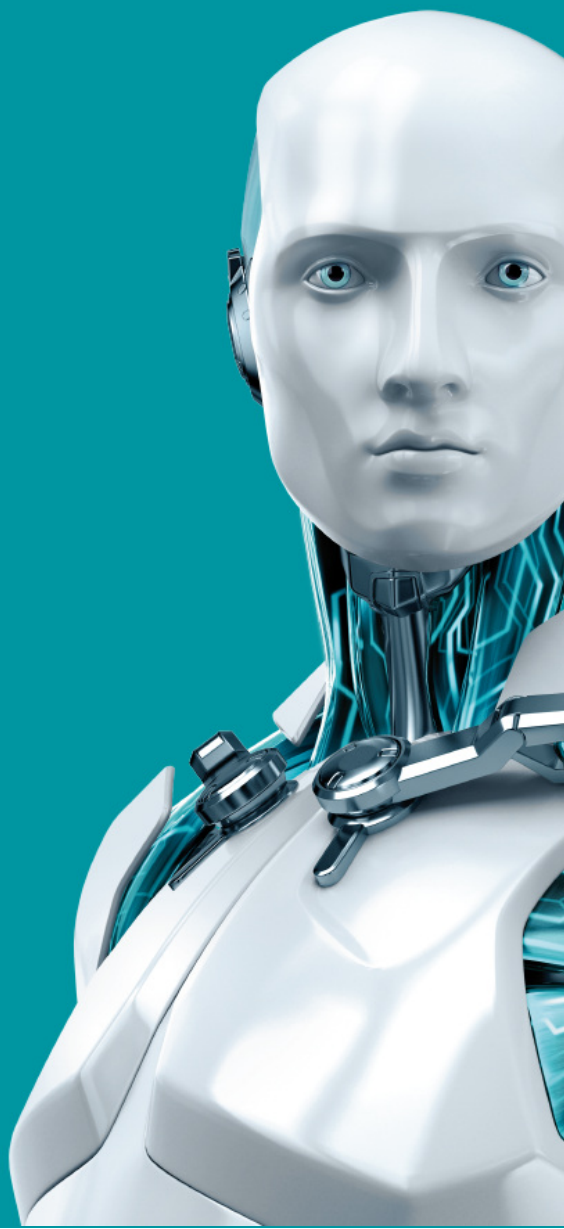
ENDPOINT ANTIVIRUS

FOR macOS

MANUAL DE USUARIO

(diseñada para la versión 6,5 o posterior del producto)

Haga clic aquí para descargar la versión más reciente de este documento



ENJOY SAFER TECHNOLOGY™

ENDPOINT ANTIVIRUS

Atención al cliente: www.eset.com/support

REV. 10/13/2017

Índice

1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 6 representa un nuevo enfoque de la seguridad informática realmente integrada. La versión más reciente del motor de análisis ThreatSense® 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 Antivirus 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 Remote Administrator 6, 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.

1.1 Novedades de la versión 6

La interfaz gráfica de usuario de ESET Endpoint Antivirus 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:

- **Protección del tráfico de Internet**: 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 Antivirus en segundo plano y suprime las ventajas emergentes y las tareas programadas.
- **Caché local compartida**: permite lograr mejoras en la velocidad de análisis en entornos virtualizados.

1.2 Requisitos del sistema

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

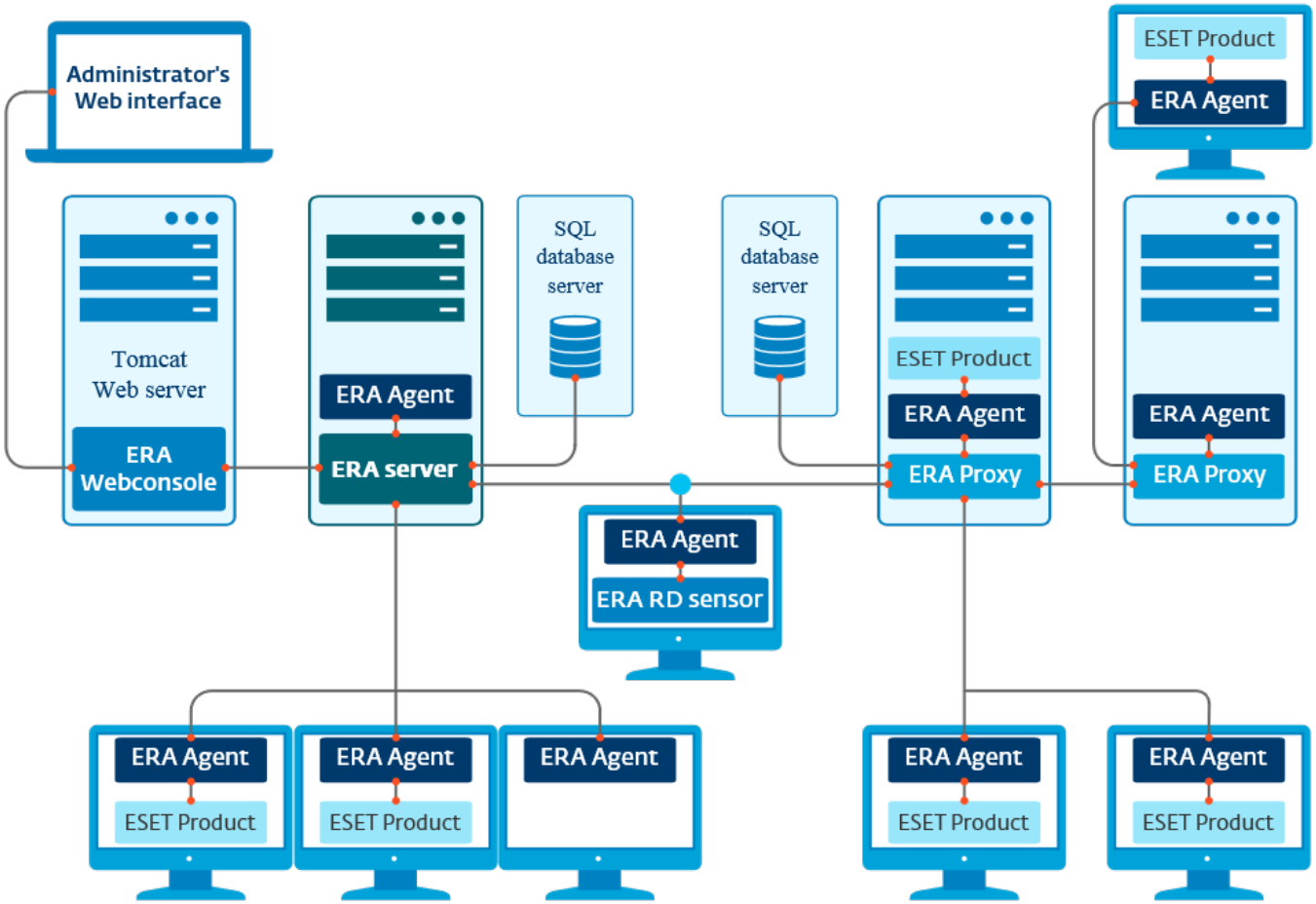
	Requisitos del sistema:
Arquitectura de procesador	Intel de 32 bits o 64 bits
Sistema operativo	macOS 10.9 y posterior macOS Server 10.7 y posterior
Memoria	300 MB
Espacio libre en disco	200 MB

