ESET Endpoint Security for macOS

Manual de usuario

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

ESET Endpoint Security for macOS está desarrollado por ESET, spol. s r.o.

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

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

REV. 17/03/2023

ESET Endpoint Security for macOS

ESET Endpoint Security for macOS 6 representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense®, combinada con nuestro cortafuegos personalizado, emplea la velocidad y la precisión para mantener su ordenador seguro. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que podrían amenazar su ordenador.

ESET Endpoint Security for macOS 6 es una solución de seguridad integral desarrollada tras un gran esfuerzo por combinar el nivel máximo de protección con un impacto mínimo en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial son capaces de eliminar proactivamente la infiltración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques que albergan en Internet sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

El producto está diseñado principalmente para su uso en estaciones de trabajo en empresas grandes o pequeñas. Se puede utilizar con ESET PROTECT (conocido anteriormente como ESET Security Management Center), de forma que puede administrar fácilmente cualquier número de estaciones de trabajo cliente, aplicar políticas y reglas, controlar detecciones y administrar de manera remota modificaciones en cualquier ordenador de la red.

Novedades de la versión 6

La interfaz gráfica de usuario de ESET Endpoint Security for macOS presenta un diseño totalmente nuevo que mejora la visibilidad y ofrece una experiencia de usuario más intuitiva. A continuación se indican algunas de las muchas mejoras que incluye la versión 6:

- Compatibilidad con ESET Enterprise Inspector: desde la versión 6.9 de ESET Endpoint Security for macOS, ESET Endpoint Security for macOS se puede conectar con ESET Enterprise Inspector. ESET Enterprise Inspector (EEI) es un completo sistema de detección y respuesta para puntos de conexión que incluye funciones como las siguientes: detección de incidentes, administración de incidentes y respuesta, recopilación de datos, indicadores de detección de riesgo, detección de anomalías, detección de comportamientos e incumplimientos de políticas. Para obtener más información sobre ESET Enterprise Inspector, su instalación y sus funciones, consulte la ayuda de ESET Enterprise Inspector.

- **Compatibilidad con arquitecturas de 64 bits**.

- **Cortafuegos**: ahora puede crear reglas de cortafuegos directamente desde la ventana de registro o notificación de IDS (Intrusion detection system), y asignar perfiles a las interfaces de red.

- **Control web**: le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo o inadecuado.

- **Protección del acceso a la Web**: supervisa la comunicación entre los navegadores web y los servidores remotos.

- **Protección del correo electrónico**: proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP.

- **Protección Anti-Phishing**: le protege frente a intentos de obtener contraseñas y otra información

confidencial; para ello, restringe el acceso a sitios web maliciosos que suplantan a sitios legítimos.

- **Control de dispositivos**: le permite analizar, bloquear o ajustar los filtros o permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo determinado y trabajar en él. Esta función está disponible en la versión 6.1 del producto y en versiones posteriores.

- **Modo presentación**: esta opción le permite ejecutar ESET Endpoint Security for macOS en segundo plano y suprime las ventanas emergentes y las tareas planificadas.

- **Caché local compartida**: permite lograr mejoras en la velocidad de análisis en entornos virtualizados.

Requisitos del sistema

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

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

Además de la compatibilidad con Intel existente, las versiones 6.10.900.0 y posteriores de ESET Endpoint Security for macOS admiten el chip Apple ARM con Rosetta 2.

Introducción a ESET PROTECT

ESET PROTECT le permite administrar los productos de ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central.

Con ESET PROTECT Web Console, puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas en ordenadores remotos. Consulte también la visión general de los elementos de la infraestructura y la arquitectura de ESET PROTECT, la Introducción a ESET PROTECT Web Console y los Entornos de aprovisionamiento de escritorios compatibles.

ESET PROTECT lo conforman los siguientes componentes:

- ESET PROTECT Server: ESET PROTECT Server se puede instalar en servidores Windows y Linux, y también está disponible como dispositivo virtual. Se ocupa de la comunicación con los agentes, y recopila y almacena datos de aplicaciones en la base de datos.

- ESET PROTECT Consola Web: ESET PROTECT es la interfaz principal que le permite administrar ordenadores cliente en su entorno. Muestra información general del estado de los clientes en la red y le permite implementar de forma remota soluciones de ESET en ordenadores no administrados. Tras instalar ESET PROTECT Server (Server), puede acceder a la consola web a través del navegador web. Si configura el servidor

web para que esté disponible desde Internet, puede utilizar ESET PROTECT desde prácticamente cualquier lugar o dispositivo con conexión a Internet.

- ESET Management Agent: ESET Management Agent facilita la comunicación entre ESET PROTECT Server y los ordenadores cliente. El agente debe instalarse en el ordenador cliente para establecer comunicación entre ese ordenador y ESET PROTECT Server. Como está en el ordenador cliente y puede almacenar varios contextos de seguridad, el uso de ESET Management Agent reduce considerablemente el tiempo de reacción a las nuevas detecciones. Con ESET PROTECT Web Console puede implementar ESET Management Agent en los ordenadores no administrados que identifica Active Directory o el Sensor de RD de ESET. También puede instalar de forma manual ESET Management Agent en los ordenadores cliente en caso de que sea necesario.

- Rogue Detection Sensor: ESET PROTECT Rogue Detection (RD) Sensor detecta los ordenadores no administrados presentes en su red y envía su información a ESET PROTECT Server. Esto le permite agregar fácilmente nuevos ordenadores cliente a su red protegida. El Sensor de RD recuerda los ordenadores que se han detectado y no envía la misma información dos veces.

- Proxy HTTP Apache: es un servicio que puede usarse en combinación con ESET PROTECT para:

  - Distribuir actualizaciones entre los ordenadores cliente y paquetes de instalación a ESET Management Agent.

  - Reenviar la comunicación de las instancias de ESET Management Agent a ESET PROTECT Server.

- Conector del dispositivo móvil: es un componente que permite la administración de dispositivos móviles con ESET PROTECT, gracias a la que puede administrar dispositivos móviles (Android e iOS) y ESET Endpoint Security para Android.

- Dispositivo virtual de ESET PROTECT: el dispositivo virtual de ESET PROTECT está pensado para aquellos usuarios que quieren ejecutar ESET PROTECT en un entorno virtualizado.

- Host del agente virtual de ESET PROTECT: un componente de ESET PROTECT que virtualiza entidades de agente para poder administrar máquinas virtuales sin agentes. Esta solución activa la automatización, la utilización de grupos dinámicos y el mismo nivel de administración de tareas de ESET Management Agent en los ordenadores físicos. El agente virtual recopila información de las máquinas virtuales y la envía a ESET PROTECT Server.

- Herramienta Mirror: la herramienta Mirror es necesaria para las actualizaciones de módulos sin conexión. Si los ordenadores cliente no tienen conexión a Internet, puede utilizar la herramienta Mirror para descargar archivos de actualización de servidores de actualizaciones de ESET y almacenarlos localmente.

- ESET Remote Deployment Tool: esta herramienta le permite implementar paquetes todo en uno creados en <%PRODUCT%> Consola Web. Permite distribuir con facilidad ESET Management Agent con un producto de ESET por los ordenadores de una red.

- ESET Business Account: el nuevo portal de licencias de productos empresariales de ESET le permite administrar las licencias. Consulte la sección ESET Business Account de este documento para obtener las instrucciones de activación del producto, o consulte la Guía del usuario de ESET Business Account para obtener más información sobre el uso de ESET Business Account. Si ya dispone de un nombre de usuario y una contraseña emitidos por ESET y desea convertirlos en una clave de licencia, consulte la sección Convertir credenciales de licencia heredada.

- ESET Enterprise Inspector: un completo sistema Endpoint de detección y respuesta que incluye funciones como las siguientes: detección de incidentes, administración de incidentes y respuesta, recopilación de datos,

indicadores de detección de riesgo, detección de anomalías, detección de comportamientos e incumplimientos de políticas.

Con ESET PROTECT Web Console puede implementar soluciones ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas en ordenadores remotos.

Para obtener más información, consulte la guía del usuario de ESET PROTECT en línea.

Introducción a ESET PROTECT CLOUD

ESET PROTECT CLOUD le permite administrar los productos de ESET en estaciones de trabajo y servidores en un entorno de red desde una ubicación central sin necesidad de tener un servidor físico o virtual como para ESET PROTECT oESET Security Management Center. Con (ESET PROTECT CLOUD Consola Web), podrá implementar soluciones de ESET, administrar tareas, aplicar políticas de seguridad, supervisar el estado del sistema y responder rápidamente a problemas o amenazas que se produzcan en ordenadores remotos.

- Lea más acerca de esto en la guía del usuario de ESET PROTECT CLOUD en línea

Instalación remota

Antes de la instalación

macOS 10.15 y versiones anteriores

Antes de instalar ESET Endpoint Security for macOS en macOS 10.13 y versiones posteriores, permita las extensiones del kernel de ESET y que, en macOS 10.14 y versiones posteriores, también permita acceso de disco completo en los ordenadores de destino. Si se permiten estas opciones tras la instalación, los usuarios recibirán las notificaciones **Extensiones del sistema bloqueadas** y **Su ordenador está protegido parcialmente** hasta que se permitan las extensiones del kernel de ESET y el acceso total al disco.

Para permitir las extensiones del kernel de ESET y el Acceso total al disco de manera remota, tendrá que inscribir su ordenador en un servidor de MDM (Administración de dispositivos móviles), como Jamf.

Permitir las extensiones del sistema de ESET

Para permitir las extensiones del kernel en su dispositivo de forma remota:

- Si está utilizando Jamf como MDM, consulte el artículo de la base de conocimiento relacionado.

- Si utiliza un MDM distinto, descargue el perfil de configuración .plist. Genere dos UUID con el generador de UUID que prefiera y utilice un editor de texto para sustituir las cadenas de texto `insert your UUID 1 here` e `insert your UUID 2 here` en el perfil de configuración descargado. Implemente el archivo del perfil de configuración .plist con el servidor MDM. Tendrá que inscribir su ordenador en el servidor MDM para poder implementar perfiles de configuración en estos ordenadores.

Permitir acceso total al disco

En macOS 10.14, recibirá la notificación **Su ordenador está parcialmente protegido** de ESET Endpoint Security for

macOS tras la instalación. Para acceder a todas las funciones de ESET Endpoint Security for macOS e impedir que aparezca la notificación, tendrá que permitir **Acceso total al disco** a ESET Endpoint Security for macOS antes de la instalación del producto. Para permitir **Acceso total al disco** de forma remota:

- Si está utilizando Jamf como MDM, consulte el artículo de la base de conocimiento relacionado.
- Para permitir **Acceso total al disco** de forma remota, descargue el archivo de configuración .plist. Genere dos UUID con el generador de UUID que prefiera y utilice un editor de texto para sustituir las cadenas de texto `insert your UUID 1 here` e `insert your UUID 2 here` en el perfil de configuración descargado. Descargue el archivo del perfil de configuración .plist con el servidor MDM. Tendrá que inscribir su ordenador en el servidor MDM para poder implementar perfiles de configuración en estos ordenadores.

macOS Big Sur (11)

Antes de instalar ESET Endpoint Security for macOS en macOS Big Sur debe permitir permita las extensiones del sistema de ESET y Acceso total al disco en los ordenadores de destino. Si se permiten estas opciones tras la instalación, los usuarios recibirán las notificaciones **Extensiones del sistema bloqueadas** y **Su ordenador está protegido parcialmente** hasta que se permitan las extensiones del sistema de ESET y el Acceso total al disco. Las extensiones del sistema solo pueden permitirse de forma remota antes de la instalación de ESET Endpoint Security for macOS.

Para permitir las extensiones del sistema de ESET y el Acceso total al disco de manera remota, tendrá que inscribir su ordenador en un servidor de MDM (Administración de dispositivos móviles), como Jamf.

Permitir las extensiones del sistema de ESET

Para permitir las extensiones del sistema en su dispositivo de forma remota:

- Si está utilizando Jamf como MDM, consulte el artículo de la base de conocimiento relacionado.
- Si está usando un MDM distinto, descargue el perfil de configuración .plist. Implemente el archivo de perfil de configuración .plist con el servidor MDM. Su ordenador debe estar inscrito en el servidor MDM para implementar perfiles de configuración en dichos ordenadores. Para crear su propio perfil de configuración, utilice los ajustes siguientes:

Identificador del equipo (TeamID)	`P8DQRXPVLP`

Identificador del paquete (BundleID)	`com.eset.endpoint`
	`com.eset.network`
	`com.eset.firewall`
	`com.eset.devices`

Permitir acceso total al disco

Para permitir el **Acceso total al disco** de forma remota:

- Si está utilizando Jamf como MDM, consulte el artículo de la base de conocimiento relacionado.
- Para permitir **Acceso total al disco** de forma remota, descargue el archivo de configuración .plist. Implemente el archivo de perfil de configuración .plist con el servidor MDM. Su ordenador debe estar inscrito en el servidor MDM para poder implementar perfiles de configuración en dichos ordenadores. Para crear su propio perfil de configuración, utilice los ajustes siguientes:

ESET Endpoint Security	
Identificador	com.eset.ees.6
Tipo de identificador	bundleID
Requisito del código	identifier "com.eset.ees.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplicación o servicio	SystemPolicyAllFiles
Acceder	Allow

ESET Endpoint Antivirus y ESET Endpoint Security	
Identificador	com.eset.devices
Tipo de identificador	bundleID
Requisito del código	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplicación o servicio	SystemPolicyAllFiles
Acceder	Allow

ESET Endpoint Antivirus y ESET Endpoint Security	
Identificador	com.eset.endpoint
Tipo de identificador	bundleID
Requisito del código	identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplicación o servicio	SystemPolicyAllFiles
Acceder	Allow

Instalación

Antes de la instalación puede crear un paquete de instalación remota con una configuración de ESET Endpoint Security for macOS preestablecida que posteriormente podrá implementar mediante ESET PROTECT o el servidor MDM que elija.

