterior, use el menú desplegable **Establecer período de suspensión en** para indicar el período de tiempo por el que quiere suspender las actualizaciones. Si selecciona **hasta que se revoquen** las actualizaciones normales no se reanudarán hasta que las restaure manualmente. Para restaurar las actualizaciones manualmente, haga clic en **Permitir**. Tenga precaución cuando establezca el período de tiempo de suspensión de actualizaciones.

**Establecer la edad máxima del motor de detección automáticamente** Le permite establecer el periodo máximo (en días) luego del que los módulos de detección son declarados obsoletos. El valor predeterminado es 7 días.

## Cómo crear tareas de actualización

Se pueden activar las actualizaciones manualmente al hacer clic en **Actualizar** en el menú principal y luego al hacer clic en **Actualizar módulos**.

Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea

programada, haga clic en **Herramientas > Tareas programadas**. Las siguientes tareas se encuentran activas de forma predeterminada en ESET Cyber Security Pro:

- **Actualización automática de rutina**
- **Actualización automática tras el registro del usuario**

Puede modificar las tareas de actualización mencionadas según sus necesidades. Además de las tareas de actualización predeterminadas, puede crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más detalles sobre la creación y la configuración de tareas de actualización, lea la sección [Tareas programadas](#).

## Reemplazo de ESET Cyber Security Pro por una nueva versión

Para obtener la máxima protección, es importante usar la última compilación de ESET Cyber Security Pro. Para comprobar si hay una nueva versión, 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 otra ventana con el número de versión de la nueva compilación y el historial de cambios.

Haga clic en **Sí** para descargar la última compilación o haga clic en **No ahora** para cerrar la ventana y descargar la actualización más tarde.

Si hizo clic en **Sí**, el archivo se descargará en su carpeta de descargas (o en la carpeta predeterminada del explorador). Cuando el archivo se haya terminado de descargar, ejecútelo y siga las instrucciones de instalación. El Nombre de usuario y la Contraseña se transferirán automáticamente a la nueva instalación. Recomendamos que verifique las mejoras con regularidad, en especial, luego de haber instalado ESET Cyber Security Pro desde un CD/DVD.

## Actualizaciones del sistema

La función de actualización del sistema de macOS es un componente importante diseñado para proteger a los usuarios del software malicioso. Por razones de seguridad máxima, se recomienda instalar estas actualizaciones tan pronto como se encuentren disponibles. ESET Cyber Security Pro le notificará acerca de actualizaciones faltantes de acuerdo con el nivel especificado por usted. Puede ajustar la disponibilidad de las notificaciones de actualizaciones en **Configuración > Ingresar preferencias de aplicación ...** ( o presionar *cmd+,*) > **Alertas y notificaciones > Configuración...** modificando las opciones de **Condiciones de visualización** junto a las **Actualizaciones del sistema operativo**.

- **Mostrar todas las actualizaciones** - se mostrará una notificación cada vez que se detecte una actualización del sistema faltante
- **Mostrar solo recomendadas** - se le notificará solamente acerca de las actualizaciones recomendadas

Si no desea recibir notificaciones acerca de las actualizaciones faltantes, desactive la casilla de verificación **Actualizaciones del sistema operativo**.

La ventana de notificación proporciona un resumen de las actualizaciones disponibles para el sistema operativo macOS y las aplicaciones actualizadas a través de la herramienta nativa de macOS: actualizaciones de software.

Puede ejecutar la actualización directamente en la ventana de actualizaciones o en la sección **Inicio** de ESET Cyber Security Pro haciendo clic en **Instalar la actualización faltante**.

La ventana de aplicaciones contiene nombre, versión, tamaño, propiedades (indicadores) e información adicional acerca de las actualizaciones disponibles. La columna Banderas contiene la siguiente información:

- **[recomendada]**: el fabricante del sistema operativo le recomienda que instale esta actualización para aumentar la seguridad y la estabilidad del sistema.
- **[reinicio]**: se requiere reiniciar el equipo para la siguiente instalación.
- **[apagado]**: se debe apagar el equipo y, luego, encenderlo en la siguiente instalación.

La ventana de notificaciones muestra las actualizaciones recuperadas por la herramienta de línea de comando llamada "softwareupdate". Las actualizaciones recuperadas por esta herramienta pueden variar en comparación con las actualizaciones que se muestran en la aplicación "Software updates". Si desea instalar todas las actualizaciones disponibles que se muestran en la ventana de actualizaciones del sistema operativo y además aquellas que no aparecen en la aplicación "software updates", debe utilizar una herramienta de línea de comando. Para obtener más información acerca de esta herramienta, lea el manual "actualizaciones del software" escribiendo `man softwareupdate` en una ventana de Terminal. Se recomienda solo para usuarios avanzados.

## Herramientas

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

## Archivos de registro

Los archivos de registro contienen información sobre los sucesos importantes del programa que se llevaron a cabo y proporcionan una visión general de las amenazas detectadas. La emisión de registros constituye una herramienta esencial para la exploración del sistema, la detección de amenazas y la solución de problemas. La emisión de registros se mantiene activa en segundo plano sin necesidad de la interacción del usuario. La información se registra de acuerdo con el nivel de detalles actualmente configurado. Se pueden ver los mensajes de texto y los registros directamente desde el entorno de ESET Cyber Security Pro, donde además se pueden archivar registros.

Puede acceder a los archivos de registros desde el menú principal de ESET Cyber Security Pro si hace clic en **Herramientas > Registros**. Seleccione el tipo de registro deseado mediante el menú desplegable **Registro** en la parte superior de la ventana. Se encuentran disponibles los siguientes registros:

1. **Amenazas detectadas**: utilice esta opción para ver toda la información relacionada con la detección de infiltraciones.
2. **Sucesos**: esta opción está diseñada para ayudar a que los administradores del sistema y los usuarios puedan solucionar problemas. Todas las acciones importantes que ESET Cyber Security Pro lleva a cabo se registran en los registros de sucesos.
3. **Exploración del equipo**: en este registro se muestran los resultados de todas las exploraciones completadas. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración bajo demanda correspondiente.

4. **Parental**: lista de todas las páginas web bloqueadas por el control parental.

5. **Firewall**: este registro contiene los resultados de todos los eventos relacionados con la red.

6. **Sitios web filtrados**: esta lista es útil si desea visualizar una lista de sitios web bloqueados por la protección de acceso web. En estos registros puede ver la hora, la URL, el estado, la dirección IP, el usuario y la aplicación que abrió una conexión con el sitio Web en particular.

En cada una de las secciones, la información mostrada se puede copiar directamente en el portapapeles seleccionando la entrada y haciendo clic en el botón **Copiar**.

## Mantenimiento de registros

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

- **Eliminar automáticamente los historiales de registros antiguos**: las entradas de registros anteriores a la cantidad de días especificada se eliminan automáticamente (90 días de manera predeterminada).
- **Optimizar archivos de registro automáticamente**: habilita la desfragmentación automática de archivos de registro si se excedió el porcentaje especificado de historiales sin usar (25 % de manera predeterminada).