2. Conexión de usuarios a través de ESET Remote Administrator

ESET Remote Administrator (ERA) 6 es una aplicación que le permite gestionar los productos de ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas de ESET Remote Administrator le permite instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y amenazas. ESET Remote Administrator no proporciona protección frente a código malicioso por sí solo, sino que confía en la presencia de soluciones de seguridad de ESET en cada cliente.

Las soluciones de seguridad de ESET son compatibles con redes que incluyan varios tipos de plataforma. Su red puede incluir una combinación de sistemas operativos actuales de Microsoft, Linux, macOS y sistemas operativos de dispositivos móviles (teléfonos móviles y tabletas).

En la imagen siguiente se muestra una arquitectura de ejemplo para una red protegida con soluciones de seguridad de ESET administradas mediante ERA:



NOTA: para obtener más información, consulte la documentación en línea de ESET Remote Administrator.

2.1 Servidor de ESET Remote Administrator

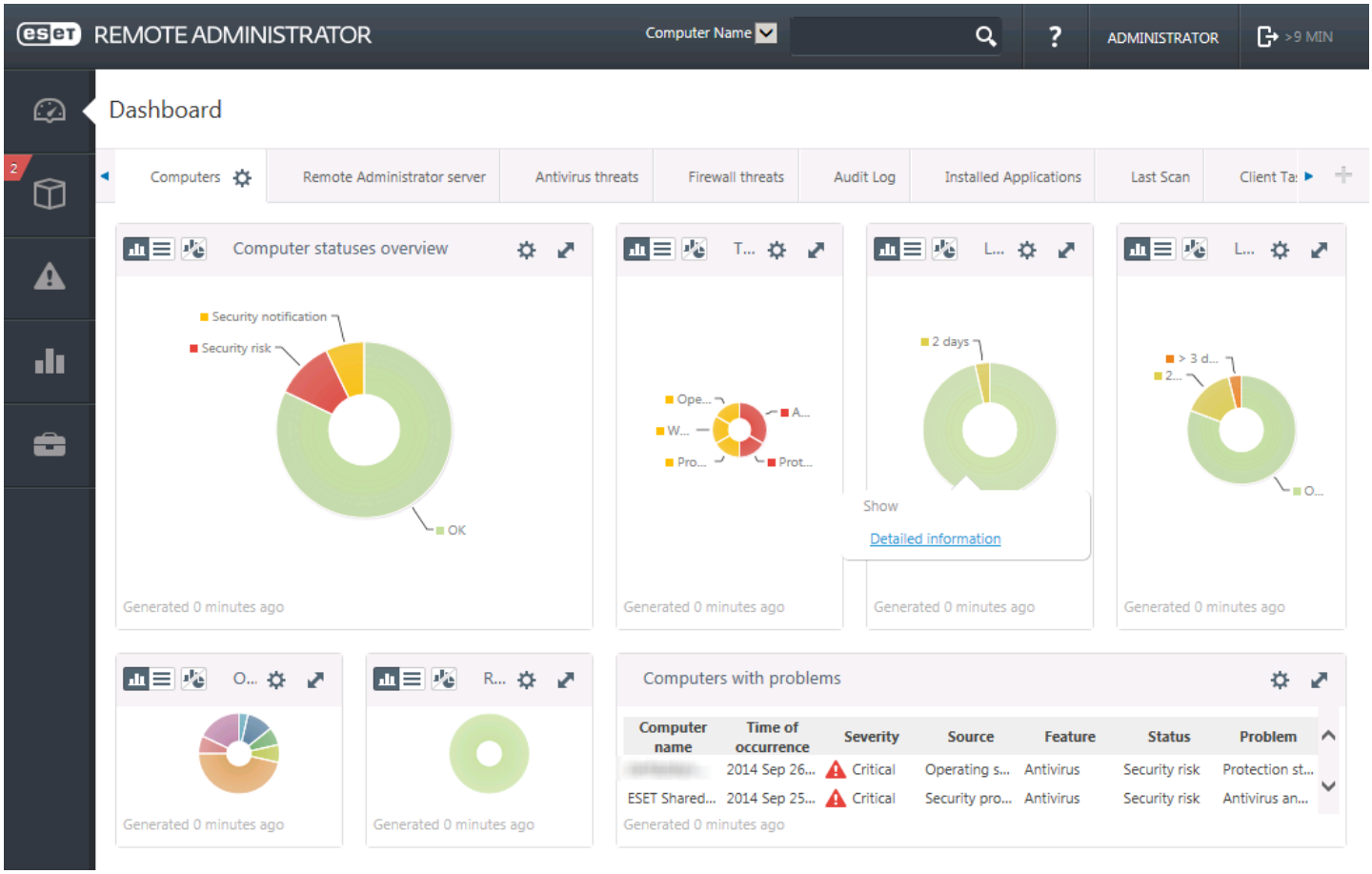
ESET Remote Administrator Server es el componente ejecutivo de ESET Remote Administrator. Procesa todos los datos recibidos de los clientes que se conectan al servidor (a través de ERA Agent 8). ERA Agent facilita la comunicación entre el cliente y el servidor. Los datos (registros de clientes, configuración, replicación del agente, etc.) se almacenan en una base de datos con fines de generación de informes.