- Cree un paquete de instalación remota.

Instale ESET Endpoint Security for macOS de forma remota mediante la creación de una **Tarea de instalación del software** en el sistema de administración de ESET:

- Tarea de instalación del software ESET PROTECT
- Tarea de instalación del software ESET Security Management Center

Tras la instalación

Los usuarios recibirán la siguiente notificación: **"**ESET Endpoint Security for macOS**" desea filtrar contenido de red**. Cuando los usuarios reciban esta notificación, haga clic en **Permitir**. Si hace clic en **No permitir**, la Protección de acceso a la web no funcionará.

Creación de un paquete de instalación remota

Creación de un paquete de instalación para la instalación de Apple Remote Desktop

1. Descargue el paquete de instalación estándar del sitio web de ESET:
ESET Endpoint Security for macOS

2. Para iniciar el instalador de ESET Endpoint Security for macOS, haga doble clic en el archivo descargado.

1. Haga clic en **Instalar**ESET Endpoint Security for macOS.

2. Cuando se le indique, haga clic en **Permitir** para autorizar al instalador a determinar si se puede instalar el software.

3. Haga clic en **Continuar.** Si está creando un paquete de instalación remota, ESET Endpoint Security for macOS no se instalará.

4. Revise los requisitos del sistema y haga clic en **Continuar**.

5. Lea el acuerdo de licencia del software de ESET y haga clic en **Continuar** → **Aceptar** si está de acuerdo.

6. En el paso **Modo de instalación**, seleccione **Remoto**.

7. Elija qué componentes del producto desea instalar. Todos los componentes vienen seleccionados de forma predeterminada. Haga clic en **Continuar**.

8. En el paso **Servidor proxy**, seleccione la opción que coincida con su conexión a Internet. Si no está seguro, utilice la configuración predeterminada del sistema. Haga clic en **Siguiente**. Si está utilizando un servidor proxy, en el siguiente paso se le pedirá que introduzca la dirección del proxy, su nombre de usuario y la contraseña.

9. Seleccione quién puede modificar la configuración del programa. Solo los usuarios y grupos con privilegios pueden modificarla. Al grupo de administradores se le conceden los privilegios de forma predeterminada. Active la casilla **Mostrar todos los usuarios** o **Mostrar todos los grupos** para mostrar todos los usuarios y grupos virtuales, como programas y procesos.

10. Active ESET LiveGrid en el ordenador de destino, si corresponde.

11. Active la detección de aplicaciones potencialmente indeseables en el ordenador de destino, si corresponde.

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

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

13. Guarde el archivo de instalación en el ordenador. Si ya creó anteriormente un archivo de instalación en la ubicación predeterminada, debe cambiar la ubicación de la carpeta de destino o eliminar los archivos anteriores para poder continuar. Con esta acción, se finaliza la primera fase de la instalación remota. El instalador local se cierra y crea archivos de instalación remota en la carpeta de destino que ha seleccionado.

Los archivos de instalación remota son los siguientes:

- *esets_setup.dat*: datos de configuración que ha introducido en la sección de configuración del instalador

- *program_components.dat*: información de configuración de los componentes del programa seleccionados (este archivo es opcional; se crea cuando elige no instalar determinados componentes de ESET Endpoint Security for macOS)

- *esets_remote_install.pkg*: paquete de instalación remota

- *esets_remote_uninstall.sh*: script de desinstalación remota

Instalación de Apple Remote Desktop

1. Abra Apple Remote Desktop y conéctese al ordenador de destino. Para obtener más información, consulte la documentación de Apple Remote Desktop.

2. Copie los siguientes archivos con la opción de **copiar archivo o carpeta** de Apple Remote Desktop en la carpeta */tmp* del ordenador de destino:

Si va a instalar todos los componentes, copie:
- *esets_setup.dat*

Si no va a instalar todos los componentes del producto, copie:
- *esets_setup.dat*
- *product_components.dat*

3. Utilice el comando **Instalar paquetes** para instalar *esets_remote_install.pkg* en el ordenador de destino.

Desinstalación remota de Apple Remote Desktop

1. Abra Apple Remote Desktop y conéctese al ordenador de destino. Para obtener más información, consulte la documentación de Apple Remote Desktop.

2. Copie el script *esets_remote_uninstall.sh* con la opción de **copiar archivo o carpeta** de Apple Remote Desktop en la carpeta */tmp* del ordenador de destino.

3. En Apple Remote Desktop, utilice la opción **Enviar comando UNIX** al ordenador de destino:

```
/tmp/esets_remote_uninstall.sh
```

Una vez que finalice el proceso de desinstalación, la consola aparece en Apple Remote Desktop en el ordenador de destino.

Instalación

El Asistente de instalación le guiará por el proceso de configuración básico. Para obtener una guía detallada, visite el artículo de la base de conocimiento sobre instalación..

1. Para iniciar el instalador de ESET Endpoint Security for macOS, haga doble clic en el archivo descargado.

1. Para iniciar la instalación, haga clic en **Instalar** ESET Endpoint Security for macOS.

Instalación desde el archivo .pkg

Durante la instalación y el inicio de sus productos ESET para macOS, es necesario que tenga conexión a Internet en su Mac para que Apple pueda verificar la notarización de las extensiones del sistema de ESET.

2. Cuando se le indique, haga clic en **Permitir** para autorizar al instalador a determinar si se puede instalar el software.

3. Elimine las aplicaciones de seguridad existentes, como antivirus, antiespía o cortafuegos de su ordenador, si aún no lo ha hecho. Haga clic en **Continuar** si no hay ninguna otra aplicación de seguridad instalada.

4. Revise los requisitos del sistema y haga clic en **Continuar**.

5. Lea el acuerdo de licencia del software de ESET y haga clic en **Continuar** → **Aceptar** si está de acuerdo.

6. Seleccione el tipo de instalación correspondiente.

- Instalación típica
- Instalación personalizada
- Instalación remota

Actualización de versión

En la fase inicial, el instalador comprueba automáticamente la existencia de una versión del producto más reciente en Internet. Si la encuentra, se le ofrecerá la opción de descargar la versión más reciente antes de proceder con la instalación.

Instalación típica

El modo de instalación típica incluye opciones de configuración que son adecuadas para la mayoría de los usuarios. Esta configuración proporciona una seguridad máxima junto con un excelente rendimiento del sistema. La instalación típica es la opción predeterminada y se recomienda cuando no es necesaria una configuración específica.

1. En la ventana de **ESET LiveGrid**, seleccione la opción que desee y haga clic en **Continuar**. Si más adelante decide que desea cambiar esta configuración, podrá hacerlo mediante la **Configuración de LiveGrid**. Si desea obtener más información sobre ESET LiveGrid, visite nuestro glosario.
2. En la ventana **Aplicaciones potencialmente indeseables**, seleccione la opción que prefiera (consulte ¿Qué es una aplicación potencialmente indeseable?) y haga clic en **Continuar**. Si más adelante decide que desea cambiar esta configuración, utilice **Configuración avanzada**.

3. Haga clic en **Instalar**. Si se le solicita que introduzca la contraseña de macOS, introdúzcala y haga clic en **Instalar software**.

Tras la instalación de ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. Permita las extensiones del sistema.

2. Permitir acceso total al disco.

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

macOS 10.15 y versiones anteriores

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

2. En macOS 10.14 y posteriores recibirá la notificación **Su ordenador está protegido parcialmente** de ESET Endpoint Security for macOS. Para acceder a todas las funciones de ESET Endpoint Security for macOS, tendrá que permitir **Acceso total al disco** a ESET Endpoint Security for macOS. Haga clic en **Abrir Preferencias del Sistema** > **Seguridad y privacidad**. Diríjase a la ficha **Privacidad** y marque la opción **Acceso total al disco**. Haga clic en el icono para activar la edición. Haga clic en el signo más y seleccione la aplicación ESET Endpoint Security for macOS. Su ordenador mostrará una notificación de reinicio del ordenador. Haga clic en **Más tarde**. No reinicie el ordenador ahora. Haga clic en **Iniciar de nuevo** en la ventana de notificación de ESET Endpoint Security for macOS o reinicie el ordenador. Para obtener información más detallada, visite este artículo de la Base de conocimiento.

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

Instalación personalizada

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

- **Componentes del programa**
  ESET Endpoint Security for macOS le permite instalar el producto sin alguno de los componentes básicos (por ejemplo, la protección de la web y el correo electrónico). Desactive la casilla de verificación situada junto al componente del producto que desee no incluir en la instalación.

- **Servidor Proxy**
  Si utiliza un servidor proxy, seleccione **Uso un servidor proxy** para definir sus parámetros. En la ventana siguiente, introduzca la dirección IP o la URL de su servidor proxy en el campo **Dirección**. En el campo **Puerto**, especifique el puerto en el que el servidor Proxy acepte conexiones (el 3128, de forma predeterminada). En el caso de que el servidor proxy requiera autenticación, debe introducir un **nombre de usuario** y una **contraseña** válidos para poder acceder al servidor proxy. Si no utiliza un servidor proxy, seleccione **No se utiliza un servidor proxy**. Si no está seguro de si usa un servidor proxy o no, seleccione **Utilizar configuración del sistema (Recomendado)** para utilizar la configuración actual del sistema.

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

- **ESET LiveGrid®**
  Si desea obtener más información sobre ESET LiveGrid, visite nuestro glosario.

- **Aplicaciones potencialmente indeseables**
  Si desea obtener más información sobre las aplicaciones potencialmente indeseables, visite nuestro glosario.

- **Cortafuegos**
  Elija el modo de filtrado del cortafuegos. Para obtener más información, consulte Modos de filtrado.

Tras la instalación de ESET Endpoint Security for macOS:

macOS Big Sur (11)

1. Permita las extensiones del sistema.

2. Permitir acceso total al disco.

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

macOS 10.15 y versiones anteriores

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

2. En macOS 10.14 y posteriores recibirá la notificación **Su ordenador está protegido parcialmente** de ESET Endpoint Security for macOS. Para acceder a todas las funciones de ESET Endpoint Security for macOS, tendrá que permitir **Acceso total al disco** a ESET Endpoint Security for macOS. Haga clic en **Abrir Preferencias del Sistema** > **Seguridad y privacidad**. Diríjase a la ficha **Privacidad** y marque la opción **Acceso total al disco**. Haga clic en el icono para activar la edición. Haga clic en el signo más y seleccione la aplicación ESET Endpoint Security for macOS. Su ordenador mostrará una notificación de reinicio del ordenador. Haga clic en **Más tarde**. No reinicie el ordenador ahora. Haga clic en **Iniciar de nuevo** en la ventana de notificación de ESET Endpoint Security for macOS o reinicie el ordenador. Para obtener información más detallada, visite este artículo de la Base de conocimiento.

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

Permitir las extensiones del sistema localmente

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

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

Actualice de la versión anterior de macOS a Big Sur.

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

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

Permitir las extensiones del sistema de forma manual

1. Haga clic en **Abrir Preferencias del Sistema** o **Abrir Preferencias de seguridad** en uno de los cuadros de diálogo de alerta.

2. Haga clic en el icono del candado situado en la parte inferior izquierda para permitir cambios en la ventana de configuración.

3. Utilice su Touch ID o haga clic en **Usar contraseña**, escriba su nombre de usuario y contraseña y, a continuación, haga clic en **Desbloquear**.

4. Haga clic en **Detalles**.

5. Seleccione las tres opciones de ESET Endpoint Security for macOS**.app**.

6. Haga clic en **Aceptar**.

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

Permitir acceso total al disco localmente

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

1. Haga clic en **Abrir Preferencias del Sistema** en la ventana del cuadro de diálogo de alerta.

2. Haga clic en el icono del candado situado en la parte inferior izquierda para permitir cambios en la ventana de configuración.

3. Utilice su Touch ID o haga clic en **Usar contraseña**, escriba su nombre de usuario y contraseña y, a continuación, haga clic en **Desbloquear**.

4. Seleccione ESET Endpoint Security for macOS**.app** en la lista.

5. Se mostrará una notificación de reinicio de ESET Endpoint Security for macOS. Haga clic en Ms tarde.

6. Seleccione **Protección del sistema de archivos en tiempo real** de ESET en la lista.

> **No está presente la opción Protección del sistema de archivos en tiempo real de ESET**
> Si la opción de **Protección del sistema de archivos en tiempo real** no está en la lista, tiene que permitir las extensiones del sistema para su producto de ESET.