Toda la información relevante que se muestra en la interfaz gráfica de usuario, las amenazas y los mensajes sobre sucesos pueden almacenarse en formatos de texto legibles para los usuarios como texto simple o CSV (Comma-separated values). Si desea que estos archivos estén disponibles para el procesamiento con herramientas de terceros, seleccione la casilla de verificación junto a **Habilitar la emisión de registros a archivos de texto**.

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

En base a las opciones seleccionadas en **Archivos de registro de texto: Editar**, puede guardar registros con la siguiente información escrita:

○ Los sucesos tales como *Nombre de usuario y contraseña no válidos, Los módulos no se pueden actualizar* etc. se escriben al archivo `eventslog.txt`.

○ Las amenazas detectadas por la exploración inicial, la protección en tiempo real o la exploración del equipo se guardan en el archivo llamado `threatslog.txt`.

○ Los resultados de todas las exploraciones completadas se guardan en el formato `scanlog.NÚMERO.txt`.

○ Todos los eventos relacionados con la comunicación a través de Firewall están escritos en `firewalllog.txt`

Para configurar los filtros para el **Historiales predeterminados de registro de exploraciones del equipo**, haga clic en **Edit** y seleccione los tipos de registros o quite la selección según sea necesario. Puede encontrar explicaciones adicionales acerca de estos tipos de registros en [Filtrado de registros](#).

## Filtrado de registros

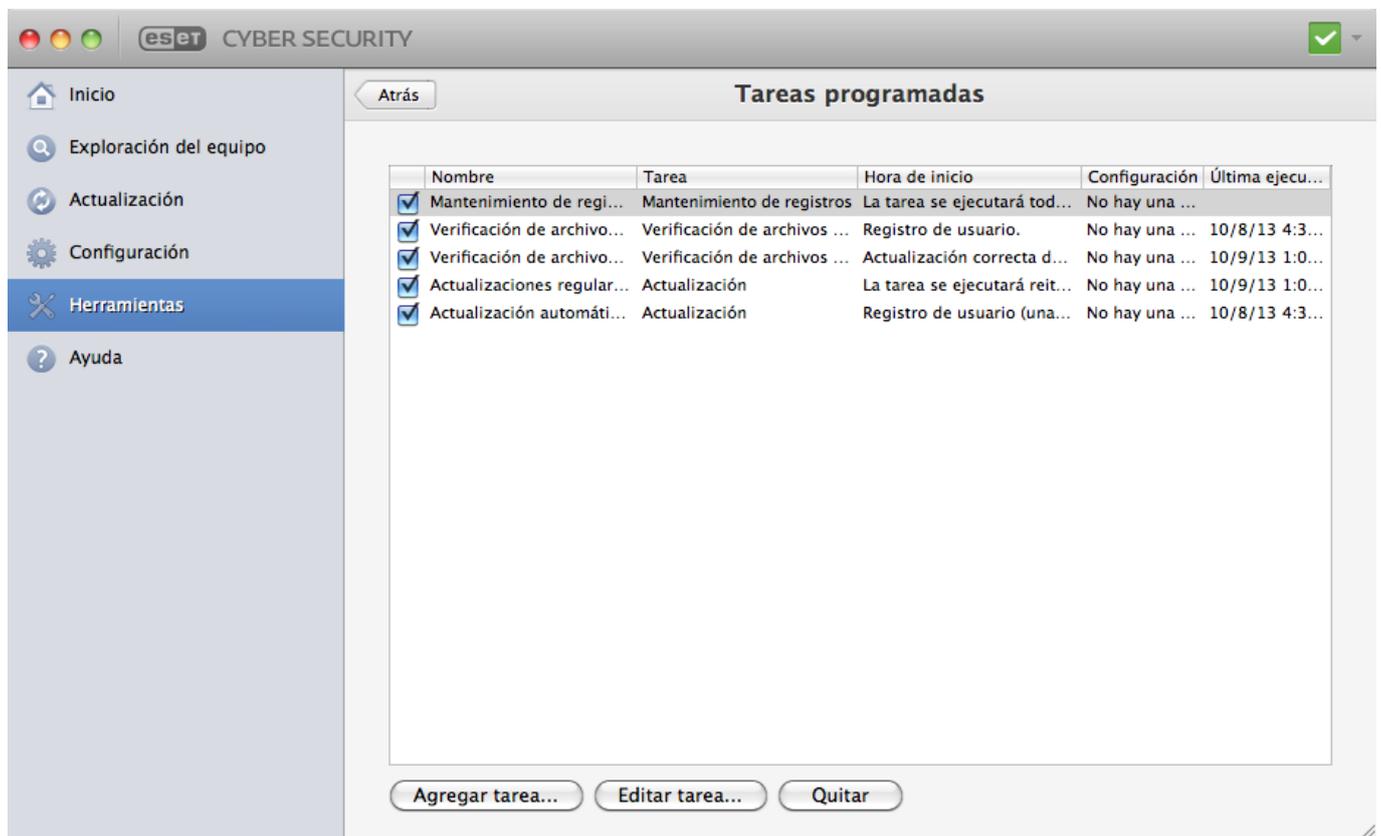
Los registros almacenan información sobre los sucesos importantes del sistema. La función de filtrado de registros permite mostrar historiales acerca de un tipo específico de suceso.

Los tipos de registro usados con mayor frecuencia se muestran en la lista a continuación:

- **Advertencias críticas:** errores críticos del sistema (por ej., falló el inicio de la protección antivirus).
- **Errores:** mensajes de error, tales como “*Error al descargar el archivo*” y errores críticos.
- **Advertencias:** mensajes de advertencia.
- **Historiales informativos:** mensajes informativos entre los que se incluyen las actualizaciones completadas correctamente, las alertas, etc.
- **Historiales de diagnóstico:** información necesaria para poner a punto el programa así como todos los registros descritos arriba.

## Tareas programadas

Puede encontrar las **Tareas programadas** en el menú principal de ESET Cyber Security Pro en la sección **Herramientas**. La sección **Tareas programadas** contiene una lista de todas las tareas programadas y propiedades de configuración, como la fecha y la hora predefinidas, y el perfil de análisis utilizado.



Desde la sección de tareas programadas se administran y ejecutan tareas programadas según configuraciones y propiedades predefinidas. La configuración y las propiedades contienen información, como la fecha y la hora, además de perfiles especificados para utilizar durante la ejecución de la tarea.

De forma predeterminada, se muestran las siguientes tareas programadas:

- Mantenimiento de registros (después de habilitar la opción **Mostrar tareas del sistema** en la configuración de las tareas programadas).
- Inicio de la verificación de archivos tras el registro del usuario

- Verificación de archivos de inicio después de una actualización con éxito de los módulos de detección
- Actualización automática de rutina
- Actualización automática tras el registro del usuario

Para editar la configuración de una tarea programada existente (ya sea predeterminada o definida por el usuario), presione CTRL+, haga clic en la tarea que desea modificar y seleccione **Editar** o seleccione la tarea y haga clic en el botón **Editar tarea**.