ERA Server necesita una conexión estable a un servidor de bases de datos para procesar los datos correctamente. Le recomendamos que instale ERA Server y la base de datos en servidores diferentes para optimizar el rendimiento. El ordenador donde se instale ERA Server debe configurarse de modo que acepte todas las conexiones de agente, proxy y sensor RD, que se verifican mediante certificados. Una vez que haya instalado ERA Server, puede abrir ERA Web Console 7 para administrar las estaciones de trabajo de extremo que tienen soluciones de ESET instaladas.

2.2 Web Console

ERA Web Console es una interfaz web de usuario que presenta datos de ERA Server 6 y permite administrar las soluciones de seguridad ESET de su red. A Web Console se accede desde un navegador. Muestra información general del estado de los clientes en la red y se puede utilizar para implementar de forma remota soluciones de ESET en ordenadores no administrados. Puede hacer que el servidor web sea accesible desde Internet para permitir el uso de ESET Remote Administrator desde prácticamente cualquier lugar o dispositivo.

El tablero de Web Console:



La herramienta de **Búsqueda rápida** se encuentra en la parte superior de Web Console. Seleccione en el menú desplegable la opción **Nombre del ordenador**, **IPv4/Dirección IPv6** o **Nombre de la amenaza**, escriba la cadena de búsqueda en el campo de texto, y haga clic en el símbolo de la lupa o pulse **Intro** para buscar. Se abrirá la sección Grupos, en la que se muestran los resultados de la búsqueda.

2.3 Proxy

ERA Proxy es otro componente de ESET Remote Administrator que tiene dos funciones. En el caso de una red de tamaño mediano o de empresa con muchos clientes (por ejemplo, 10 000 clientes o más), puede utilizar ERA Proxy para distribuir la carga entre varios servidores ERA Proxy y así reducir la carga del ERA Server 6 principal. La otra ventaja de ERA Proxy es que lo puede utilizar cuando se conecta a una sucursal remota con un vínculo débil. Esto significa que el ERA Agent de cada cliente no se conecta directamente al ERA Server principal, sino que lo hace a través de ERA Proxy, situado en la misma red local de la sucursal. Esta configuración libera el vínculo de conexión con la sucursal. ERA Proxy acepta conexiones desde todos los ERA Agent locales, recoge sus datos y los carga al ERA Server principal (o a otro ERA Proxy). Esto permite que la red dé cabida a más clientes sin poner en peligro el rendimiento de la red y de las consultas a la base de datos.

Según la configuración de la red, es posible que un ERA Proxy se conecte a otro ERA Proxy y, después, se conecte al ERA Server principal.

Para que ERA Proxy funcione correctamente, el ordenador host donde se instale debe tener instalado un ESET Agent y estar conectado al nivel superior (ya sea un ERA Server o un ERA Proxy superior, si lo hay) de la red.

2.4 Agente

ERA Agent es un componente esencial de ESET Remote Administrator. Las soluciones de seguridad de ESET instaladas en ordenadores cliente (por ejemplo, ESET Endpoint Antivirus) se comunican con ERA Server a través del agente. Esta comunicación permite la administración de las soluciones de seguridad de ESET de todos los clientes remotos desde una ubicación central. El agente recopila información del cliente y la envía al servidor. Cuando el servidor envía una tarea al cliente, la tarea se envía al agente y este se comunica a continuación con el cliente. Toda la comunicación de la red tiene lugar entre el agente y la parte superior de la red de ERA (el servidor y el proxy).

El agente de ESET utiliza uno de estos tres métodos para conectarse al servidor:

1. El agente del cliente se conecta directamente al servidor.
2. El agente del cliente se conecta a través de un proxy que está conectado al servidor.
3. El agente del cliente se conecta al servidor a través de varios proxies.

El agente de ESET se comunica con las soluciones de ESET instaladas en un cliente, recopila información de los programas en dicho cliente y envía al cliente la información de configuración recibida del servidor.