7. Haga clic en Iniciar de nuevo en la ventana del cuadro de diálogo de la alerta de ESET Endpoint Security for macOS o reinicie el ordenador. Para obtener información más detallada, consulte el artículo de nuestra base de conocimiento.

Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto. Se pueden usar varios métodos de activación. La disponibilidad de un método de activación determinado puede variar en función del país, además de los medios de distribución (CD/DVD, página web de ESET, etc.) del producto.

Si desea activar su copia de ESET Endpoint Security for macOS directamente desde el programa, haga clic en el icono de ESET Endpoint Security for macOS situado en la barra de menús de macOS (parte superior de la pantalla) y haga clic en **Activación del producto**. El producto también se puede activar desde el menú principal, en **Ayuda** > **Administrar licencia** o **Estado de protección** > **Activar producto**.

Puede utilizar cualquiera de estos métodos para activar ESET Endpoint Security for macOS:

- **Activar con clave de licencia**: es una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y que se usa para identificar al propietario de la licencia y para activar la misma. La clave de licencia está en el correo electrónico recibido al comprar el producto, o en la tarjeta de licencia incluida en la caja.

- **Administrador de seguridad**: es una cuenta creada en el portal de ESET License Administrator con credenciales (dirección de correo electrónico y contraseña). Este método le permite gestionar varias licencias desde una ubicación.

- **Licencia sin conexión**: se trata de un archivo generado automáticamente que se transferirá al producto de ESET para proporcionar información sobre la licencia. El archivo de licencia sin conexión se genera en el portal de ESET License Administrator y se utiliza en aquellos entornos en los que la aplicación no se puede conectar a la autoridad de concesión de licencias.

También puede activar este cliente más tarde, si su ordenador es miembro de una red gestionada y el administrador tiene previsto utilizar ESET Remote Administrator para activar el producto.

> **Activación silenciosa**
> ESET Remote Administrator puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador.

ESET Endpoint Security for macOS versión 6.3.85.0 (o posterior) le ofrece la opción de activar el producto con Terminal. Para hacer esto, emita el siguiente comando:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Sustituya `XXXX-XXXX-XXXX-XXXX-XXXX` por una clave de licencia que ya se haya utilizado para la activación de ESET Endpoint Security for macOS o registrado en el ESET License Administrator. El comando devolverá el estado "OK" o un error si se produce un error en la activación.

Desinstalación

Hay varias formas de iniciar el programa de desinstalación de ESET Endpoint Security for macOS:

- Abra el archivo de instalación de ESET Endpoint Security for macOS (*.dmg*) y haga doble clic en **Desinstalar**
- Inicie **Finder**, abra la carpeta **Aplicaciones** de la unidad de disco duro, pulse Ctrl y haga clic en el icono de **ESET Endpoint Security for macOS** y seleccione la opción **Mostrar contenido del paquete**. Abra la carpeta **Contents** > **Helpers** y haga doble clic en el icono **Uninstaller**.

> **Desinstalación**
> Durante el proceso de desinstalación, tendrá que introducir la contraseña de administrador varias veces para desinstalar por completo ESET Endpoint Security for macOS.

Información general básica

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

Desde el menú principal se puede acceder a los siguientes apartados:

- **Estado de protección** – contiene información sobre el estado de protección del ordenador, la web y el correo electrónico y del cortafuegos.
- **Análisis del ordenador**: este apartado le permite configurar e iniciar el análisis del ordenador a petición.
- **Actualización**: muestra información sobre actualizaciones de los módulos.
- **Configuración**: seleccione esta opción para ajustar el nivel de seguridad del ordenador.
- **Herramientas**: proporciona acceso a Archivos de registro, Planificador de tareas, Cuarentena, Procesos en

ejecución y otras características del programa.

- **Ayuda**: proporciona acceso a los archivos de ayuda, la base de conocimientos en Internet, el formulario de solicitud del servicio de atención al cliente e información adicional del programa.

Accesos directos del teclado

ESET Endpoint Security for macOS es compatible con los siguientes accesos directos del teclado:

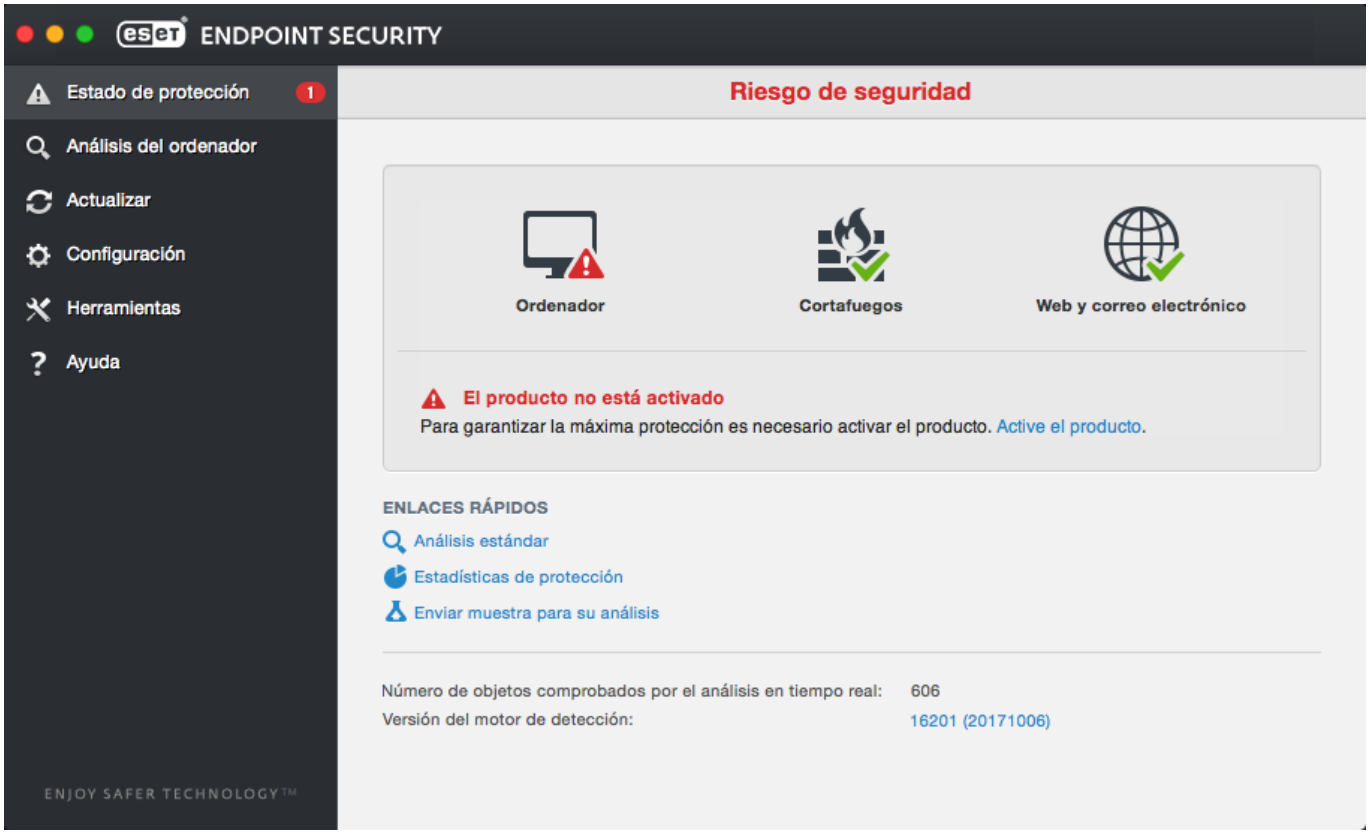
- *cmd+,*: muestra las preferencias de ESET Endpoint Security for macOS.
- *cmd+O*: restaura el tamaño predeterminado de la ventana principal de la GUI de ESET Endpoint Security for macOS y la mueve al centro de la pantalla.
- *cmd+Q*: oculta la ventana principal de la GUI de ESET Endpoint Security for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

Los siguientes accesos directos del teclado solo funcionan si está activada la opción **Utilizar menú estándar** en **Configuración** > **Introducir preferencias de aplicación...** > **Interfaz**:

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

Comprobación del funcionamiento del sistema

Para consultar el estado de la protección, haga clic en **Estado de la protección** en el menú principal. En la ventana principal se mostrará un resumen del estado de funcionamiento de los módulos de ESET Endpoint Security for macOS.



Qué hacer si el programa no funciona correctamente

Cuando un módulo funciona correctamente presenta un icono de marca de verificación verde. Cuando un módulo no funciona correctamente se muestra un signo de exclamación rojo o un icono de notificación naranja. En la ventana principal del programa también se muestra información adicional acerca del módulo y una sugerencia para resolver el problema. Para cambiar el estado de cada módulo, haga clic en el vínculo azul disponible debajo de cada mensaje de notificación.

Si no consigue solucionar el problema con estas sugerencias, puede buscar una solución en la base de conocimiento de ESET o ponerse en contacto con el Servicio de atención al cliente de ESET. El Servicio de atención al cliente responderá a sus preguntas rápidamente y le ayudará a resolver su problema con ESET Endpoint Security for macOS.

Protección del ordenador

Puede consultar la configuración del ordenador en **Configuración** > **Ordenador**. Muestra el estado de la **Protección del sistema de archivos en tiempo real**. Para desactivar módulos individuales, establezca el módulo deseado en **DESACTIVADO**. Tenga en cuenta que esto puede disminuir el nivel de protección del ordenador. Para acceder a la configuración detallada de cada módulo, haga clic en **Configuración**.

Protección antivirus y antispyware

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

General

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

- **Aplicaciones potencialmente indeseables**: estas aplicaciones no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de manera negativa. Dichas aplicaciones suelen necesitar que se consienta su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontrase antes de la instalación). Entre los cambios más significativos, destacan las ventanas emergentes no deseadas, la activación y ejecución de procesos ocultos, el aumento del uso de los recursos del sistema, los cambios en los resultados de búsqueda y las aplicaciones que se comunican con servidores remotos.

- **Aplicaciones potencialmente peligrosas**: estas aplicaciones son software comercial y legítimo que podría ser utilizado por atacantes si se instala sin consentimiento del usuario. En esta clasificación se incluyen programas como, por ejemplo, las herramientas de acceso remoto, de ahí que esta opción esté desactivada de forma predeterminada.

- **Aplicaciones sospechosas**: estas aplicaciones incluyen programas comprimidos con empaquetadores o protectores. Los autores de código malicioso suelen aprovechar estos tipos de protectores para evitar que se detecte. Los empaquetadores son ejecutables de autoextracción en tiempo real que incluyen varios tipos de código malicioso en un solo paquete. Los empaquetadores más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo código malicioso se puede detectar de diferente manera cuando se comprime con un empaquetador diferente. Los empaquetadores también tienen la capacidad de hacer que sus "firmas" muten con el tiempo, dificultando su detección y eliminación.

Para configurar Las exclusiones del sistema de archivos, web y correo electrónico, haga clic en **Configuración**.

Exclusiones

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

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

- **Ruta**: ruta hacia los archivos y carpetas excluidos.

- **Amenaza**: si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha amenaza, pero no por completo. Si más adelante este archivo se infecta con otro código malicioso, el módulo antivirus lo detectará.

-  : crea una exclusión nueva. Introduzca la ruta de un objeto (también puede utilizar los comodines *y ?) o seleccione la carpeta o el archivo en la estructura de árbol.

-  : elimina las entradas seleccionadas.

- **Predeterminado**: recupera el último estado guardado de las exclusiones.

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

Protección de inicio

La verificación de archivos en el inicio analiza los archivos automáticamente al iniciar el sistema. De forma predeterminada, este análisis se ejecuta periódicamente como tarea planificada después del inicio de sesión del usuario o de una actualización correcta de los módulos. Para modificar la configuración de los parámetros del motor de ThreatSense aplicables al análisis del inicio, haga clic en **Configuración**. Encontrará más información sobre la configuración del motor ThreatSense en este apartado.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y activa un análisis en función de varios sucesos. Cuando se utiliza la tecnología ThreatSense (descrita en Configuración de parámetros del motor ThreatSense), la protección del sistema de archivos en tiempo real puede ser diferente para los archivos recién creados y los archivos existentes. Los archivos recién creados pueden controlarse con un nivel de detalle superior.

De forma predeterminada, todos los archivos se analizan cuando se **abren**, **crean** o **ejecutan**. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador. La protección en tiempo real comienza cuando se inicia el sistema y proporciona un análisis ininterrumpido. En algunos casos especiales (por ejemplo, en caso de conflicto con otro programa de análisis en tiempo real), la protección en tiempo real se puede desactivar. Para desactivarla, haga clic en el icono de ESET Endpoint Security for macOS, situado en la barra de menús (parte superior de la pantalla) y, a continuación, seleccione **Desactivar la protección del sistema de archivos en tiempo real**. La protección en tiempo real también se puede desactivar en la ventana principal del programa (haga clic en **Configuración** > **Ordenador** y establezca **Protección del sistema de archivos en tiempo real** en **DESACTIVADO**).