## Creación de tareas nuevas

Para crear una nueva tarea programada, haga clic en **Agregar tarea...** o haga CTRL+clic en el campo en blanco y seleccione **Agregar...** del menú contextual. Se encuentran disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación**
- **Actualización**
- **Mantenimiento de registros**
- **Exploración del equipo a petición**
- **Verificación de archivos de inicio del sistema**



### Ejecutar aplicación

Al elegir **Ejecutar aplicación**, puede ejecutar programas como un usuario de sistema llamado "nadie". Los permisos de las aplicaciones en ejecución mediante Tareas programadas son definidos por macOS. Para cambiar el usuario desde la forma predeterminada, escriba el nombre de usuario seguido de dos puntos (:) delante de la instrucción. También puede usar el usuario **raíz** en esta característica.



### Ejemplo: Ejecute una tarea como usuario

En este ejemplo, programaremos la aplicación de la calculadora para comenzar a una hora seleccionada como un usuario llamado **UsuarioUno**:

1. En el **Programador**, seleccione **Agregar tarea**.
2. Escriba en el nombre de la tarea. Seleccione **Ejecutar aplicación** como una **Tarea programada**. En la ventana **Ejecutar tarea**, seleccione **Una vez** para ejecutar esta tarea una única vez. Haga clic en **Siguiente**.
3. Haga clic en Examinar y seleccione la aplicación de la calculadora.
4. Escriba **UserOne:** antes de la ruta de la aplicación (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') y haga clic en **Siguiente**.
5. Seleccione una hora para ejecutar la tarea y haga clic en **Siguiente**.
6. Seleccione una opción alternativa si no se puede ejecutar la tarea y haga clic en **Siguiente**.
7. Haga clic en **Finalizar**.
8. El programador ESET iniciará la aplicación de la calculadora a la hora que seleccionó.



### Ejemplo: Tarea de actualización

En este ejemplo crearemos una tarea de actualización que se ejecutará en una hora especificada.

1. Desde del menú desplegable **Tarea programada** seleccione **Actualizar**.
2. Ingrese el nombre de la tarea en el campo **Nombre de tarea**.
3. Seleccione la frecuencia de la tarea en el menú desplegable **Ejecutar tarea**. Según la frecuencia seleccionada, se le pedirá que especifique los diferentes parámetros de actualización. Si selecciona **Definido por el usuario**, se le pedirá que especifique fecha y hora en formato cron (consulte la sección [Creación de tarea definida por el usuario](#) para obtener más información).
4. En el siguiente paso, defina que acción tomar si no se puede realizar o completar la tarea a la hora programada.
5. En el último paso, se mostrará una ventana resumen con la información acerca de la tarea programada actual. Haga clic en **Finalizar**. Se agregará la nueva tarea programada a la lista de tareas programadas actualmente.

De manera predeterminada ESET Cyber Security Pro contiene las tareas programadas predefinidas para asegurar la correcta funcionalidad del producto. Estos no se pueden alterar, y se ocultan de manera predeterminada. Para que se vean estas tareas, en el menú principal, haga clic en **Configuración > Ingresar preferencias de aplicación...** (O presione *cmd+,*) > **Programador** y seleccione **Mostrar tareas del sistema**.

## Exploración como propietario del directorio

Puede explorar los 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 explorar la carpeta /tmp como un usuario actualmente registrado:

```
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 hora de la tarea **Definida por el usuario** se debe ingresar en el formato cron con año extendido (una cadena compuesta por 6 campos separados por un espacio):

```
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 expresiones cron:

- asterisco (\*): la expresión coincidirá con todos los valores del campo; por ejemplo, el asterisco en el 3.er

campo (día del mes) significa todos los días

- guion (-): define rangos; por ejemplo, 3-9
- coma (,): separa elementos de una lista; por ejemplo, 1, 3, 7, 8
- barra (/): define incrementos de rangos; por ejemplo, 3-28/5 en el 3.er campo (día del mes) significa el 3.er día del mes y luego cada 5 días.

Nombres de días (Monday-Sunday) y nombres de meses (January-December) no son compatibles.



### Ejecutar comandos

Si define tanto el día del mes como el día de la semana, el comando se ejecutará solamente cuando ambos campos coincidan.

## Cuarentena

El objetivo principal de la cuarentena consiste en almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena cuando no se pueden limpiar, cuando no es seguro o recomendable eliminarlos o cuando son detectados erróneamente por ESET Cyber Security Pro.

Puede elegir poner cualquier archivo en cuarentena. Esta acción es recomendable cuando un archivo se comporta de manera sospechosa pero la exploración antivirus no lo detecta. 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 visualizar en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta a la ubicación original de los archivos infectados, su tamaño en bytes, el motivo (por ej., agregado por el usuario) y la cantidad de amenazas (por ej., si se trata de un archivo comprimido que contiene varias infiltraciones). La carpeta de cuarentena con los archivos en cuarentena () permanecerá en el sistema incluso después de desinstalar ESET Cyber Security Pro. Los archivos en cuarentena se guardan en un formato seguro codificado y se pueden restaurar nuevamente tras instalar ESET Cyber Security Pro.

## Envío de archivos a cuarentena

ESET Cyber Security Pro envía automáticamente a cuarentena los archivos eliminados (a menos que se anule la selección de esta opción en la ventana de alerta). Puede ingresar manualmente en cuarentena a cualquier archivo sospechoso al hacer clic en **Cuarentena...** . También puede utilizar el menú contextual para este fin, haga CTRL+clic en el campo en blanco, seleccione **Cuarentena**, seleccione el archivo que desea ingresar en cuarentena y haga clic en **Abrir**.

## Restauración desde Cuarentena

Los archivos en cuarentena también se pueden restaurar a su ubicación original, para hacerlo, seleccione un archivo en cuarentena y haga clic en **Restaurar**. La restauración además está disponible desde el menú contextual, haga clic en CTRL+ sobre un archivo determinado en la ventana de Cuarentena y haga clic en **Restaurar**. Asimismo, el menú contextual ofrece la opción **Restaurar a...**, que permite restaurar un archivo en una ubicación diferente de la que tenía cuando fue eliminado.

# Envío de archivos desde Cuarentena

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

## Procesos en ejecución

La lista de **Procesos en ejecución**, muestra los procesos en ejecución en el equipo. ESET Cyber Security Pro proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología de ESET Live Grid.