NOTA: el proxy de ESET tiene su propio agente, que gestiona todas las tareas de comunicación entre clientes, otros proxies y el servidor.

2.5 Sensor RD

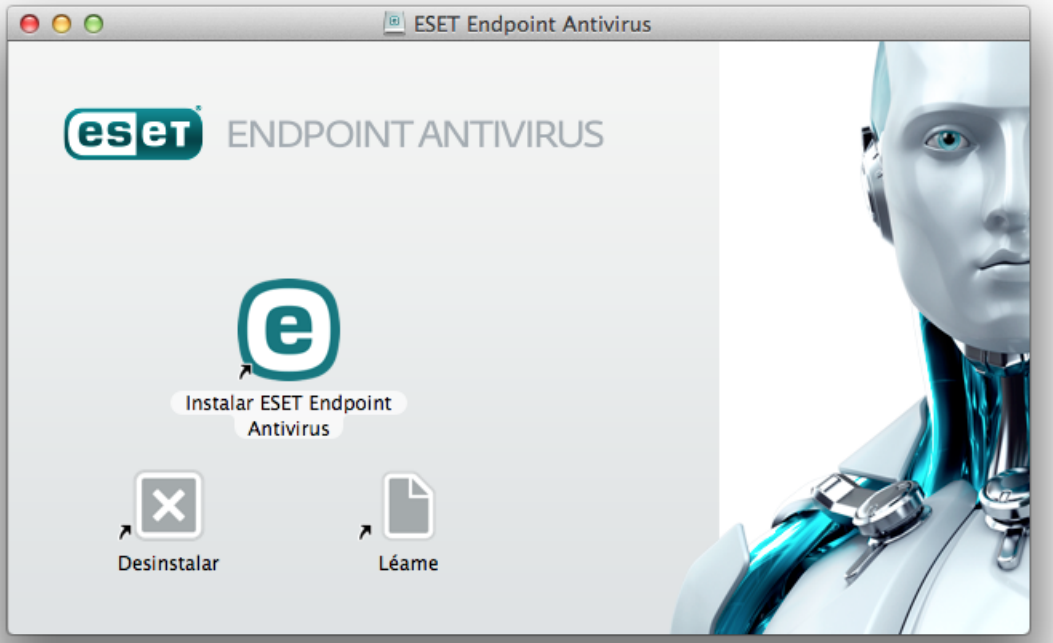
Sensor RD (Rogue Detection) es un componente de ESET Remote Administrator diseñado para localizar ordenadores en su red. Ofrece un método práctico para añadir ordenadores nuevos a ESET Remote Administrator sin tener que buscarlos y añadirlos manualmente. En Web Console se muestran todos los ordenadores detectados en la red, que se añaden al grupo Todos predeterminado. Desde aquí puede realizar otras acciones con los ordenadores clientes individuales.

RD Sensor es un oyente pasivo que detecta los ordenadores que están presentes en la red y envía información sobre ellos a ERA Server. ERA Server evalúa si los PC que se encuentran en la red son desconocidos o ya están administrados.

3. Instalación

El instalador de ESET Endpoint Antivirus puede ejecutarse de dos maneras:

- Si está instalando desde el CD/DVD de instalación, inserte el disco en la unidad de CD/DVD-ROM y haga doble clic en el icono de instalación de ESET Endpoint Antivirus para abrir el instalador.
- Si va a realizar la instalación desde un archivo descargado, haga doble clic en el archivo para iniciar el instalador.



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

Tras aceptar el acuerdo de licencia de usuario final, puede elegir entre las siguientes opciones de instalación:

- Instalación típica 9
- Instalación personalizada 10
- Instalación remota 11

3.1 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.

ESET Live Grid
El sistema de alerta temprana Live Grid de ESET contribuye a garantizar que ESET se mantiene informado de las nuevas amenazas de forma continua e inmediata para proteger rápidamente a nuestros clientes. El sistema permite que las nuevas amenazas se envíen al laboratorio de amenazas de ESET, donde se analizan y procesan. Haga clic en **Configuración** para modificar la configuración detallada para el envío de archivos sospechosos. Para obtener más información, consulte Live Grid 36.

Aplicaciones potencialmente indeseables
El último paso del proceso de instalación consiste en configurar la detección de **Aplicaciones potencialmente indeseables**. Estos programas no tienen por qué ser maliciosos, pero pueden influir negativamente en el comportamiento del sistema operativo. Estas aplicaciones suelen instalarse con otros programas y puede resultar difícil detectarlas durante la instalación. Aunque estas aplicaciones suelen mostrar una notificación durante la instalación, se pueden instalar fácilmente sin su consentimiento.

Después de instalar ESET Endpoint Antivirus, debe realizar un análisis del ordenador para comprobar si existe código malicioso. En la ventana principal del programa, haga clic en **Análisis del ordenador** y, a continuación, en **Análisis estándar**. Para obtener más información sobre los análisis del ordenador a petición, consulte el apartado Análisis del ordenador a petición 21.

3.2 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 Antivirus 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, puede definir ahora sus parámetros seleccionando **Conexión mediante servidor Proxy**. En la ventana siguiente, introduzca la dirección IP o la URL de su servidor proxy en el campo **Dirección**. En el campo Puerto, especifique el puerto 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
En el paso siguiente 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, a continuación, **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 Live Grid
El sistema de alerta temprana Live Grid de ESET contribuye a garantizar que ESET se mantiene informado de las nuevas amenazas de forma continua e inmediata para proteger rápidamente a nuestros clientes. El sistema permite que las nuevas amenazas se envíen al laboratorio de amenazas de ESET, donde se analizan y procesan. Haga clic en **Configuración** para modificar la configuración detallada del envío de archivos sospechosos. Para obtener más información, consulte Live Grid 36.