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

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

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

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

Opciones avanzadas

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

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

Parámetros adicionales de ThreatSense para los archivos ejecutados: de forma predeterminada, la **heurística avanzada** no se utiliza cuando se ejecutan archivos. Se recomienda encarecidamente mantener activadas las opciones Optimización inteligente y ESET LiveGrid® con el fin de mitigar su repercusión en el rendimiento del sistema.

Aumentar compatibilidad con volúmenes de red: esta opción potencia el rendimiento al acceder a los archivos a través de la red. Debe habilitarse si sufre ralentización al acceder a las unidades de red. Esta función utiliza el coordinador de archivos del sistema en OS X 10.10 y versiones posteriores. Tenga en cuenta que no todas las aplicaciones son compatibles con el coordinador de archivos; por ejemplo, Microsoft Word 2011 no es compatible, pero Word 2016 sí.

Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más importante para mantener un sistema seguro. Tenga cuidado cuando modifique los parámetros de protección en tiempo real. Es aconsejable que los modifique únicamente en casos concretos. Por ejemplo, si se produce un conflicto con una aplicación determinada o durante el análisis en tiempo real de otro programa antivirus.

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

Comprobación de la protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, utilice el archivo de prueba de eicar.com. Se trata de un archivo inofensivo especial detectable por todos los programas antivirus. El archivo fue creado por el instituto EICAR (European Institute for Computer Antivirus Research, Instituto europeo para la investigación de antivirus de ordenador) para comprobar la funcionalidad de los programas antivirus.

Para comprobar el estado de la protección en tiempo real sin recurrir a ESET Security Management Center, conéctese al ordenador cliente de forma remota con **Terminal** y emita el comando siguiente:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

El estado del análisis en tiempo real se mostrará como `RTPStatus=Enabled` o `RTPStatus=Disabled`.

El resultado del comando bash de Terminal también incluye estos estados:

- versión de ESET Endpoint Security for macOS instalada en el ordenador cliente
- fecha y versión del motor de detección
- ruta al servidor de actualización

> **Uso de terminal**
> solo se recomienda el uso de Terminal a usuarios avanzados.

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

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

Protección en tiempo real desactivada

Si un usuario desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para volver a activar la protección en tiempo real, vaya a **Configuración** > **Ordenador** en el menú principal y establezca **Protección del sistema de archivos en tiempo real** en **ACTIVADO**. También puede activar la protección del sistema de archivos en tiempo real en la ventana de preferencias de la aplicación, con la opción **Activar la protección del sistema de archivos en tiempo real** de **Protección en tiempo real**.

La protección en tiempo real no detecta ni desinfecta las amenazas

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

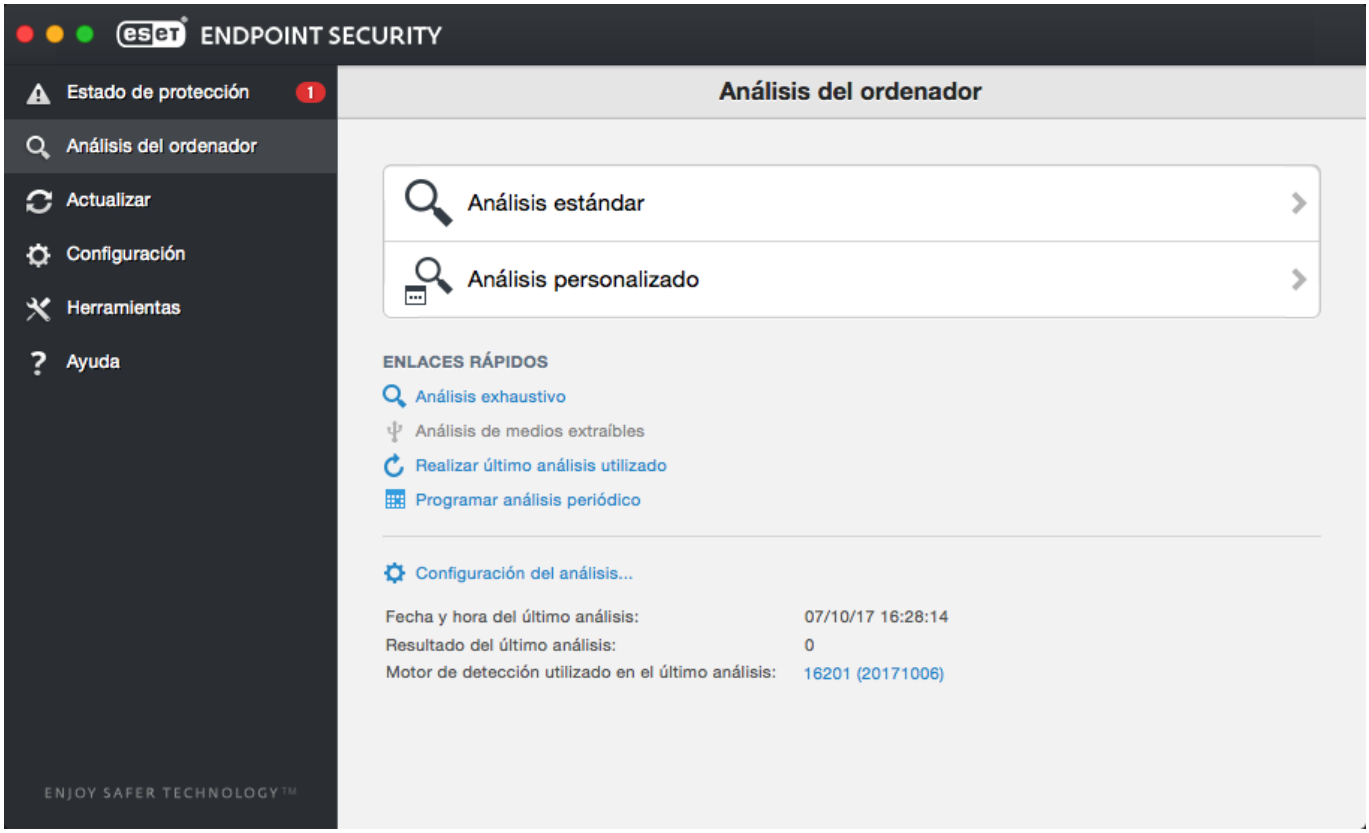
La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema, es posible que se deba a que entra en conflicto con otros programas. Si tiene este problema, póngase en contacto con el servicio de atención al cliente de ESET.

Análisis del ordenador a petición

Si sospecha que su ordenador está infectado (se comporta de manera anormal), ejecute un **Análisis estándar** para examinarlo en busca de infecciones. Para lograr la máxima protección, el ordenador debe analizarse de forma periódica como parte de las medidas de seguridad rutinarias, no únicamente cuando se cree que hay alguna amenaza. Los análisis regulares ayudan a detectar amenazas que no se detectaron durante el análisis en tiempo real cuando se guardaron en el disco. Esto puede ocurrir si el análisis en tiempo real estaba desactivado en el

momento de la infección o si los módulos no están actualizados.



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

También puede arrastrar y soltar los archivos y carpetas seleccionados desde el escritorio o desde la ventana del **Finder** a la pantalla principal de ESET Endpoint Security for macOS, el icono del Dock, el icono de la barra de menús (parte superior de la pantalla) o el icono de la aplicación (situado en la carpeta */Aplicaciones*).

Tipo de análisis

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

Análisis estándar

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

Análisis personalizado

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

Para seleccionar objetos de análisis, seleccione **Análisis del ordenador** > **Análisis personalizado** y, a continuación, seleccione los **Objetos del análisis** específicos que desee en la estructura de árbol. Los objetos del análisis también se pueden especificar con más precisión si se introduce la ruta a la carpeta o los archivos que se desean incluir en el análisis. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Además, puede seleccionar uno de los tres niveles de desinfección si hace clic en **Configurar...** > **Desinfección**.

> **Análisis personalizado**
> Los análisis del ordenador en el modo personalizado solo están recomendados para usuarios avanzados que tienen experiencia previa con programas antivirus.

Objetos de análisis

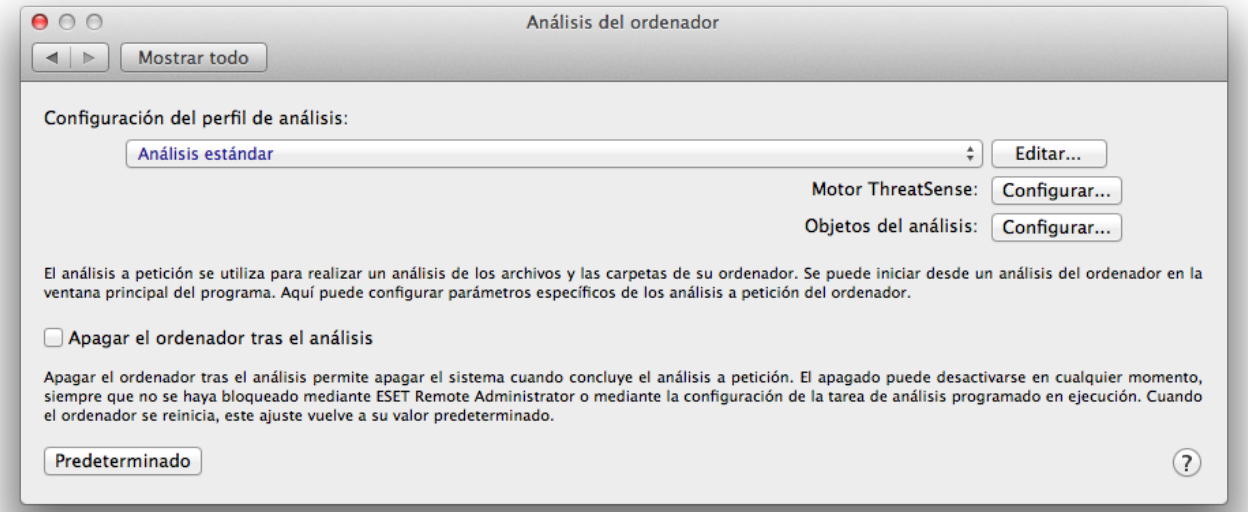
La estructura de árbol de objetos del análisis le permite seleccionar los archivos y carpetas que se analizarán en busca de virus. Las carpetas también se pueden seleccionar según la configuración de un perfil.

Los objetos del análisis se pueden especificar con más precisión introduciendo la ruta a la carpeta o los archivos que se desean incluir en el análisis. Seleccione los objetos en la estructura de árbol en la que aparecen todas las carpetas disponibles del ordenador activando la casilla de verificación que corresponde a un archivo o carpeta determinados.

Perfiles de análisis

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

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



Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte la sección Configuración de parámetros del motor ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

> **Ejemplo**
> Supongamos que desea crear su propio perfil de análisis y parte de la configuración del análisis estándar es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar una desinfección exhaustiva. En la ventana **Lista de perfiles del análisis a petición**, escriba el nombre del perfil, haga clic en **Agregar** y, a continuación en, **Aceptar** para confirmar. Ajuste los parámetros de **Motor ThreatSense** y **Objetos del análisis** para adaptarlos a sus necesidades.

Si desea desactivar el sistema operativo y apagar el ordenador cuando concluya el análisis a petición, utilice la opción **Apagar el ordenador tras el análisis**.

Configuración de parámetros del motor ThreatSense

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

Las opciones de configuración de la tecnología ThreatSense permiten al usuario especificar distintos parámetros de análisis:

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

- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **Configuración > Introducir preferencias de aplicación...** (o pulse *cmd+,*) y, a continuación, haga clic en el botón **Configuración** del motor ThreatSense disponible en los módulos **Protección del inicio**, **Protección en tiempo real** y **Análisis del ordenador**, que utilizan la tecnología ThreatSense (véase a continuación). Es posible que cada escenario de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

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

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

Objetos

En el apartado **Objetos** se pueden definir los archivos que se analizarán en busca de amenazas.

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

empaquetadores estáticos estándares (como UPX, yoda, ASPack, FGS).

Opciones

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

- **Heurística**: la tecnología heurística emplea un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de la detección heurística es la capacidad para detectar nuevo software malicioso que anteriormente no existía.

- **Heurística avanzada**: la heurística avanzada consiste en un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. La capacidad de detección del programa es muy superior gracias a esta tecnología heurística avanzada.

Desinfección

La configuración de desinfección determina el comportamiento del análisis durante la desinfección de los archivos infectados. Hay 3 niveles de desinfección:

- **Sin desinfección**: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de advertencia y permitirá que el usuario seleccione una acción.

- **Desinfección estándar** el programa intenta desinfectar o eliminar de manera automática un archivo infectado. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrecerá una selección de acciones que seguir. La selección de acciones que seguir también aparecerá si no se puede completar una acción predefinida.

- **Desinfección estricta**: el programa desinfectará o eliminará todos los archivos infectados (incluidos los archivos comprimidos). Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un archivo, se mostrará una notificación y se pedirá al usuario que seleccione el tipo de acción que desea realizar.