- **Proceso:** nombre del proceso que se está ejecutando actualmente en el equipo. Para ver todos los procesos en ejecución, también puede usar Monitor de actividades (que se encuentra en */Applications/Utilities*).
- **Nivel de riesgo:** en la mayoría de los casos, ESET Cyber Security Pro y la tecnología de ESET Live Grid asignan niveles de riesgo a los objetos (archivos, procesos, etc.) mediante una serie de reglas heurísticas que examinan las características de cada objeto y, luego, evalúan su potencial de actividad maliciosa. Según estas heurísticas, los objetos se asignan a un nivel de riesgo. Las aplicaciones conocidas marcadas con verde están definitivamente limpias (están en la lista blanca) y se excluirán de la exploración. Esto mejora la velocidad tanto de las exploraciones bajo demanda como de las exploraciones en tiempo real. Si una aplicación está marcada como desconocida (con amarillo), no significa necesariamente que sea software malicioso. Por lo general, es una aplicación más nueva. Si no está seguro acerca de un archivo, puede enviarlo al Laboratorio de amenazas de ESET para su análisis. Si el archivo resulta ser una aplicación maliciosa, se agregará su firma en una de las próximas actualizaciones.
- **Cantidad de usuarios:** cantidad de usuarios que usan una determinada aplicación. Esta información es recopilada por la tecnología de ESET Live Grid.
- **Tiempo de detección:** período de tiempo desde que la tecnología de ESET LiveGrid® detectó la aplicación.
- **Identificación del paquete de la aplicación:** nombre del proveedor o del proceso de la aplicación.

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

- **Archivo:** ubicación de una aplicación en el equipo
- **Tamaño del archivo:** tamaño físico del archivo en el disco
- **Descripción del archivo:** características del archivo según la descripción proporcionada por el sistema operativo
- **Identificación del paquete de la aplicación:** nombre del proveedor o del proceso de la aplicación
- **Versión del archivo:** información proporcionada por el desarrollador de la aplicación
- **Nombre del producto:** nombre de la aplicación o nombre comercial

# Conexiones de red

Conexiones de red es una lista de conexiones de red activa en su equipo. ESET Cyber Security Pro Proporciona información detallada acerca de cada conexión y le permite crear una regla para bloquear estas conexiones.

## Crear 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, puede hacer clic con el botón secundario sobre la conexión y seleccionar **Crear regla de bloqueo para esta conexión**.

1. Seleccione el **Perfil** de conexión para el cual desea crear la regla y escriba el nombre de la regla. Seleccione la aplicación de la regla a la que se debe aplicar o seleccione la casilla de verificación para que la regla se aplique a todas las aplicaciones.
2. Seleccione una acción para la conexión, ya sea para denegar (bloquear) la conexión o permitirla. Seleccione la dirección de la comunicación a la que se debe aplicar la regla. Para crear un archivo de registro para la regla, haga clic en la **regla de registro**.
3. Seleccione el protocolo de conexión y los tipos de puertos. Seleccione el puerto para el servicio o especifique un rango de puertos con el formato: Desde-Hasta.
4. Seleccione el destino e ingrese la información en el campo obligatorio, según su destino.

## Live Grid

El sistema de alerta temprana Live Grid mantiene a ESET informado sobre las nuevas infiltraciones de forma instantánea y continua. El sistema bidireccional de alerta temprana Live Grid tiene un único propósito: mejorar la protección que le ofrecemos al usuario. La mejor forma de asegurarnos de ver las nuevas amenazas ni bien aparecen es establecer un “vínculo” con la mayor cantidad posible de clientes, que cumplirán el papel de exploradores de amenazas. Hay dos opciones:

1. Decidir que no desea habilitar el sistema de alerta temprana Live Grid. Se mantendrán las mismas funciones del software y usted seguirá recibiendo la mejor protección que le podemos ofrecer.
2. Configurar el sistema de alerta temprana Live Grid para enviar información anónima sobre nuevas amenazas y sobre el contexto donde se encuentra dicho código. Es posible enviar esta información a ESET para su análisis detallado. El estudio de dichas amenazas le servirá a ESET para actualizar su motor de detección y mejorar la capacidad de detección de amenazas del programa.

El sistema de alerta temprana Live Grid recopilará información anónima sobre el equipo en relación con las nuevas amenazas detectadas. Dicha información puede incluir una muestra o copia del archivo donde apareció la amenaza, la ruta a ese archivo, el nombre del archivo, la fecha y la hora, el proceso mediante el cual apareció la amenaza en su equipo y la información sobre el sistema operativo del equipo.

Aunque cabe la posibilidad de que ocasionalmente este proceso revele cierta información acerca del usuario o del equipo (nombres de usuario en la ruta a un directorio, etc.) al Laboratorio de amenazas de ESET, la información no se usará BAJO NINGUNA CIRCUNSTANCIA con otro propósito que no sea para ayudar a responder de inmediato a nuevas amenazas.

Para acceder a la configuración de Live Grid en el menú principal, haga clic en **Configuración > Ingresar preferencias de aplicación...** (o presione *cmd+,*) > **Live Grid**. Seleccione **Habilitar el sistema de advertencia**

**temprana de Live Grid** para activar Live Grid y luego haga clic en **Configuración...** Ubicado junto a **Opciones Avanzadas**.

## Configuración de Live Grid

De forma predeterminada, ESET Cyber Security Pro está configurado para enviar archivos sospechosos al Laboratorio de amenazas de ESET para su análisis detallado. Si no desea enviar estos archivos automáticamente, anule la selección **Envío de archivos**.

Si encuentra un archivo sospechoso, puede enviarlo a nuestro Laboratorio de amenazas 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.

**Envío de estadística anónima:** el sistema de alerta temprana ESET Live Grid recopila información anónima sobre el equipo relacionada con las nuevas amenazas detectadas. Esta información incluye el nombre de la infiltración, la fecha y la hora en que fue detectada, la versión del producto de seguridad de ESET, la versión del sistema operativo y la configuración de la ubicación. Típicamente, estas estadísticas se envían a los servidores de ESET una o dos veces por día.

**Filtro de exclusión:** esta opción le permite excluir ciertos tipos de archivos del envío. Por ejemplo, quizá resulte útil excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen de forma predeterminada (.doc, .rtf, etc.). Es posible agregar tipos de archivos a la lista de archivos excluidos.

**Correo electrónico de contacto (opcional):** se usará su dirección de correo electrónico en caso de que se requiera información adicional para el análisis. Recuerde que no recibirá ninguna respuesta de ESET a menos que se necesite información adicional.

## Enviar muestra para su análisis

Si encuentra un archivo de conducta sospechosa en su equipo, puede enviarlo al laboratorio de investigación de ESET para su análisis.



### Antes de enviar muestras a ESET

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

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

Para realizar un envío de muestra, utilice el formulario de envío de muestras de su producto. Está ubicado en **Herramientas > Enviar muestra para su análisis**.

En el formulario **Enviar muestra para su análisis**, complete lo siguiente:

**Archivo** – la ruta al archivo que desea enviar.

**Comentario** – describa el motivo por el que envía el archivo.

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



### Es posible que no obtenga respuesta de ESET.

No obtendrá una respuesta de ESET a menos que se requiera más información, ya que nuestros servidores reciben decenas de miles de archivos por día, lo que hace imposible responder a todos los envíos.

Si la muestra resulta ser una aplicación maliciosa o sitio malicioso, se agregará su detección a una de las próximas actualizaciones de ESET.