Aplicaciones potencialmente indeseables
El siguiente paso del proceso de instalación consiste en configurar la detección de **aplicaciones potencialmente indeseables**. Estos programas no tienen por qué ser maliciosos, pero pueden influir negativamente en el comportamiento del sistema operativo. Estas aplicaciones suelen instalarse con otros programas y puede resultar difícil detectarlas durante la instalación. Aunque estas aplicaciones suelen mostrar una notificación durante la instalación, se pueden instalar fácilmente sin su consentimiento.

Después de instalar ESET Endpoint Antivirus, debe realizar un análisis del ordenador para comprobar si existe código malicioso. En la ventana principal del programa, haga clic en **Análisis del ordenador** y, a continuación, en **Análisis estándar**. Para obtener más información sobre los análisis del ordenador a petición, consulte el apartado Análisis del ordenador a petición 21.

3.3 Instalación remota

La instalación remota le permite crear un paquete de instalación que se puede instalar en los ordenadores de destino por medio de software de escritorio remoto. Cuando la instalación concluye, ESET Endpoint Antivirus puede administrarse a través de ESET Remote Administrator.

La instalación remota consta de dos fases:
1. Creación del paquete de instalación remota con el instalador de ESET 11
2. Instalación remota con el software de escritorio remoto 12

Con la versión más reciente de ESET Remote Administrator 6 puede realizar la instalación remota también en ordenadores cliente con macOS. Siga los pasos que se describen en este artículo de la base de conocimientos para obtener información detallada. (Es posible que el artículo no esté disponible en su idioma).

3.3.1 Creación de un paquete de instalación remota

Componentes del programa
ESET Endpoint Antivirus 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, puede definir ahora sus parámetros seleccionando **Conexión mediante servidor Proxy**. En la ventana siguiente, introduzca la dirección IP o la URL de su servidor proxy en el campo **Dirección**. En el campo Puerto, especifique el puerto 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
En el paso siguiente 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, a continuación, **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 Live Grid
El sistema de alerta temprana Live Grid de ESET contribuye a garantizar que ESET se mantiene informado de las nuevas amenazas de forma continua e inmediata para proteger rápidamente a nuestros clientes. El sistema permite que las nuevas amenazas se envíen al laboratorio de amenazas de ESET, donde se analizan y procesan. Haga clic en **Configuración** para modificar la configuración detallada del envío de archivos sospechosos. Para obtener más información, consulte Live Grid 36.

Aplicaciones potencialmente indeseables
El siguiente paso del proceso de instalación consiste en configurar la detección de **aplicaciones potencialmente indeseables**. Estos programas no tienen por qué ser maliciosos, pero pueden influir negativamente en el comportamiento del sistema operativo. Estas aplicaciones suelen instalarse con otros programas y puede resultar difícil detectarlas durante la instalación. Aunque estas aplicaciones suelen mostrar una notificación durante la instalación, se pueden instalar fácilmente sin su consentimiento.

Archivos de instalación remota
En el último paso del asistente de instalación, seleccione una carpeta de destino para el paquete de instalación (esets_remote_Install.pkg), el script shell de configuración (esets_setup.sh) y el script shell de desinstalación (esets_remote_UnInstall.sh).

3.3.2 Instalación remota en ordenadores de destino

ESET Endpoint Antivirus se puede instalar en los ordenadores de destino con Apple Remote Desktop o cualquier otra herramienta que permita la instalación de paquetes macOS estándar (.pkg); para realizar la instalación, se copian los archivos en los ordenadores de destino y se ejecutan los scripts shell.

Para instalar ESET Endpoint Antivirus con Apple Remote Desktop:

1. Haga clic en el icono **Copy** (Copiar) de Apple Remote Desktop.
2. Haga clic en **+**, desplácese hasta el script shell de instalación (esets_setup.sh) y selecciónelo.
3. Seleccione **/tmp** en el menú desplegable **Place items in** (Colocar elementos en) y haga clic en **Copy** (Copiar).
4. Haga clic en **Install** (Instalar) para enviar el paquete a los ordenadores de destino.

Para obtener instrucciones detalladas sobre la administración de ordenadores cliente con ESET Remote Administrator, consulte la documentación en línea de ESET Remote Administrator.

3.3.3 Desinstalación remota

Para desinstalar ESET Endpoint Antivirus de los ordenadores cliente:

1. Utilice el comando **Copy Items** de Apple Remote Desktop, localice el script shell de desinstalación (*esets_remote_unInstall.sh*, creado con el paquete de instalación) y cópielo en el directorio /tmp de los ordenadores de destino (por ejemplo */tmp/esets_remote_uninstall.sh*).
2. En **Run command as** (Ejecutar comando como), seleccione User (Usuario) y escriba **root** en el campo **User** (Usuario).
3. Haga clic en **Send** (Enviar). Tras la desinstalación, se mostrará un registro de la consola.

3.3.4 Actualización remota

Utilice el comando **Install packages** (Instalar paquetes) de Apple Remote Desktop para instalar la versión más reciente de ESET Endpoint Antivirus cuando haya una nueva versión disponible.

4. 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 Antivirus directamente desde el programa, haga clic en el icono de ESET Endpoint Antivirus 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 Antivirus:

- **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 entonos 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.