Modo de desinfección estándar: desinfección de archivos comprimidos

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

Exclusiones

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

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

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

log

cfg

tmp

Límites

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

- **Tamaño máximo:**define el tamaño máximo de los objetos que se van a analizar. El módulo antivirus analizará solo los objetos cuyo tamaño sea inferior al especificado. Se recomienda no modificar el valor predeterminado, ya que normalmente no hay motivo para ello. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos de mayor tamaño.

- **Tiempo máximo de análisis:**define el tiempo máximo asignado para analizar un objeto. Si se introduce aquí un valor definido por el usuario, el módulo antivirus detendrá el análisis de los objetos cuando se haya agotado el tiempo, independientemente de si ha finalizado el análisis o no.

- **Nivel máximo de anidamiento:** especifica la profundidad máxima del análisis de archivos comprimidos. Le recomendamos que no cambie el valor predeterminado de 10: en circunstancias normales, no debería haber motivos para hacerlo. Si el análisis finaliza antes de tiempo debido al número de archivos anidados, el archivo comprimido quedará sin analizar.

- **Tamaño máximo del archivo:** esta opción le permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se van a analizar. Si el análisis finaliza antes de tiempo debido a este límite, el archivo comprimido quedará sin analizar.

Otros

Activar optimización inteligente

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

Analizar flujo de datos alternativo (solo análisis a petición)

Los flujos de datos alternativos (bifurcaciones de recursos/datos) que utiliza el sistema de archivos son asociaciones de carpetas y archivos que escapan a las técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.

Detección de una amenaza

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

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

1. Haga clic en **Análisis del ordenador**.

2. Haga clic en **Análisis estándar** (para obtener más información, consulte el apartado Análisis estándar).

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

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

A modo de ejemplo general de cómo se gestionan las amenazas en ESET Endpoint Security for macOS, suponga que el supervisor del sistema de archivos en tiempo real, que utiliza el nivel de desinfección predeterminado, detecta una amenaza. La protección en tiempo real intentará desinfectar o eliminar el archivo. Si no hay ninguna acción predefinida para el módulo de protección en tiempo real, una ventana de alerta le pedirá que seleccione una opción. Normalmente están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados permanecerían infectados. Esta opción está pensada para situaciones en las que está seguro de que el archivo es inofensivo y se ha detectado por error.

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

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

Protección de web y correo electrónico

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

> **Excepciones de análisis**
> ESET Endpoint Security for macOS no analiza los protocolos cifrados HTTPS, POP3S e IMAPS.

- **Protección del tráfico de Internet**: supervisa la comunicación HTTP entre los navegadores web y los

servidores remotos.

- **Protección del cliente de correo electrónico**: proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing**: bloquea posibles ataques de phishing procedentes de sitios web o dominios.
- **Control web**: le permite bloquear las páginas web que puedan contener material que podría resultar ofensivo o inadecuado.

Protección del acceso a la Web

La protección del tráfico de Internet controla la comunicación entre los navegadores web y los servidores remotos para cumplir con las reglas HTTP (Protocolo de transferencia de hipertexto).

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

Puertos

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

Listas de URL

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

Si desea permitir el acceso exclusivamente a las URL de la lista **URL permitidas**, seleccione **Restringir direcciones URL**.

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

Los símbolos especiales *(asterisco) y ?(marca de interrogación) pueden usarse a la hora de crear listas de URL. El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista.

Protección del correo electrónico

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

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

Añadir mensajes de etiqueta a la nota al pie de los correos electrónicos: después de analizarse un correo electrónico, se puede añadir al mensaje una notificación que contenga los resultados del análisis. No conviene confiar exclusivamente en los mensajes con etiquetas, ya que algunos virus pueden falsificarlas o bien se pueden omitir en mensajes HTML problemáticos. Están disponibles las siguientes opciones:

- **Nunca**: no se agregará ningún mensaje de etiqueta.
- **Solo al correo electrónico infectado**: únicamente se etiquetarán como analizados los mensajes que contengan software malintencionado.
- **A todos los correos electrónicos analizados**: ESET Endpoint Security for macOS agregará mensajes de etiqueta a todos los correos electrónicos analizados.

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

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

- %avstatus%: añade el estado de infección del correo electrónico (por ejemplo: limpio, infectado...).
- %virus%: añade el nombre de la amenaza.
- %product%: añade el nombre de su producto ESET (en este caso, ESET Endpoint Security for macOS).
- %product_url%: añade el vínculo al sitio web de ESET (www.eset.com).

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

- Comprobación del protocolo POP3
- Comprobación del protocolo IMAP

Comprobación del protocolo POP3

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

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema y, después, está activo en la memoria. Asegúrese de que el módulo esté activado para que el filtrado del protocolo funcione correctamente. La comprobación del protocolo POP3 se efectúa automáticamente, sin que tenga que configurar de nuevo el cliente de correo electrónico. De forma predeterminada se analizan todas las comunicaciones realizadas en el puerto 110, pero se pueden agregar otros puertos de comunicación si es necesario. Los números de puerto deben delimitarse con una coma.

Si la opción **Activar la comprobación del protocolo POP3** está activada, se comprueba la presencia de software malicioso en todo el tráfico POP3.

Comprobación del protocolo IMAP

El protocolo de acceso a mensajes de Internet (IMAP) es otro protocolo de Internet para la recuperación de mensajes de correo electrónico. IMAP presenta algunas ventajas sobre POP3; por ejemplo, permite la conexión simultánea de varios clientes al mismo buzón de correo y conserva la información de estado (si el mensaje se ha leído, contestado o eliminado). ESET Endpoint Security for macOS ofrece protección para este protocolo independientemente del cliente de correo electrónico que se utilice.

El módulo de protección que proporciona este control se inicia automáticamente al arrancar el sistema y, después, está activo en la memoria. Asegúrese de que la comprobación del protocolo IMAP esté activada para que el módulo funcione correctamente. El control del protocolo IMAP se efectúa automáticamente, sin que tenga que configurar de nuevo el cliente de correo electrónico. De forma predeterminada se analizan todas las comunicaciones realizadas en el puerto 143, pero se pueden agregar otros puertos de comunicación si es necesario. Los números de puerto deben delimitarse con una coma.

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

Anti-Phishing

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

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

Cortafuegos

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

> **Excepciones de análisis**
> ESET Endpoint Security for macOS no analiza los protocolos cifrados HTTPS, POP3S e IMAPS.

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

Si activa **Bloquear todo el tráfico de red: desconectar la red** el cortafuegos bloqueará todas las comunicaciones entrantes y salientes. Utilice esta opción únicamente si considera que existen riesgos de seguridad críticos que requieran la desconexión del sistema de la red.

Modos de filtrado

El cortafuegos de ESET Endpoint Security for macOS cuenta con tres modos de filtrado. La configuración del modo de filtrado está disponible en Configuración **Introducir las preferencias de la aplicación...** > **Cortafuegos**. El comportamiento del cortafuegos cambia en función del modo seleccionado. Los modos de filtrado influyen también en el nivel necesario de interacción del usuario.

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

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

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

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

Reglas del cortafuegos

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

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

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

Permitir que el software firmado por Apple acceda a la red automáticamente: de manera predeterminada, las aplicaciones firmadas por Apple pueden acceder automáticamente a la red. Para que la aplicación pueda interactuar con los servicios de Apple o instalarse en dispositivos, esta aplicación debe estar firmada con un certificado emitido por Apple. Si quiere desactivar esta función, anule la selección de esta opción. Las aplicaciones que no estén firmadas con el certificado de Apple requerirán la acción del usuario o una regla para acceder a la red.

Cuando esta opción está desactivada, la comunicación de red con servicios firmados de Apple requiere la aprobación del usuario, a menos que la defina una regla de cortafuegos.

En las versiones anteriores es distinto: ESET Endpoint Security for macOS 6.8 y las versiones anteriores bloqueaban la comunicación entrante a los servicios con un certificado de Apple. En la versión actual, ESET Endpoint Security for macOS es capaz de identificar el receptor local de la comunicación entrante y, si esta opción está activada, se permite dicha comunicación.

Creación de reglas nuevas

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

1. Para crear una regla nueva, haga clic en **Agregar...** , escriba el nombre de la regla y arrastre y coloque el icono de la aplicación en el campo en blanco, o haga clic en **Examinar** para buscar el programa en la carpeta */Aplicaciones*. Si desea aplicar la regla a todas las aplicaciones instaladas en el ordenador, seleccione la opción **Todas las aplicaciones**.

2. En la siguiente ventana, especifique la **acción** (permitir o denegar la comunicación entre la aplicación seleccionada y la red) y la **dirección** de la comunicación (entrante, saliente o ambas). Seleccione **Regla de registro** para registrar todas las comunicaciones asociadas a esta regla. Para revisar los registros del cortafuegos, haga clic en **Herramientas** > **Archivos de registro** en el menú principal de ESET Endpoint Security for macOS y seleccione **Cortafuegos** en el menú desplegable **Registro**.

3. Defina en el apartado **Protocolo/Puertos** el protocolo y el puerto que utiliza la aplicación (si se ha seleccionado protocolo TCP o UDP) para comunicarse. La capa del protocolo de transporte ofrece una transferencia de datos segura y eficiente.

4. Por último, especifique los criterios del **Destino** (dirección IP, rango, subred, Ethernet o Internet) para la regla.

Zonas del cortafuegos

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

Estas zonas pueden crearse haciendo clic en **Agregar.** Introduzca un **nombre** y una **descripción** (opcional) para la zona, seleccione el perfil al que pertenecerá y agregue una dirección IPv4/IPv6, un rango de direcciones, una subred, una red Wi-Fi o una interfaz.

Perfiles del cortafuegos

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

cortafuegos.

Registros del cortafuegos

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

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

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

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

Control del dispositivo

ESET Endpoint Security for macOS le permite analizar, bloquear o ajustar los filtros o permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo de memoria determinado y trabajar en él. Esta opción puede resultar útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

> **Control de dispositivos en macOS 11 y versiones posteriores**
> ESET Endpoint Security for macOS instalado en macOS 11 y versiones posteriores analiza solo los dispositivos de memoria (como unidades USB, CD, DVD, etc.).

Dispositivos externos admitidos en macOS 10.15 y versiones anteriores:

- Almacenamiento en disco (unidad de disco duro, unidad flash USB)
- CD/DVD
- Impresora USB

- Dispositivo de imagen
- Puerto serie
- Red
- Dispositivo portátil

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

El registro del control de dispositivos crea una entrada para todos los incidentes que activan el control de dispositivos. Las entradas de registro se pueden ver desde la ventana principal del programa de ESET Endpoint Security for macOS en **Herramientas** > Archivos de registro.

Editor de reglas

Las opciones de configuración del control del dispositivo se pueden modificar en **Configuración** > **Introducir las preferencias de la aplicación...** > **Control del dispositivo**.

Al hacer clic en **Activar el Control de dispositivos** se activa la función de Control de dispositivos de ESET Endpoint Security for macOS. Una vez que el Control de dispositivos esté activado podrá gestionar y editar las funciones de Control de dispositivos. Active la casilla de verificación situada junto al nombre de una regla para activar o desactivar dicha regla.

Utilice los botones + o − para añadir o eliminar reglas. Las reglas se muestran en orden de prioridad; las que tienen más prioridad se muestran más arriba en la lista. Para reorganizar el orden, arrastre y coloque una regla en su nueva posición, o haga clic en ⚙ y elija una de las opciones.

ESET Endpoint Security for macOS detecta automáticamente todos los dispositivos actualmente insertados y sus parámetros (Tipo de dispositivo, Proveedor, Modelo, Número de serie). En lugar de crear las reglas de forma manual, haga clic en la opción **Llenar**, seleccione el dispositivo y haga clic en **Continuar** para crear la regla.

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

Nombre
Introduzca una descripción de la regla en el campo **Nombre** para facilitar su identificación. La casilla de verificación **Regla activada** activa o desactiva esta regla; esta opción puede resultar útil si no desea eliminar la regla de forma permanente.

Tipo de dispositivo

Seleccione el tipo de dispositivo externo en el menú desplegable. La información del tipo de dispositivo se recopila del sistema operativo. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Ejemplos de dispositivos de imagen son escáneres o cámaras. Como estos dispositivos solo proporcionan información sobre sus acciones y no sobre los usuarios, solo pueden bloquearse a nivel global.

Acción

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

Lectura/Escritura: se permitirá el acceso completo al dispositivo.

Solo lectura: solo se permitirá el acceso de lectura al dispositivo.

Bloquear: se bloqueará el acceso al dispositivo.

Tipo de criterios

Seleccione **Grupo de dispositivos** o **Dispositivo**. A continuación se muestran otros parámetros que se pueden usar para ajustar las reglas y adaptarlas a dispositivos.

Proveedor: filtrado por nombre o identificador del proveedor.

Modelo: el nombre del dispositivo.

Número de serie: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio en cuestión, no en la unidad de CD o DVD.

> **Sin parámetros definidos**
>
> Si no se definen estos parámetros, la regla ignorará estos cambios a la hora de establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).