## Interfaz del usuario

Las opciones de configuración de la interfaz del usuario permiten ajustar el entorno de trabajo conforme a sus necesidades. Estas opciones están disponibles en el menú principal al hacer clic en **Configuración > Ingresar preferencias de aplicación...** (o presionar *cmd+,*) > **Interfaz**.

- Para habilitar la pantalla de bienvenida de ESET Cyber Security Pro al iniciar el programa, seleccione la opción **Mostrar la pantalla de bienvenida al iniciar el programa**.
- La opción **Aplicación presente en la barra inferior Dock** permite mostrar el ícono ESET Cyber Security Pro  en el Dock de macOS y cambiar entre ESET Cyber Security Pro y otras aplicaciones en ejecución presionando *cmd-tab*. Los cambios se aplican después de reiniciar ESET Cyber Security Pro (generalmente activado mediante el reinicio del sistema).
- La opción **Usar el menú estándar** permite usar ciertos accesos directos del teclado (consulte [Accesos directos del teclado](#)) para ver elementos del menú estándar (Interfaz del usuario, Configuración y Herramientas) en la barra del menú de macOS (en la parte superior de la pantalla).
- Para habilitar descripciones emergentes para determinadas opciones de ESET Cyber Security Pro, seleccione la opción **Mostrar descripción emergente**.
- **Mostrar archivos ocultos** permite ver y seleccionar archivos ocultos durante la configuración de los **Objetos para explorar** de una **Exploración del equipo**.
- De forma predeterminada, el ícono de ESET Cyber Security Pro  se muestra en los Extras de la barra de menús que aparecen a la derecha de la barra de menús de macOS (parte superior de la pantalla). Para desactivarlo, deseccione **Mostrar ícono en la barra de menús extras**. Estos cambios se aplican después de reiniciar ESET Cyber Security Pro (generalmente activado mediante el reinicio del sistema).

## Alertas y notificaciones

La sección **Alertas y notificaciones** le permite configurar cómo ESET Cyber Security Pro gestionará las alertas ante amenazas y las notificaciones del sistema.

Deshabilitar la opción **Mostrar alertas** deshabilitará todas las ventanas de alerta y únicamente se recomienda en situaciones específicas. Para la mayoría de los usuarios, recomendamos dejar esta opción en su configuración

predeterminada (habilitada). Las opciones avanzadas se describen [en este capítulo](#).

Seleccionar la opción **Mostrar notificaciones en el escritorio** hará que las ventanas de alerta no requieran la interacción del usuario en el escritorio (aparecerán en forma predeterminada en la esquina superior derecha de la pantalla). Puede definir la duración de la visualización de las notificaciones ajustando el valor **Cerrar notificaciones automáticamente después de X segundos** (5 segundos de manera predeterminada).

A partir de la versión 6.2 de ESET Cyber Security Pro, también puede evitar que determinados **Estados de protección** se muestren en la pantalla principal del programa (ventana **Estado de protección**). Para obtener más información acerca de esto, visite la sección [Estados de protección](#).

## Mostrar alertas

ESET Cyber Security Pro muestra ventanas de diálogo de alertas que le informan acerca de nuevas versiones del programa, actualizaciones del sistema operativo, la inhabilitación de ciertos componentes del programa, la eliminación de registros, etc. Puede suprimir las notificaciones individualmente mediante la selección de la opción **No volver a mostrar este cuadro de diálogo**.

**Lista de cuadros de diálogo (Configuración > Ingresar preferencias de aplicación... > Alertas y notificaciones > Configuración...)** muestra la lista de todos los diálogos activados por ESET Cyber Security Pro. Para habilitar o suprimir cada notificación, seleccione la casilla de verificación a la izquierda del **Nombre del diálogo**. Además, puede definir **Mostrar condiciones** según las cuales se mostrarán las notificaciones acerca de la nueva versión del programa y de la actualización del sistema operativo.

## Estado de la protección

El estado de protección actual de ESET Cyber Security Pro se puede alterar al activar o desactivar estados en **Configuración > Ingresar preferencias de aplicación... > Alertas y notificaciones > Mostrar en la pantalla de Estado de protección: Configuración**. El estado de varias características del programa se mostrarán u ocultarán de la pantalla principal de ESET Cyber Security Pro (ventana de **Estado de la protección**).

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

- Firewall
- Anti-Phishing
- Protección del acceso a la Web
- Protección del cliente de correo electrónico
- Actualización de sistema operativo
- ¡La licencia expiró!
- Se requiere el reinicio del equipo

## Privilegios

ESET Cyber Security Pro La configuración puede ser muy importante para la directiva de seguridad de la empresa. Las modificaciones no autorizadas pueden poner en peligro la estabilidad y la protección del sistema. Por este

motivo, es posible seleccionar los usuarios que tendrán permiso para editar la configuración del programa.

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



### Acerca de la actualización

Si deja vacía la lista de Usuarios seleccionados, todos los usuarios se consideraran privilegiados.