NOTA: ESET Remote Administrator puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador.

ESET Endpoint Antivirus 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 Antivirus o registrado en el administrador de licencias de ESET. El comando devolverá el estado "OK" o un error si se produce un error en la activación.

5. Desinstalación

Hay varias formas de iniciar el programa de desinstalación de ESET Endpoint Antivirus:

- Inserte el CD/DVD de instalación de ESET Endpoint Antivirus en el ordenador, ábralo desde el escritorio o la ventana del **Finder** y haga doble clic en **Desinstalar**.
- Abra el archivo de instalación de ESET Endpoint Antivirus (*.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 Antivirus** y seleccione la opción **Mostrar contenido del paquete**. Abra la carpeta **Contents** > **Helpers** y haga doble clic en el icono **Uninstaller**.

6. Información general básica

La ventana principal del programa ESET Endpoint Antivirus está dividida en dos apartados 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 la protección**: contiene información sobre el estado de protección del ordenador, la web y el correo electrónico.
- **Análisis del ordenador**: este apartado le permite configurar e iniciar el análisis del ordenador a petición 21.
- **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 32, Planificador de tareas 34, Cuarentena 37, Procesos en ejecución 39 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.

6.1 Accesos directos del teclado

ESET Endpoint Antivirus es compatible con los siguientes accesos directos del teclado:

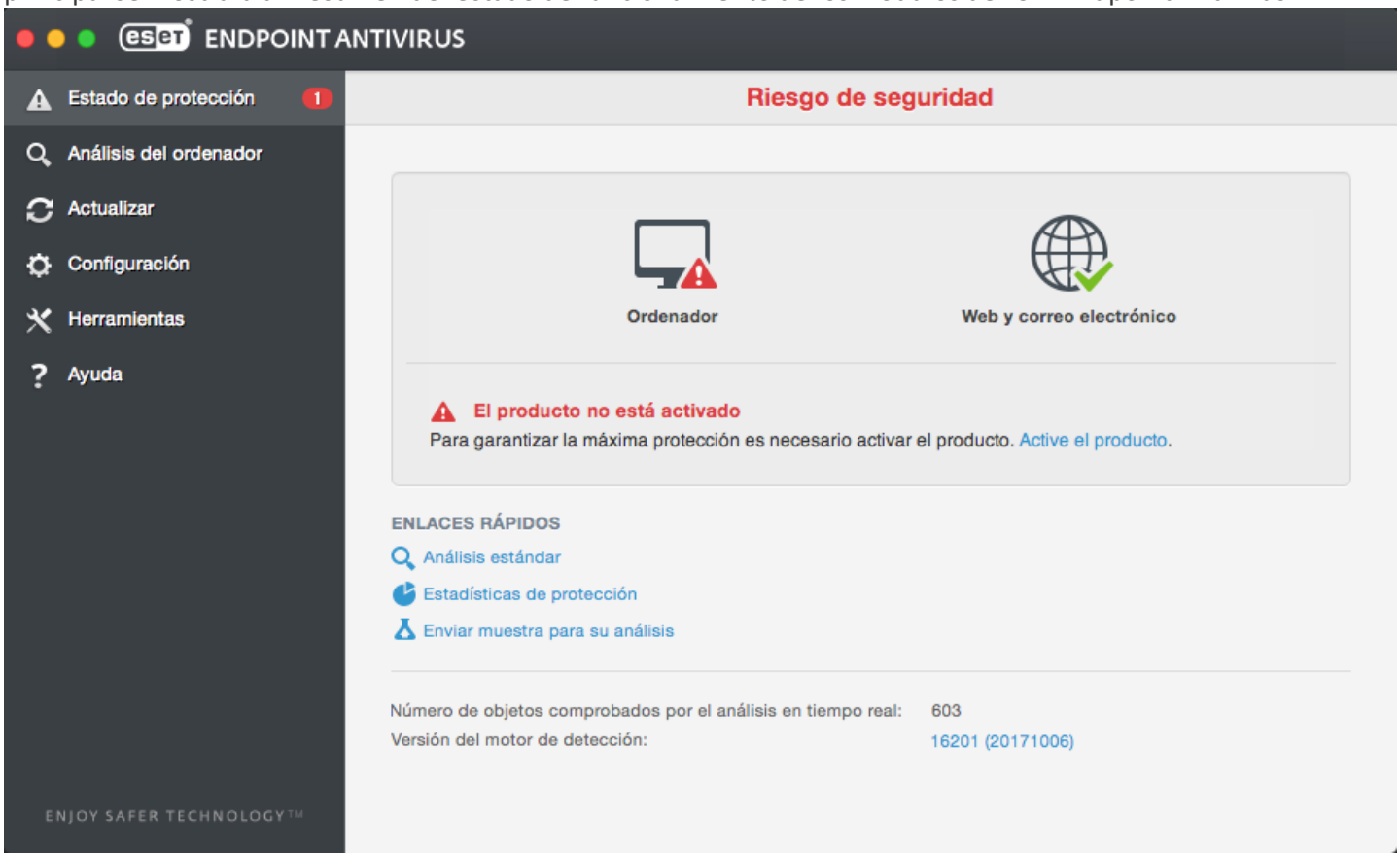
- *cmd+,*: muestra las preferencias de ESET Endpoint Antivirus.
- *cmd+O*: restaura el tamaño predeterminado de la ventana principal de la GUI de ESET Endpoint Antivirus y la mueve al centro de la pantalla.
- *cmd+Q*: oculta la ventana principal de la GUI de ESET Endpoint Antivirus. Se puede abrir haciendo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

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 el apartado **Archivos de registro**.
- *cmd+alt+S*: abre el apartado **Planificador de tareas**.
- *cmd+alt+Q*: abre el apartado **Cuarentena**.