> **CONSEJO**
>
> Para ver información sobre un dispositivo, cree una regla para ese tipo de dispositivo y conecte el dispositivo a su ordenador. Una vez que el dispositivo se haya conectado, los detalles del mismo se mostrarán en el Registro de control de dispositivos.

Nivel de registro

Siempre: registra todos los sucesos.

Diagnóstico: registra la información necesaria para ajustar el programa.

Información: registra los mensajes informativos, además de todos los registros anteriores.

Advertencia: registra errores graves y mensajes de advertencia.

Ninguno: no se registra nada.

Lista de usuarios

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios si se agregan a la lista de usuarios:

Editar...: abre el **Editor de identidad**, donde puede seleccionar usuarios o grupos. Para definir una lista de usuarios, selecciónelos en la lista **Usuarios** de la izquierda y haga clic en **Agregar**. Para quitar un usuario, seleccione su nombre en la lista **Usuarios seleccionados** y haga clic en **Quitar**. Para ver todos los usuarios del sistema, seleccione **Mostrar todos los usuarios**. Si la lista está vacía, todos los usuarios estarán autorizados.

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

Control de acceso web

La función **Control web** permite configurar las opciones que protegen a su empresa frente al riesgo de responsabilidad jurídica, y además le permite regular el acceso a sitios web que infrinjan los derechos de propiedad intelectual. El objetivo es impedir que los empleados accedan a páginas con contenido inapropiado o perjudicial, o páginas que puedan afectar negativamente a la productividad en el trabajo. Los empleados o administradores del sistema pueden prohibir el acceso a más de 27 categorías de sitios web predefinidas y más de 140 subcategorías.

De forma predeterminada, el control de acceso web está desactivado. Para activarlo, haga clic en **Configuración** > **Introducir preferencias de aplicación** > **Control de acceso web** y active la casilla de verificación situada junto a **Habilitar control de acceso web**.

En la ventana del Editor de reglas se muestran reglas existentes basadas en URL o en categorías. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de bloqueo, la acción que debe realizarse cuando coincide una regla de control de acceso web y la gravedad del registro.

Para crear una regla nueva, haga clic en el botón +. Haga doble clic en el campo **Nombre** y escriba una descripción de la regla para facilitar su identificación.

La casilla de verificación del campo **Activada** activa y desactiva la regla; esta opción puede resultar útil si desea usar la regla más tarde pero no quiere eliminarla permanentemente.

Tipo

Acción basada en una URL: acceso al sitio web proporcionado. Haga doble clic en el campo **URL/Categoría** e introduzca la dirección URL correspondiente.

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

Acción basada en una categoría: haga doble clic en el campo **URL/Categoría** y seleccione las categorías.

Identidad

Le permite seleccionar los usuarios a los que se aplicará la regla.

Derechos de acceso

Permitir: se permitirá el acceso a la dirección URL o a la categoría.

Bloquear: bloquea la dirección URL o la categoría.

Gravedad (para filtrar archivos de registro).

Siempre: registra todos los sucesos.

Diagnóstico: registra la información necesaria para ajustar el programa.

Información: registra los mensajes informativos, además de todos los registros anteriores.

Alerta: registra errores graves y mensajes de alerta.

Ninguno: no se crea ningún registro.

Herramientas

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

Archivos de registro

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

Se puede acceder a los archivos de registro desde el menú principal de ESET Endpoint Security for macOS haciendo clic en **Herramientas** > **Archivos de registro**. Seleccione el tipo de registro deseado con el menú desplegable Registro disponible en la parte superior de la ventana. Están disponibles los siguientes registros:

1. **Amenazas detectadas**: información sobre sucesos relacionados con la detección de infiltraciones.

2. **Sucesos**: todas las acciones importantes realizadas por ESET Endpoint Security for macOS se documentan en los registros de sucesos.

3. **Análisis del ordenador**: en esta ventana se muestran los resultados de todos los análisis completados. Haga doble clic en cualquier entrada para ver los detalles del análisis de un ordenador concreto.

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

5. **Cortafuegos**: el registro del cortafuegos muestra todos los ataques remotos detectados por el cortafuegos. Los registros del cortafuegos contienen información sobre los ataques al sistema detectados. En la columna **Suceso** se enumeran los ataques detectados, la columna **Fuente** ofrece más información sobre el atacante, y la columna **Protocolo** revela el protocolo de comunicación empleado para el ataque.

6. **Control web**: muestra las direcciones URL bloqueadas o permitidas e información sobre su clasificación.

7. **Sitios web filtrados**: esta lista es útil si desea ver una lista de sitios web bloqueados por Protección del acceso a la Web. o el Control web han bloqueado.. En estos registros puede ver la hora, la URL, el estado, la

dirección IP, el usuario y la aplicación que estableció una conexión con el sitio web determinado.

Haga clic con el botón derecho del ratón sobre cualquier archivo de registro y elija **Copiar** para copiar al portapapeles el contenido de dicho archivo de registro.

Mantenimiento de registros

La configuración de registros de ESET Endpoint Security for macOS está disponible en la ventana principal del programa. Haga clic en **Configuración** > **Introducir las preferencias de la aplicación** > **Herramientas** > **Archivos de registro**. Puede especificar las siguientes opciones para los archivos de registro:

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

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

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

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

- Los sucesos como *Nombre de usuario y contraseña no válidos*, *No se pueden actualizar los módulos*, etc. se registran en el archivo *eventslog.txt*.
- Las amenazas detectadas por Análisis en el inicio, Protección en tiempo real o Análisis del ordenador se guardan en el archivo *threatslog.txt*.
- Los resultados de todos los análisis completados se guardan en formato *scanlog.NÚMERO.txt*
- Los dispositivos bloqueados por el control de dispositivos se registran en devctllog.txt
- Los sucesos relacionados con la comunicación a través del cortafuegos se registran en firewalllog.txt
- Las páginas web bloqueadas por el control de acceso web se registran en webctllog.txt

Para configurar los filtros de **Filtro predeterminado de registros de análisis del ordenador**, haga clic en **Editar** y seleccione o anule la selección de los tipos de registro que desee. Encontrará una explicación más detallada de estos tipos de registro en Filtrado de registros.

Filtrado de registros

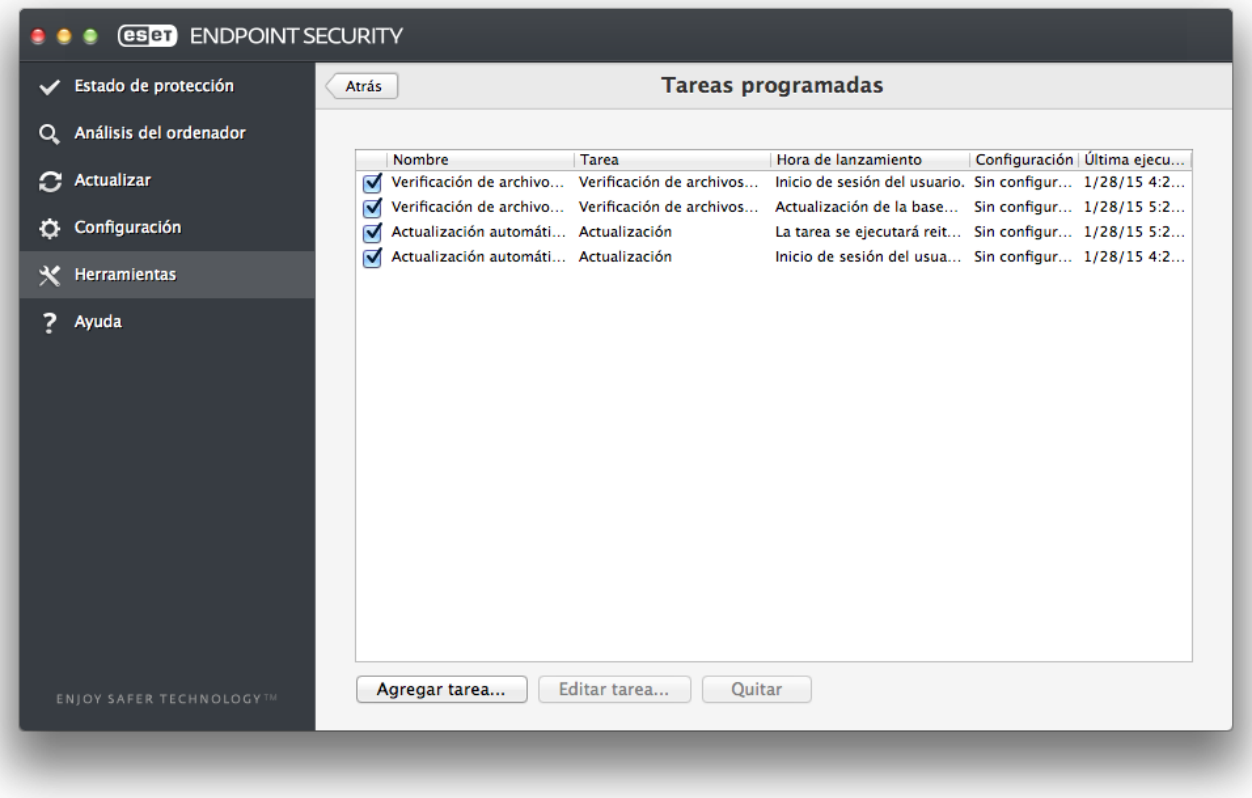
Los registros guardan información sobre sucesos importantes del sistema. La función de filtrado de registros permite ver los registros de sucesos determinados.

A continuación se incluyen los tipos de registros utilizados con más frecuencia:

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

Planificador de tareas

La opción **Tareas programadas** está disponible en el menú principal de ESET Endpoint Security for macOS, en **Herramientas**. **Tareas programadas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.



Las Tareas programadas administran e inician las tareas programadas con la configuración y las propiedades predefinidas. La configuración y las propiedades contienen información como la fecha y la hora, así como los

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

De forma predeterminada, en las Tareas programadas se muestran las siguientes tareas programadas:

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

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

Creación de nuevas tareas

Para crear una nueva tarea en Tareas programadas, haga clic en **Agregar tarea** o pulse control y haga clic en el espacio en blanco y seleccione **Agregar** en el menú contextual. Hay cuatro tipos de tareas programadas disponibles:

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

> **Tareas definidas por el usuario**
> De forma predeterminada, un usuario especial creado por ESET con derechos restringidos ejecuta las aplicaciones. Si desea cambiar el valor predeterminado del usuario, escriba el nombre de usuario seguido de dos puntos (:) delante del comando. Con esta característica también puede utilizar el usuario **root**.

Ejemplo: Ejecutar tarea como usuario

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

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

Limitaciones de nombre de usuario

No se pueden utilizar espacios ni caracteres de espacio en blanco delante de un nombre de usuario. Los espacios tampoco se pueden utilizar en el nombre de usuario. En su lugar, debe utilizarse un carácter en blanco.

Análisis como propietario de un directorio

Puede analizar directorios como propietario del directorio:
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done

También puede analizar la carpeta /tmp como el usuario que ha iniciado sesión:
root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

Ejemplo: Tarea de actualización

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

1. Seleccione **Actualización** en el menú desplegable **Tarea programada**.
2. Escriba el nombre de la tarea en el campo **Nombre de la tarea**.
3. Seleccione la frecuencia de la tarea en el menú desplegable **Ejecutar tarea**. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización. Si selecciona **Definido por el usuario**, se le pedirá que especifique la fecha y la hora en formato cron (para obtener más información, consulte el apartado Creación de tareas definidas por el usuario).
4. En el siguiente paso, seleccione una opción alternativa si la tarea no se puede realizar o completar a la hora programada.
5. Haga clic en **Finalizar**. La nueva tarea programada se agregará a la lista de tareas programadas actualmente.

De forma predeterminada, ESET Endpoint Security for macOS contiene tareas programadas predefinidas que están configuradas para garantizar el correcto funcionamiento del producto. Estas tareas no se deben modificar, por lo que están ocultas de forma predeterminada. Para ver estas tareas, diríjase al menú principal, haga clic en **Configuración** > **Introducir preferencias de aplicación** > **Tareas programadas** y, a continuación, seleccione **Mostrar tareas del sistema**.

Creación de tareas definidas por el usuario

Cuando se selecciona Definida por el usuario como tipo de tarea en el menú desplegable Ejecutar tarea se deben definir varios parámetros especiales.

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

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

Ejemplo:
`30 6 22 3 2012 4`

En las expresiones cron se admiten los siguientes caracteres especiales:

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

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

Tareas definidas por el usuario
Si define el día del mes y el día de la semana, el comando solo se ejecutará cuando ambos campos coincidan.

LiveGrid®

El sistema de alerta temprana LiveGrid® informa a ESET de las nuevas amenazas de forma inmediata y continua. El sistema de alerta temprana LiveGrid® bidireccional tiene un único objetivo: mejorar la protección que le ofrecemos. La mejor manera de garantizar la detección de nuevas amenazas en cuanto aparecen es "vincular" al mayor número posible de clientes y usar la información que recopilan para mantener nuestros módulos de detección constantemente actualizados. Seleccione una de las dos opciones para LiveGrid®:

1. Puede optar por no activar el sistema de alerta temprana LiveGrid®. El software no perderá funcionalidad, pero en algunos casos ESET Endpoint Security for macOS puede responder más rápido a nuevas amenazas que una actualización de los módulos de detección.