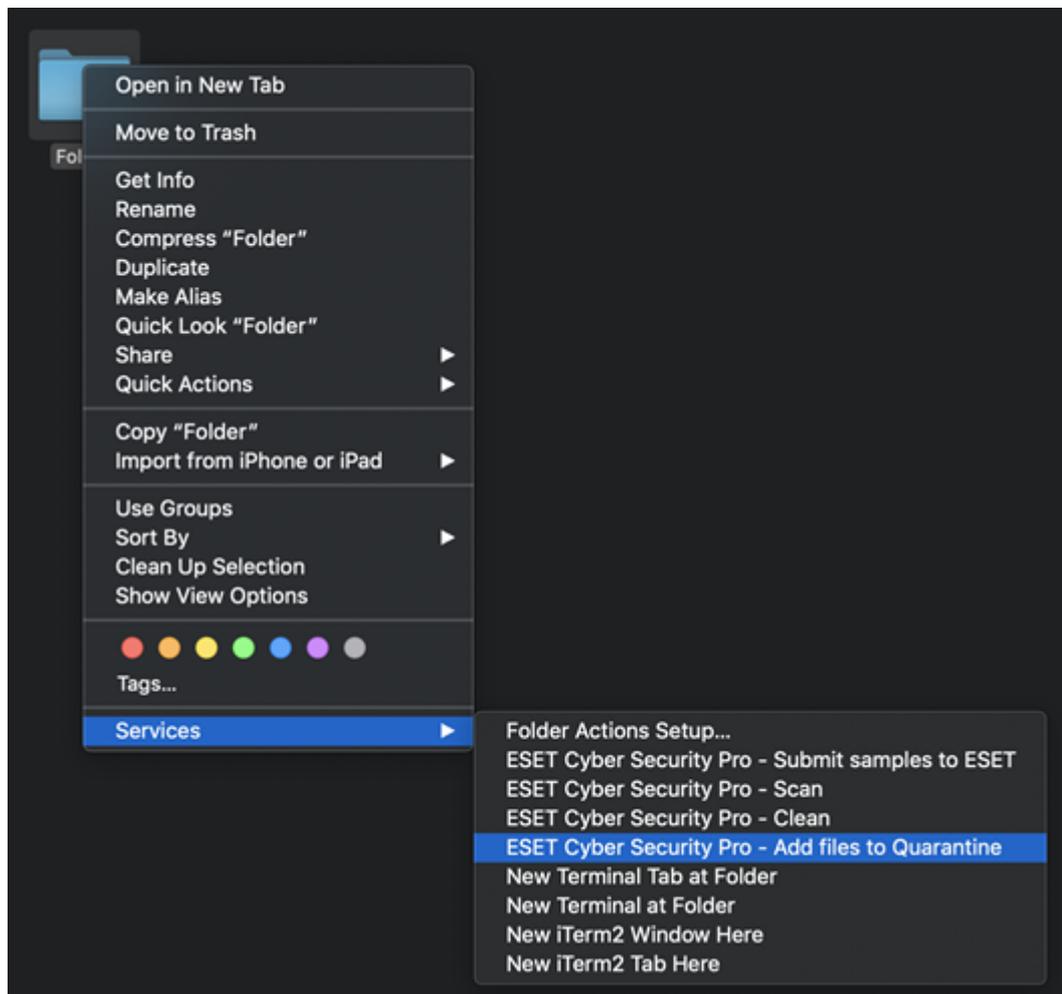
## Menú contextual

Se puede habilitar la integración del menú contextual al hacer clic en **Configuración > Introducir preferencias de aplicación...** (O presione *cmd+,*) > sección del **Menú contextual** al seleccionar la opción **Integrar en el menú contextual**. Los cambios entrarán en vigor cuando cierre sesión o reinicie el equipo. Las opciones de menú contextual estarán disponibles en la ventana **Finder** al hacer CTRL+clic en cualquier archivo.

Puede seleccionar opciones que se mostrarán en el menú contextual. Puede mostrar la opción **Solo explorar**, que le permitirá explorar el archivo seleccionado, la opción **Solo desinfectar** que le permitirá desinfectar el archivo seleccionado desde el menú contextual. Elija la opción de desinfección si un virus atacó un archivo y le ha adjuntado códigos maliciosos. Si este es el caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo está compuesto exclusivamente por códigos maliciosos, será eliminado.

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

- Enviar muestras a ESET
- Exploración
- Limpio
- [Agregar archivos a la Cuarentena](#)



## Importar y exportar configuración

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

La importación y la exportación resultan útiles cuando es necesario realizar una copia de seguridad de la configuración actual de ESET Cyber Security Pro para poder utilizarla más tarde. La configuración de exportación también es conveniente para usuarios que deseen utilizar su configuración preferida de ESET Cyber Security Pro en varios sistemas. Puede fácilmente importar un archivo de configuración para transferir sus configuraciones deseadas.



Para importar una configuración, seleccione **Importar configuración** y haga clic en **Examinar** para dirigirse al archivo de configuración que desea importar. Para exportar, seleccione **Exportar configuración** y use el explorador para seleccionar una ubicación en el equipo para guardar el archivo de configuración.

## Configuración del servidor proxy

La configuración del servidor proxy se puede configurar en **Configuración > Ingresar preferencias de aplicación...** (o presionar *cmd+,*) > **Servidor Proxy**. La especificación del servidor proxy en este nivel define la configuración global del servidor proxy para todas las funciones de ESET Cyber Security Pro. Los parámetros definidos aquí serán utilizados por todos los módulos que requieren conexión a Internet. ESET Cyber Security Pro soporta los tipos de autenticación del Acceso básico y NTLM (Administrador NT LAN).

Para especificar la configuración del servidor proxy para este nivel, seleccione **Usar servidor proxy** e introduzca la dirección IP o la dirección URL del servidor proxy en el campo **Servidor proxy**. En el campo Puerto, especifique el puerto en el que el servidor proxy aceptará las conexiones (el predeterminado es 3128). También puede hacer clic en **Detectar** para permitir que el programa complete ambos campos.

Si la comunicación con el servidor proxy requiere autenticación, introduzca un **Usuario** y **Contraseña** válidos en los campos respectivos.

## Acuerdo de licencia de usuario final

**IMPORTANTE:** Lea los términos y las condiciones del producto de aplicación que se especifican abajo antes de descargarlo, instalarlo, copiarlo o usarlo. **AL DESCARGAR, INSTALAR, COPIAR O UTILIZAR EL SOFTWARE, USTED DECLARA SU CONSENTIMIENTO CON LOS TÉRMINOS Y CONDICIONES Y RECONOCE QUE HA LEÍDO LA [POLÍTICA DE PRIVACIDAD](#).**

### Acuerdo de Licencia de Usuario Final

Bajo los términos de este Acuerdo de licencia de usuario final (en adelante, el "Acuerdo") celebrado entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, inscrita en el Registro Mercantil y de Sociedades administrado por el Tribunal del Distrito I de Bratislava, Sección Sro, Asiento n.º 3586/B, Número de registro comercial 31333532 (en adelante, "ESET" o el "Proveedor") y Usted, persona física o jurídica (en adelante, "Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el Artículo 1 del presente Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

Al hacer clic en la opción "Acepto" durante la instalación, la descarga, la copia o la utilización del Software, Usted acepta los términos y condiciones del presente Acuerdo. Si no acepta todas las disposiciones de este Acuerdo, haga clic en la opción "No acepto" de inmediato, cancele la instalación o la descarga, destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al punto de venta donde adquirió el Software.

USTED ACEPTA QUE LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE

Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

**1. Software.** Tal como se utiliza en este Acuerdo, el término "Software" significa: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todos los contenidos de los discos, CD-ROMs, DVDs, correos electrónicos y cualquier adjunto, u otros medios con los cuales se provee este Acuerdo, incluyendo el formulario del código objeto del software provisto en soporte digital, por medio de correo electrónico o descargado a través de la Internet; (iii) cualquier material escrito explicativo relacionado y cualquier otra documentación posible relacionada con el Software, sobre todo cualquier descripción del Software, sus especificaciones, cualquier descripción de las propiedades u operación del software, cualquier descripción del ambiente operativo en el cual se utiliza el Software, instrucciones de uso o instalación del Software o cualquier descripción del modo de uso del Software (en adelante referido como "Documentación"); (iv) copias del Software, parches para posibles errores del Software, adiciones al Software, extensiones del Software, versiones modificadas del Software y actualizaciones de los componentes del Software, si existieran, con la autorización que le da a Usted el Proveedor con arreglo al Artículo 3 de este Acuerdo. El Software será provisto exclusivamente en la forma de código objeto ejecutable.

**2. Instalación, equipo y clave de licencia.** El Software suministrado en un soporte digital, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. El Software debe instalarse en un equipo correctamente configurado que cumpla, como mínimo, con los requisitos especificados en la Documentación. La metodología de instalación se describe en la Documentación. No puede haber ningún programa informático ni Hardware que pudiera afectar al Software instalado en el equipo en el que instala el Software. El equipo hace referencia al Hardware que incluye, pero no se limita, a equipos personales, equipos portátiles, estaciones de trabajo, equipos de bolsillo, teléfonos inteligentes, dispositivos electrónicos portátiles o cualquier otro dispositivo para el que se diseñe el Software y en el que vaya a instalarse y/o utilizarse. La clave de licencia se refiere a una secuencia única de símbolos, letras números o caracteres especiales que se le brinda al Usuario final para permitirle el uso del Software de manera legal, así como de una versión específica de este o para brindarle una extensión de los términos de la Licencia en conformidad con el presente Acuerdo.