6.2 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 Antivirus.



6.3 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 Antivirus.

7. 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**.

7.1 Protección antivirus y antiespía

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

7.1.1 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 19, haga clic en **Configuración**.

7.1.1.1 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 archivo en la estructura de árbol.
- [−]: elimina las entradas seleccionadas.
- **Predeterminado**: cancela todas las exclusiones.

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

7.1.2 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 23.

7.1.3 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 23), 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 Antivirus, 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**: unidades de disco duro del sistema.
- **Medios extraíbles**: CD y DVD, soportes USB, dispositivos Bluetooth, etc.
- **Medios de red**: todas las unidades asignadas.

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

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 20).

7.1.3.1 Opciones avanzadas

En esta ventana puede definir los tipos de objeto que analiza el motor de 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 de ThreatSense 24.

Se recomienda no realizar cambios en el apartado **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 Live Grid 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.

7.1.3.2 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 Antivirus, 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**).

7.1.3.3 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 Remote Administrator, 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 Antivirus instalada en el ordenador cliente
- fecha y versión del motor de detección
- ruta al servidor de actualización

NOTA: solo se recomienda el uso de Terminal a usuarios avanzados.

7.1.3.4 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.

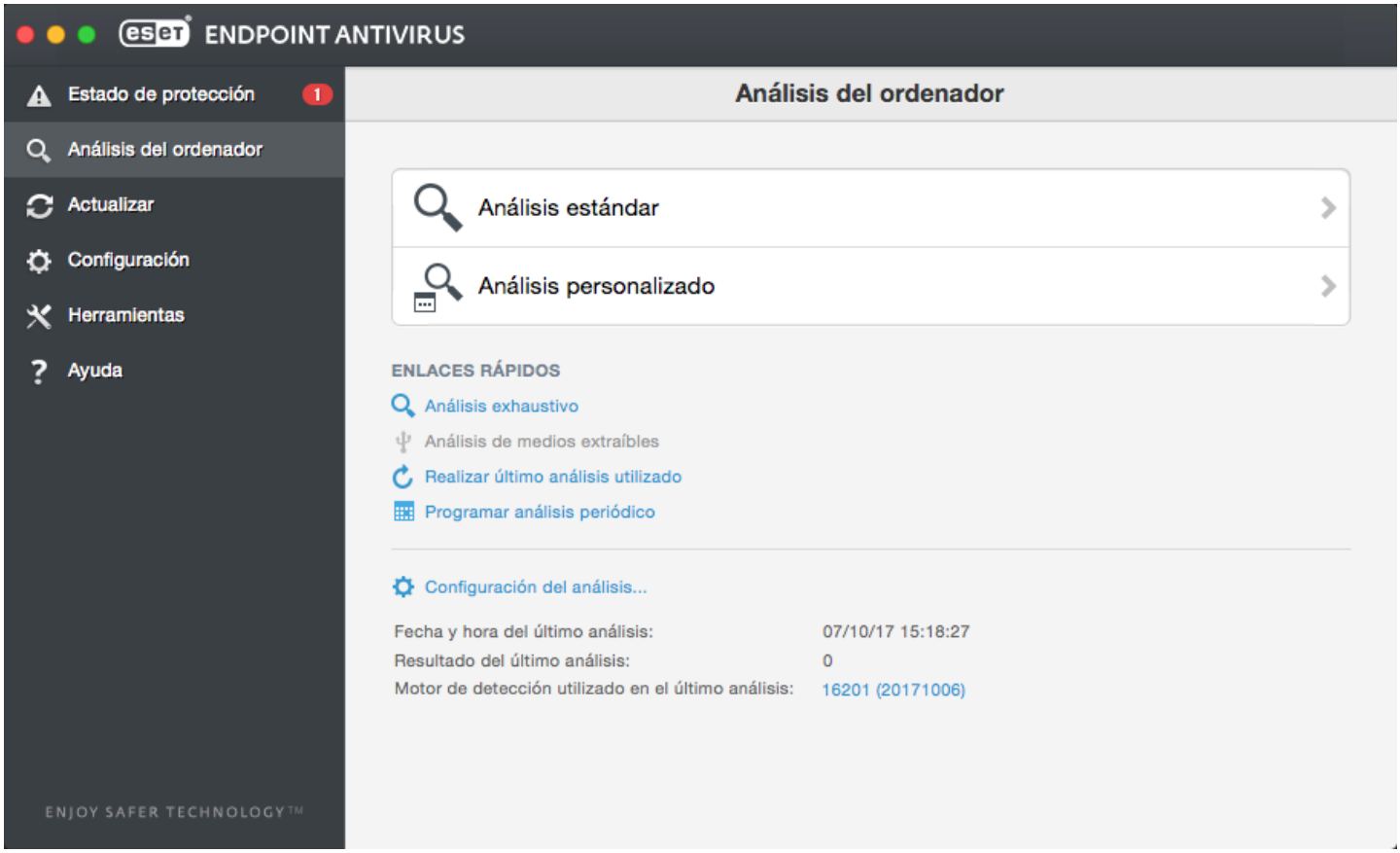
La protección en tiempo real está desactivada
Si un usuario desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para volver a activar la protección en tiempo real, diríjase al menú principal, haga clic en **Configuración** > **Ordenador** y establezca **Protección del 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 tiene instalados otros programas antivirus en el ordenador. Si están activadas dos protecciones en tiempo real al mismo tiempo, estas 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.