2. Puede configurar el sistema de alerta temprana LiveGrid® para que envíe información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso. Esta información se puede enviar a ESET para que realice un análisis detallado. El análisis de estas amenazas ayudará a ESET a actualizar su base de datos de amenazadas y mejorar nuestra capacidad para detectar amenazas.

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

Aunque existe la posibilidad de que este proceso revele cierta información acerca del usuario o su ordenador

(nombres de usuario en una ruta al directorio, etc.) al laboratorio de amenazas de ESET, esta información no se utilizará con NINGÚN propósito que no esté relacionado con la ayuda necesaria para responder inmediatamente a nuevas amenazas.

Para acceder a la configuración de LiveGrid® desde el menú principal, haga clic en **Configuración** > **Introducir preferencias de aplicación** > **LiveGrid®**. Seleccione **Activar el sistema de reputación ESET LiveGrid®™ (recomendado)** para activar LiveGrid® y, a continuación, haga clic en **Configuración** junto a **Opciones avanzadas**.

Archivos sospechosos

De forma predeterminada, ESET Endpoint Security for macOS está configurado para enviar archivos sospechosos al laboratorio de amenazas de ESET para su análisis detallado. Si no desea enviar estos archivos automáticamente, cancele la selección de la opción **Envío de archivos sospechosos (Configuración** > **Introducir preferencias de aplicación** > **LiveGrid® > Configuración)**.

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

Envío de información estadística anónima: el sistema de advertencia temprana ESET LiveGrid® recopila información anónima acerca del ordenador en relación con amenazas recién detectadas. Esta información incluye el nombre de la amenaza, la fecha y la hora en que se detectó, la versión del producto de seguridad de ESET, la versión del sistema operativo de su ordenador y la configuración regional. Normalmente, estas estadísticas se envían a los servidores de ESET una o dos veces al día.

Ejemplo: paquete de información estadística enviada

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

Filtro de exclusión: esta opción le permite excluir del envío determinados tipos de archivo. Esta opción puede ser útil, por ejemplo, para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen de manera predeterminada ((.doc, .rtf, etc.). Si lo desea, puede añadir estos tipos de archivo a la lista de archivos excluidos.

Correo electrónico de contacto (opcional): se utilizará su dirección de correo electrónico si se requiere más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

Cuarentena

La finalidad principal de la cuarentena es almacenar de forma segura los archivos infectados. Los archivos deben colocarse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Endpoint Security for macOS los detecta incorrectamente como infectados.

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

Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo por el que se puso en cuarentena (agregado por el usuario, por ejemplo) y el número de amenazas detectadas. La carpeta de cuarentena (*/Library/Application Support/Eset/esets/cache/quarantine*) permanece en el sistema incluso después de desinstalar ESET Endpoint Security for macOS. Los archivos en cuarentena se guardan en un formato cifrado seguro y se pueden restaurar tras la instalación de ESET Endpoint Security for macOS.

Poner archivos en cuarentena

ESET Endpoint Security for macOS pone en cuarentena automáticamente los archivos eliminados (si no ha anulado esta opción en la ventana de alerta). Desde la ventana Cuarentena puede hacer clic en la opción Cuarentena para poner un archivo en cuarentena. También puede pulsar la tecla Control y hacer clic en un archivo y seleccionar Servicios > ESET Endpoint Security for macOS - Agregar archivos a la carpeta Cuarentena para enviar el archivo a cuarentena.

Restauración de archivos de cuarentena

Los archivos en cuarentena pueden restaurarse a su ubicación original. Para ello, seleccione un archivo en cuarentena y haga clic en **Restaurar**. La opción Restaurar también está disponible en el menú contextual: pulse la tecla Ctrl, haga clic en un archivo determinado dentro de la ventana de Cuarentena y, a continuación, haga clic en **Restaurar**. Puede usar **Restaurar a** para restaurar un archivo a una ubicación distinta a la que presentaba antes de enviarse a cuarentena.

Envío de un archivo de cuarentena

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

Privilegios

La configuración de ESET Endpoint Security for macOS 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 modificar la configuración del programa.

Puede configurar los usuarios con privilegios en **Configuración** > **Introducir preferencias de aplicación** > **Usuario** > **Privilegios**.

Para ofrecer una seguridad máxima para su sistema es esencial que el programa se haya configurado

correctamente. Las modificaciones no autorizadas pueden provocar la pérdida de datos importantes. Para configurar una lista de usuarios con privilegios, selecciónelos en la lista **Usuarios** de la izquierda y haga clic en **Agregar**. Para quitar un usuario, seleccione su nombre en la lista **Usuarios con privilegios** de la derecha y haga clic en **Quitar**. Para ver todos los usuarios del sistema, seleccione **Mostrar todos los usuarios**.

> **Lista de usuarios con privilegios vacía**
> si la lista de usuarios con privilegios está vacía, todos los usuarios del sistema tendrán permiso para modificar la configuración del programa.

Modo Presentación

El **modo Presentación** es una función destinada a aquellos usuarios que exigen que el software funcione sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. Este modo también se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Cuando está activado, se desactivan todas las ventanas emergentes y las tareas programadas no se ejecutan. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Para activar el modo Presentación manualmente, haga clic en **Configuración** > **Introducir preferencias de aplicación...** > **Modo Presentación** > **Activar modo Presentación**.

Active la casilla de verificación situada junto a **Activar automáticamente el modo Presentación a pantalla completa** para activar el modo Presentación automáticamente cuando las aplicaciones se ejecuten en el modo de pantalla completa. Cuando esta función esté activada, el modo Presentación se ejecutará siempre que inicie una aplicación a pantalla completa, y se detendrá automáticamente cuando salga de la aplicación. Esta opción resulta especialmente práctica al realizar una presentación.

También puede seleccionar **Desactivar el modo de presentación automáticamente después de** para definir la cantidad de tiempo, en minutos, que tardará en desactivarse el modo de presentación automáticamente.

Activar el modo Presentación constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección de ESET Endpoint Security for macOS se volverá naranja y mostrará un signo de alerta.

> **Modo interactivo y Modo presentación en el cortafuegos**
> Si el cortafuegos está en Modo interactivo y el Modo presentación está activado, puede tener problemas para conectarse a Internet. Esto puede ser un problema si la aplicación necesita conexión a Internet. Por lo general, se le solicita que confirme dicha acción (si no se ha definido ninguna regla o excepción de comunicación), pero en el modo de Presentación la intervención del usuario está desactivada. La solución es definir una regla de comunicación para cada aplicación que pueda entrar en conflicto con este comportamiento o utilizar un Modo de filtrado diferente en el cortafuegos. Recuerde que si el modo de presentación está activado y accede a una página web o aplicación que presente un riesgo de seguridad potencial, esta podría bloquearse sin que se muestre ninguna explicación o alerta, ya que la intervención del usuario está desactivada.

Procesos en ejecución

En la lista **Procesos en ejecución** se muestran los procesos que se están ejecutando en el ordenador. ESET Endpoint Security for macOS proporciona información detallada sobre los procesos en ejecución para proteger a

los usuarios con la tecnología ESET LiveGrid®.

- **Proceso**: nombre del proceso que se está ejecutando actualmente en el ordenador. También puede usar el Monitor de actividad (disponible en */Applications/Utilities*) para ver todos los procesos que se encuentran en ejecución en el ordenador.

- **Nivel de riesgo**: en la mayoría de los casos, ESET Endpoint Security for macOS y la tecnología ESET LiveGrid® asignan un nivel de riesgo a los objetos (archivos, procesos, etc.) mediante una serie de reglas heurísticas que examinan las características de cada uno de ellos y, después, estiman el potencial de actividad maliciosa. De acuerdo con esta heurística, se asigna un nivel de riesgo a los diferentes objetos. Las aplicaciones conocidas marcadas en verde son totalmente seguras (incluidas en lista blanca) y se excluirán del análisis. Esto aumenta la velocidad de los análisis a petición y en tiempo real. El hecho de que una aplicación esté marcada como desconocida (amarillo) no implica necesariamente que se trate de software malicioso. Normalmente se trata de una aplicación reciente. Si no está seguro de la clasificación de un archivo, puede enviarlo al laboratorio de amenazas de ESET para su análisis. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una actualización futura.

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

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

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

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

- **Archivo**: ubicación de una aplicación en el ordenador.

- **Tamaño del archivo**: tamaño físico del archivo en el disco.

- **Descripción del archivo**: características del archivo en función de su descripción del sistema operativo.

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

- **Versión del archivo**: información sobre el editor de la aplicación.

- **Nombre del producto**: nombre de la aplicación o nombre comercial.

Interfaz de usuario

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

- Si desea ver la pantalla de inicio de ESET Endpoint Security for macOS al iniciar el sistema, seleccione **Mostrar la pantalla de bienvenida al iniciar el programa**.

- **Aplicación presente en el Dock** le permite visualizar el icono de ESET Endpoint Security for macOS en el Dock del macOS, así como alternar ESET Endpoint Security for macOS y otras aplicaciones en ejecución pulsando *cmd+tab*. Los cambios se aplican tras reiniciar ESET Endpoint Security for macOS (normalmente se activa con el reinicio del sistema).

- **Utilizar menú estándar** le permite utilizar determinados accesos directos del teclado (consulte Accesos directos del teclado) y ver los elementos del menú estándar (Interfaz de usuario, Configuración y Herramientas) en la barra de menús de macOS (parte superior de la pantalla).

- Active **Mostrar sugerencias y consejos útiles** para mostrar información cuando se coloque el cursor sobre determinadas opciones de ESET Endpoint Security for macOS.

- **Mostrar archivos ocultos** le permite ver y seleccionar los archivos ocultos en la configuración de **Objetos del análisis** de un **Análisis del ordenador**.

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

Alertas y notificaciones

El apartado **Alertas y notificaciones** le permite configurar la gestión de las alertas de amenazas, el estado de la protección y las notificaciones del sistema en ESET Endpoint Security for macOS.

La desactivación de **Mostrar alertas** desactivará todas las ventanas de alertas; esta opción solo se recomienda en situaciones concretas. Para la mayoría de los usuarios se recomienda mantener la opción predeterminada (activada). Las opciones avanzadas se describen en este capítulo.

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

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

Mostrar alertas

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

En **Lista de cuadros de diálogo** (disponible en **Configuración** > **Introducir preferencias de aplicación...** > **Alertas y notificaciones** > **Mostrar alertas: Configuración...**) se muestra la lista de todos los cuadros de diálogo de alertas

activados por ESET Endpoint Security for macOS. Para activar o suprimir cada notificación, active la casilla de verificación que aparece a la izquierda del **Nombre del cuadro de diálogo**. Cuando la casilla de verificación esté activada, la notificación siempre se mostrará y no se aplicarán las **Condiciones de visualización**. Si no quiere recibir notificaciones de un suceso concreto de la lista, desmarque esta opción. Si lo desea, también puede definir las **Condiciones de visualización** en las que se realizará una acción concreta.

Estados de protección

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

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

- Cortafuegos
- Anti-Phishing
- Protección del acceso a la Web
- Protección del cliente de correo electrónico
- Modo Presentación
- Actualización del sistema operativo
- Caducidad de la licencia
- Es necesario reiniciar el ordenador

Menú contextual

Para que las funciones de ESET Endpoint Security for macOS estén disponibles desde el menú contextual, haga clic en **Configuración** > **Introducir preferencias de aplicación** > **Menú contextual** y active la casilla de verificación situada junto a **Integrar en el menú contextual**. Los cambios entrarán en vigor cuando cierre sesión o reinicie el ordenador. Las opciones del menú contextual estarán disponibles en el escritorio y en la ventana de **Finder** al hacer CTRL + clic en cualquier archivo o carpeta.

Actualización

Es necesario actualizar ESET Endpoint Security for macOS de forma periódica para mantener el máximo nivel de seguridad. El módulo de actualización garantiza que el programa esté siempre actualizando descargando los módulos de detección más recientes.