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

a) **Instalación y uso.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) **Disposición sobre la cantidad de licencias.** El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático, o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo (en adelante, "AUC"). Si un AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo. El Usuario final tiene el derecho de ingresar la clave de licencia para acceder al Software solo en la medida en que utilice el Software en conformidad con las limitaciones que surgen de la cantidad de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

c) **Business Edition.** Para usar el Software en servidores de correo, pasarelas de correo, puertas de correo o puertas de Internet, deberá adquirir la versión Business Edition del Software.

d) **Término de la Licencia.** El derecho a utilizar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El Software de OEM estará limitado al equipo con el cual lo adquirió. No puede transferirse a otro equipo.

f) **Software NFR y versión de prueba.** Al Software clasificado como "No apto para la reventa", "NFR" o "Versión de prueba" no se le podrá asignar un pago y puede utilizarse únicamente para hacer demostraciones o evaluar las características del Software.

g) **Rescisión de la Licencia.** La Licencia se rescindirá automáticamente al finalizar el período para el cual fue otorgada. Si Usted no cumple con alguna de las disposiciones de este Acuerdo, el Proveedor tendrá el derecho de anular el Acuerdo, sin perjuicio de cualquier derecho o recurso judicial disponible para el Proveedor en dichas eventualidades. En el caso de cancelación de la Licencia, Usted deberá borrar, destruir o devolver de inmediato por su propia cuenta el Software y todas las copias de seguridad a ESET o al punto de venta donde obtuvo el Software. Tras la finalización de la Licencia, el Proveedor podrá cancelar el derecho del Usuario Final a utilizar las funciones del Software que requieran conexión a los servidores del Proveedor o de terceros.

**4. Funciones con recopilación de información y requisitos para la conexión a Internet.** Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para llevar a cabo las siguientes funciones del Software:

a) **Actualizaciones del Software.** El Proveedor tendrá el derecho de lanzar actualizaciones del Software de cuando en cuando (en adelante, "Actualizaciones"), pero no tiene la obligación de suministrar actualizaciones. Esta función se encuentra habilitada en la configuración estándar del Software, por lo que las Actualizaciones se instalan en forma automática, a menos que el Usuario final haya deshabilitado la instalación automática de las Actualizaciones. A fin de que se suministren las Actualizaciones, es necesario llevar a cabo la verificación de la autenticidad de la Licencia, que incluye información relacionada con el equipo y/o con la plataforma en la que se instale el Software en conformidad con la Política de Privacidad.

b) **Envío de infiltraciones e información al Proveedor.** El Software contiene funciones que reúnen muestras de nuevos virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URLs, paquetes de IP y marcos de Ethernet (en adelante denominados "Infiltraciones") y luego los envía al Proveedor, incluso, por ejemplo, la información sobre el proceso de instalación, el equipo o la plataforma en los cual se instala el Software, o la información sobre las operaciones y la funcionalidad del Software (en adelante referida como "Información"). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados.

La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.

ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor. El Usuario final debe activar esta función durante la instalación del Software.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo. Por medio del presente, Usted acepta recibir notificaciones y mensajes que incluye, pero que no se limitan a, información relacionada con el marketing.

**Los detalles sobre la privacidad, la protección de la información personal y sus derechos como parte interesada pueden encontrarse en la Política de Privacidad, disponible en el sitio web del Proveedor y a la que se puede acceder de manera directa desde el proceso de instalación. También puede acceder a ella desde la sección de ayuda del Software.**

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

**6. Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar el Software, Usted tiene la obligación de cumplir con las siguientes restricciones:

a) Puede crear una copia del Software en un soporte de almacenamiento permanente de datos como una copia de seguridad para archivar, siempre que su copia de seguridad para archivar no esté instalada ni se utilice en ningún equipo. Cualquier otra copia que realice del Software constituirá un incumplimiento de este Acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el Software, o transferir los derechos de su uso o copias realizadas del Software de ninguna otra forma a lo establecido en este Acuerdo.

c) No puede vender, sublicenciar, arrendar o alquilar el Software, ni usarlo para suministrar servicios comerciales.

d) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar el Software, ni intentar obtener el código fuente del Software de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.

e) Usted acepta que solo usará el Software de forma que se cumplan todas las leyes aplicables en la jurisdicción en la que lo utilice, incluyendo, pero sin limitarse a, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor

cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

g) Usted acepta no ejercer ninguna actividad que implique el uso de la clave de Licencia de manera contraria a los términos de este Acuerdo ni que implique proporcionar la clave de Licencia a personas que no estén autorizadas a hacer uso del Software, como la transferencia de la clave de Licencia usada o no. en cualquier forma, así como la reproducción no autorizada, o la distribución de claves de Licencia duplicadas o generadas. Asimismo, no utilizará el Software como resultado del uso de una clave de Licencia obtenida de una fuente que no sea el Proveedor.

**7. Copyright.** El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciatarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciatarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del Proveedor en relación con el incumplimiento de este Acuerdo.

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

**9. Versiones en varios idiomas, software en medios duales, varias copias.** En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

**10. Comienzo y rescisión del Acuerdo.** Este Acuerdo es efectivo desde la fecha en que Usted acepta los términos de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

**11. DECLARACIONES DEL USUARIO FINAL.** COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINGIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. **Sin más obligaciones.** Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD.** HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS LICENCIARIOS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, INGRESOS O VENTAS O DE PÉRDIDAS DE DATOS O COSTES SOPORTADOS PARA OBTENER PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES, ESPECIALES O SUCESIVOS CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, AGRAVIO, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO AL USO O A LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR, SUS LICENCIARIOS O SUS AFILIADOS HAYAN SIDO NOTIFICADOS SOBRE 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, LICENCIARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

15. **Soporte técnico.** ESET o los terceros autorizados por ESET suministrarán soporte técnico a discreción propia, sin ninguna garantía ni declaración. El Usuario final deberá crear una copia de seguridad de todos los datos existentes, software y prestaciones de los programas en forma previa al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET no pueden aceptar la responsabilidad por el daño o pérdida de datos, propiedad, software o hardware, o pérdida de beneficios debido al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET se reservan el derecho de decidir si la solución del problema excede el alcance del soporte técnico. ESET se reserva el derecho de rechazar, suspender o dar por finalizado el suministro de soporte técnico a discreción propia. Se puede solicitar información sobre la Licencia y cualquier otro tipo de información a fin de brindar soporte técnico conforme a la Política de Privacidad.