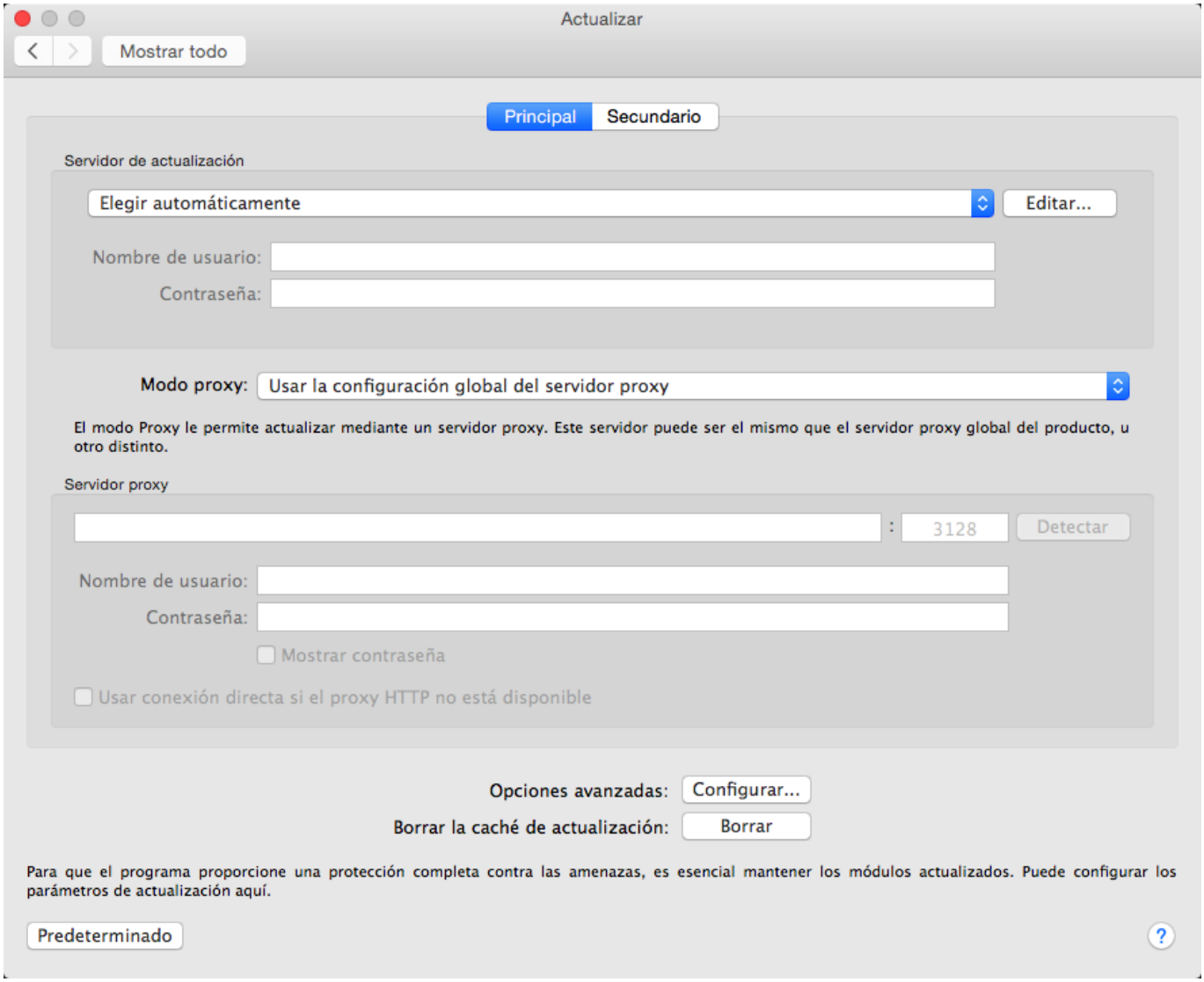
Haga clic en **Actualización** en el menú principal para comprobar el estado de la actualización actual, incluidas la fecha y la hora de la última actualización, y compruebe si es necesario actualizar el programa. Haga clic en **Actualizar módulos** para iniciar el proceso de actualización manualmente.

En circunstancias normales, cuando las actualizaciones se descarguen correctamente, se mostrará el mensaje *No es necesario actualizar los módulos, ya están actualizados* en la ventana Actualización si tiene los módulos más recientes. Si no es posible actualizar los módulos, se recomienda revisar la configuración de actualización; el motivo más habitual de este error es introducir incorrectamente los datos de licencia o la configuración de conexión.

La ventana **Actualización** también contiene el número de versión del motor de detección. Este indicador numérico está vinculado al sitio web de ESET que muestra la información de actualización del motor de detección.

Configuración de actualizaciones

En la sección de configuración de actualizaciones se especifica la información del origen de la actualización, como los servidores de actualización y sus datos de autenticación. De forma predeterminada, el menú desplegable **Servidor de actualización** está configurado en **Elegir automáticamente** para garantizar que los archivos de actualización se descargarán del servidor ESET cuando la carga de la red sea menor.



La lista de servidores de actualización disponibles está accesible en el menú desplegable **Servidor de actualización**. Para agregar un nuevo servidor de actualización, haga clic en **Editar,** introduzca la dirección del nuevo servidor en el campo de entrada **Servidor de actualización** y haga clic en **Agregar**.

ESET Endpoint Security for macOS le permite establecer un servidor de actualización alternativo o de conmutación por error. El servidor **Primario** puede ser su servidor Mirror y el **Servidor secundario** ser el de actualización estándar de ESET. El servidor secundario debe ser distinto del primario, ya que, de lo contrario, no se utilizará. Si no especifica un servidor de actualización secundario, ni un nombre de usuario ni una contraseña, la función de conmutación por error de actualización no funcionará. También puede seleccionar Elegir automáticamente para introducir el nombre de usuario y la contraseña en los campos correspondientes y que ESET Endpoint Security for macOS elija automáticamente el mejor servidor de actualización para utilizarlo.

Modo proxy le permite actualizar los módulos de detección con un servidor proxy (por ejemplo, un proxy HTTP local). El servidor puede ser el mismo servidor proxy global que se aplica a todas las características del programa que requieren una conexión, o uno distinto. La configuración del servidor proxy global se debe haber definido durante la instalación o en Configuración del servidor proxy.

Para configurar un cliente para que solo descargue las actualizaciones desde un servidor proxy:

1. Seleccione **Conexión a través de un servidor proxy** en el menú desplegable.

2. Haga clic en **Detectar** para permitir que ESET Endpoint Security for macOS rellene la dirección IP y el número de puerto (**3128** de forma predeterminada).

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

ESET Endpoint Security for macOS detecta la configuración del proxy a partir de las Preferencias del Sistema de macOS. La configuración puede definirse en macOS en > **Preferencias del Sistema** > **Red** > **Avanzado** > **Proxies**.

Si activa **Usar conexión directa si el proxy HTTP no está disponible**, ESET Endpoint Security for macOS intentará conectarse automáticamente a los servidores de actualización sin utilizar proxy. Esta opción se recomienda para usuarios móviles con MacBooks.

Si experimenta dificultades al intentar descargar actualizaciones de los módulos de detección, haga clic en **Borrar la caché de actualización para eliminar los archivos de actualización temporales**.

Opciones avanzadas

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

Active las actualizaciones de prueba para descargar módulos de desarrollo que se encuentran en la fase final de pruebas. Las actualizaciones de prueba suelen contener soluciones para problemas del producto. La actualización retrasada descarga las actualizaciones unas horas después de su publicación, con el fin de garantizar que los clientes no reciben las actualizaciones hasta que se ha confirmado que no presentan ningún problema de seguridad en estado salvaje.

ESET Endpoint Security for macOS registra instantáneas de los módulos de detección y del programa para usarlas con la función **Reversión de actualización**. Mantenga la opción **Crear instantáneas de archivos de actualización** activada para que ESET Endpoint Security for macOS registre estas instantáneas automáticamente. Si sospecha que una nueva actualización del módulo de detección o del módulo del programa puede ser inestable o estar

dañada, puede usar la función Reversión de actualización para volver a una versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente. Cuando utilice la función Reversión de actualización para volver a una actualización anterior, utilice el menú desplegable Definir periodo de suspensión en para especificar el periodo de tiempo durante el que desee suspender las actualizaciones. Si selecciona la opción Hasta que se revoque, las actualizaciones normales no se reanudarán hasta que las restaure manualmente. Tenga cuidado al establecer el periodo de tiempo durante el que desee suspender las actualizaciones.

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

Cómo crear tareas de actualización

Haga clic en Actualización > **Actualizar módulos** para activar manualmente una actualización de los módulos de detección.

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

- **Actualización automática periódica**
- **Actualización automática tras el inicio de sesión del usuario**

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

Actualizaciones del sistema

La función de actualizaciones del sistema macOS es un componente importante que tiene como objetivo proteger a los usuarios frente al software malicioso. Para una mayor seguridad, le recomendamos que instale estas actualizaciones en cuanto estén disponibles. ESET Endpoint Security for macOS le informará de las actualizaciones que faltan en función del nivel de importancia. Puede ajustar el nivel de importancia de actualización para el que se muestran notificaciones en **Configuración** > **Introducir preferencias de aplicación** > **Alertas y notificaciones** > **Configuración con el menú desplegable Condiciones de visualización** situado junto a **Actualizaciones del sistema operativo**.

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

Si no desea recibir notificaciones relativas a las actualizaciones que faltan, anule la selección de la casilla de

verificación disponible junto a **Actualizaciones del sistema operativo**.

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

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

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

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

Importar y exportar configuración

Si desea importar una configuración existente o exportar la configuración de ESET Endpoint Security for macOS, haga clic en **Configuración** > **Importar y exportar configuración.**

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

Para importar una configuración, seleccione **Importar configuración** y haga clic en **Examinar** para acceder al archivo de configuración que desee importar. Para exportar, seleccione **Exportar configuración** y utilice el navegador para seleccionar la ubicación de su ordenador en la que quiere guardar el archivo de configuración.

Configuración del servidor proxy

La configuración del servidor proxy se puede configurar en **Configuración** > **Introducir preferencias de aplicación** > **Servidor proxy**. Al especificar el servidor proxy en este nivel se define la configuración global del servidor proxy para todas las funciones de ESET Endpoint Security for macOS. Los parámetros definidos aquí los utilizarán todos los módulos que necesiten conexión a Internet. ESET Endpoint Security for macOS es compatible con los tipos de autenticación Basic Access y NTLM (NT LAN Manager).

Para especificar la configuración del servidor proxy en este nivel, seleccione **Utilizar servidor proxy** e introduzca la dirección IP o URL de su servidor proxy en el campo **Servidor proxy**. En el campo Puerto, especifique el puerto en el que el servidor Proxy acepte conexiones (el (3128, de forma predeterminada). También puede hacer clic en **Detectar** para permitir que el programa cumplimente los dos campos.

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

Caché local compartida

Si desea activar el uso de la Caché local compartida, haga clic en Configuración > Introducir preferencias de aplicación > Caché local compartida y active la casilla de verificación situada junto a Activar el almacenamiento en caché con Caché local compartida de ESET. El uso de esta función mejora el rendimiento en entornos virtualizados al eliminar el análisis duplicado en la red. De esta manera se garantiza que cada archivo se analizará solo una vez y se almacenará en la caché compartida. Cuando se activa esta opción, la información relativa a análisis de archivos y carpetas de la red se guarda en la caché local. Si realiza un análisis nuevo, ESET Endpoint Security for macOS buscará los archivos analizados en la caché. Si los archivos coinciden, no se incluirán en el análisis.

Entre los ajustes de la Caché local compartida encontramos los siguientes:

- **Dirección del servidor**: nombre o dirección IP del ordenador en el que está la caché.
- **Puerto**: número de puerto utilizado para la comunicación ((3537 de forma predeterminada).
- **Contraseña**: la contraseña de la Caché local compartida (opcional).

> **Instrucciones detalladas**
> Para obtener instrucciones detalladas sobre cómo instalar y configurar la Caché local compartida de ESET, consulte el Manual de usuario de la Caché local compartida de ESET (este documento está disponible únicamente en inglés).

Acuerdo de licencia para el usuario final

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

Acuerdo de licencia para el usuario final

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

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

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

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

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

concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

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

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

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

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

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

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

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

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

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los

derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la licencia, el usuario debe eliminar, destruir o devolver (a sus expensas) el software y todas las copias de seguridad del mismo a ESET o al lugar donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

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

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

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

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

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

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

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

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

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

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

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

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

a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.

c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.

d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.

e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.

f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.

g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. **Copyright**. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el

artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

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

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

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

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

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

13. **LIMITACIÓN DE RESPONSABILIDAD**. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE LAS PÉRDIDAS DE BENEFICIOS, INGRESOS, VENTAS, DATOS O COSTES SOPORTADOS PARA OBTENER PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, CONDUCTA INADECUADA INTENCIONADA, NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA LA OCURRENCIA DE RESPONSABILIDAD, SOPORTADOS DEBIDO A LA UTILIZACIÓN O LA INCAPACIDAD DE UTILIZACIÓN DEL SOFTWARE, INCLUSO EN EL CASO DE QUE EL PROVEEDOR O SUS PROVEEDORES DE LICENCIAS HAYAN SIDO NOTIFICADOS DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

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

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

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

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

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

19. **Cumplimiento de las normas de control comercial**.

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

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen (en adelante, las "Leyes de control de las exportaciones") y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera

de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen (en adelante, las "Leyes sancionadoras").

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

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

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

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

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

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

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

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

EULA ID: BUS-STANDARD-20-01

Privacy Policy

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

- Procesamiento de datos personales

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

Procesamiento de datos personales

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

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Algoritmos hash unidireccionales relativos a infiltraciones que forman parte del sistema de reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones contra malware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.
- Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe
  - Oinfiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
  - Oinformación sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;
  - Oinformación relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;
  - Oarchivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

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

para prestar el servicio de asistencia técnica.

Confidencialidad de los datos

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

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

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

Derechos del titular de los datos.

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

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

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

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

dpo@eset.sk