16. **Transferencia de la Licencia.** El Software puede transferirse de un sistema informático a otro, a menos que esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a usar el Software en una de las siguientes maneras: (i) a través de un certificado de licencia emitido por el Proveedor o por un tercero designado por el Proveedor; (ii) a través de un acuerdo de licencia por escrito, en caso de haberse establecido dicho acuerdo; (iii) a través de la presentación de un correo electrónico enviado por el Proveedor donde se incluyan los detalles de la Licencia (nombre de usuario y contraseña). Se puede solicitar información sobre la Licencia y datos sobre el Usuario final a para llevar a cabo la verificación de la autenticidad del Software conforme a la Política de Privacidad.

18. **Licencias para autoridades públicas y el gobierno de los Estados Unidos.** Se deberá suministrar el Software a las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

## 19. Cumplimiento del control comercial.

a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras (en adelante, "Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen

i. toda ley que controle, restrinja o imponga requisitos de licencia a la exportación, reexportación o transferencia de productos, software, tecnología o servicios, establecida o adoptada por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas (en adelante, "Leyes de Control de Exportaciones") y

ii. cualquier sanción, restricción, embargo, prohibición de exportación o importación, prohibición de transferencia de fondos o activos o prohibición de prestación de servicios, ya sea de índole económica, financiera, comercial o de otro tipo, o toda medida equivalente impuesta por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas (en adelante, "Normas sancionadoras").

b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición del Artículo 19.a del Acuerdo; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme al Acuerdo podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

**20. Avisos.** Todos los avisos, la devolución del Software y la Documentación deben enviarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

**21. Legislación aplicable.** Este Acuerdo se registrará e interpretará conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo, Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

**22. Disposiciones generales.** Si alguna disposición de este Acuerdo no es válida o aplicable, no afectará la validez de las demás disposiciones del Acuerdo, que seguirán siendo válidas y ejecutables bajo las condiciones aquí estipuladas. En caso de existir diferencias entre las versiones idiomáticas de este Acuerdo, prevalecerá el texto en lengua inglesa. Las revisiones de este Acuerdo pueden realizarse únicamente por escrito y deberán estar firmadas ya sea por un representante autorizado por el Proveedor o por una persona expresamente autorizada para actuar

en su nombre según lo establezcan las disposiciones de un poder notarial.

Este es el acuerdo entero entre el proveedor y Usted relacionado con el Software y reemplaza a cualquier representación, discusión, garantía, comunicación o publicidad previa relacionadas con el Software.

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, inscrita en el Registro comercial del Tribunal de distrito de Bratislava I, Sección Sro, Registro No 3586/B, Número de registro de empresa: 31333532 como Controlador de datos (“ESET” o “Nosotros”) desea ser transparente con el procesamiento de datos personales y la privacidad de nuestros clientes. A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”) acerca de los siguientes temas:

- Procesamiento de datos personales,
- Confidencialidad de datos,
- Datos de la persona registrada.

## Procesamiento de datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del Acuerdo de licencia de usuario final (“EULA”), pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos distintos servicios descritos en el EULA y la documentación del producto, como el servicio de actualización, ESET LiveGrid®, la protección contra el mal uso de los datos, la asistencia, etc. Para hacer que todo funcione, necesitamos recolectar 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.
- Funciones hash unidireccionales relativas a infiltraciones como parte del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección frente a programas malignos comparando archivos analizados con una base de datos de elementos puestos en listas blancas y negras en la nube.
- Muestras y metadatos sospechosos de la circulación, parte del sistema de realimentación de ESET LiveGrid®, que permite a ESET reaccionar de forma inmediata ante las necesidades de sus usuarios finales y responder a las amenazas más recientes. Nosotros dependemos de que Usted nos envíe:

○ infiltraciones como muestras potenciales de virus y otros programas malignos y sospechosos; objetos problemáticos o potencialmente no deseados o inseguros, como archivos ejecutables, mensajes de correo electrónico que haya clasificado, como correo no deseado o que nuestro producto haya marcado;

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

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

• Archivos de volcado de memoria y la información que contienen.

No necesitamos recopilar datos por fuera de este ámbito. Sin embargo, en algunas ocasiones no podemos evitarlo. Los datos recopilados accidentalmente pueden incluirse como malware y Nosotros no pretendemos que sean parte de nuestros sistemas o procesarlos para el cumplimiento de los objetivos detallados en la presente Política de privacidad.

- Para fines de facturación, verificación de autenticidad de la licencia y prestación de nuestros servicios, se requiere información de licencia como identificación de licencia y datos personales, como nombre, apellido, dirección y dirección de correo electrónico.
- Pueden ser necesarios datos de contacto y datos contenidos en sus solicitudes de soporte para el servicio técnico. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, datos de licencia, detalles del producto y descripción de su caso de asistencia. Podemos solicitarle que proporcione información adicional para facilitar la prestación del servicio de soporte.

## Confidencialidad de los datos

ESET es una compañía que opera globalmente a través de entidades o socios afiliados como parte de nuestra red de distribución, servicio y soporte. Los datos procesados por ESET pueden ser transferidos desde y hasta las entidades afiliadas o socios para ejecutar EULA, como por ejemplo la prestación de servicios o soporte o facturación. Según la ubicación y servicio que Usted decida utilizar, Nosotros podemos solicitarle que transfiera sus datos a un país sin una decisión adecuada de la Comisión Europea. Incluso en tal situación, cada transferencia de datos se encuentra sujeta a la regulación de la protección de datos y se realiza solo si es necesaria. Se deben establecer cláusulas contractuales estándar, normas corporativas vinculantes u otra forma de protección adecuada sin excepción.

Nosotros 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 la validez de su licencia para que tenga tiempo de renovarla de una forma sencilla y cómoda. Pueden continuar procesándose estadísticas y otros datos minimizados y seudonimizados de ESET LiveGrid® con fines estadísticos.

ESET implementa medidas técnicas y de organización para asegurar un nivel de seguridad apropiado ante riesgos potenciales. Hacemos todo lo posible para garantizar una continua confiabilidad, integridad, disponibilidad y capacidad de recuperación de los sistemas operativos y servicios. Sin embargo, si ocurre una filtración de datos que resulta en un riesgo para sus derechos y libertades, Nosotros estamos preparados para notificar a la autoridad supervisora así como también a las personas registradas. Como persona registrada, Usted tiene el derecho de presentar una queja con una autoridad supervisora.

## Derechos de la persona registrada

ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. De conformidad con las condiciones establecidas por las leyes aplicables de protección de los datos, usted tiene los siguientes derechos como sujeto de datos:

- derecho a que ESET le solicite acceso a sus datos personales,
- derecho a rectificación de datos personales de ser erróneos (Usted también tiene el derecho a completar los datos personales que estén incompletos),

- derecho a solicitar la eliminación de sus datos personales,
- derecho a solicitar una restricción al procesamiento de sus datos personales
- derecho a oponerse al procesamiento
- derecho a presentar un reclamo así como
- derecho a la portabilidad de datos.

Si desea ejercer su derecho como persona registrada o tiene una consulta o preocupación, envíenos un mensaje a:

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