7.1.4 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 Antivirus, 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*).

7.1.4.1 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.

7.1.4.1.1 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 25.

7.1.4.1.2 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 de análisis** específicos que desee en la estructura de árbol. Los objetos de análisis también se pueden especificar con más precisión introduciendo 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 haciendo clic en **Configuración...** > **Desinfección**.

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

7.1.4.2 Objetos del análisis

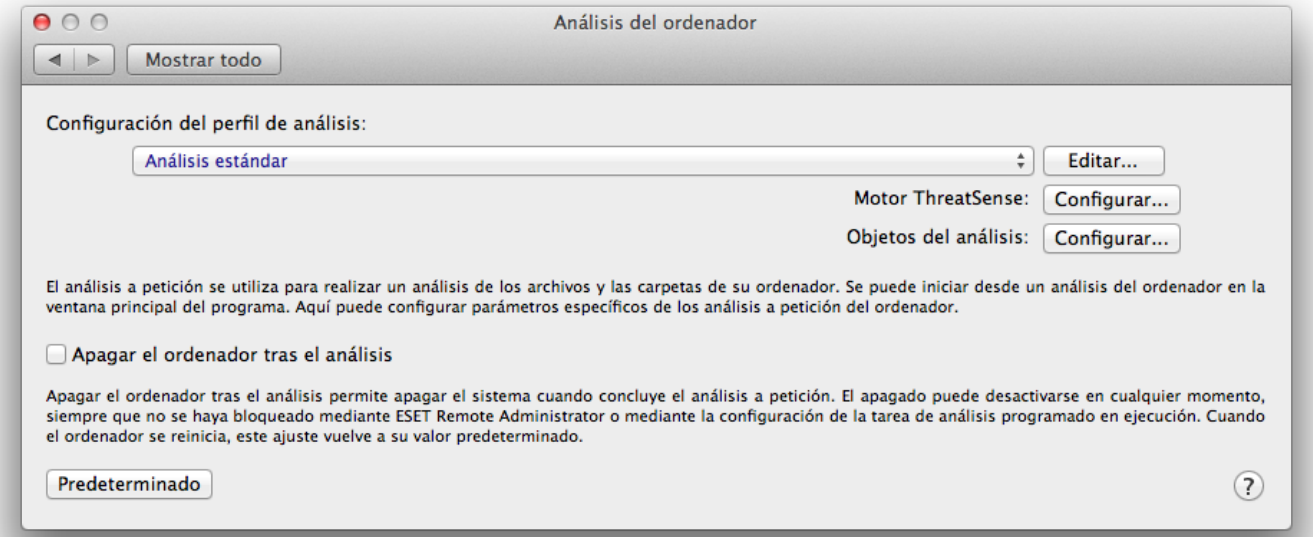
La estructura de árbol de objetos del análisis le permite seleccionar los archivos y carpetas que se analizarán en busca de virus. Las carpetas también se pueden seleccionar según la configuración de un perfil.

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.

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



Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte el apartado Configuración de parámetros del motor ThreatSense 23 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**.

7.1.5 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 del 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 en tiempo real del sistema de archivos, el sistema podría ralentizarse. Por este motivo, se recomienda que no modifique los parámetros predeterminados de ThreatSense en ningún módulo, a excepción de Análisis del ordenador.

7.1.5.1 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 provocar 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 conocimiento.
- **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 convencionales, los empaquetadores en tiempo real se descomprimen en la memoria. Cuando se activa esta opción también se analizan los empaquetadores estáticos estándares (como UPX, yoda, ASPack, FGS).

7.1.5.2 Opciones

En el apartado **Opciones** se pueden seleccionar los métodos utilizados durante un análisis del sistema. Están disponibles las siguientes opciones:

- **Heurística**: la heurística emplea un algoritmo que analiza la actividad (malintencionada) de los programas. La ventaja principal de la detección heurística es la capacidad de detectar nuevo software malintencionado 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 bastante superior gracias a la tecnología heurística avanzada.

7.1.5.3 Desinfección

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

- **Sin desinfección**: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción.
- **Desinfección estándar** : el programa intentará desinfectar o eliminar los archivos infectados de manera automática. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrecerá una selección de acciones que seguir. La selección de acciones que seguir también aparecerá si no se puede completar una acción predefinida.
- **Desinfección exhaustiva**: el programa desinfectará o eliminará todos los archivos infectados (incluidos los archivos comprimidos). La única excepción la constituyen 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.

Advertencia: en el modo de desinfección predeterminado (Desinfección estándar), solamente se elimina el archivo comprimido 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.

7.1.5.4 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 este apartado de la configuración de parámetros de ThreatSense es posible definir los tipos de archivos que se desean 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, por ejemplo, cuando el análisis de ciertos tipos de archivos impide que el programa funcione de forma correcta. 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

7.1.5.5 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. Se recomienda no modificar el valor predeterminado de 10; en circunstancias normales, no debería haber motivo para ello. 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.

7.1.5.6 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 Antivirus mediante actualizaciones periódicas. Si la Optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo de ThreatSense del módulo donde se realice el análisis.

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.

7.1.6 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 22).
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 Antivirus, 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.

7.2 Protección de web y correo electrónico

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

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

7.2.1 Protección del tráfico de Internet

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 puede lograrse definiendo los números de puerto para la comunicación HTTP 27 o las direcciones URL 27.

7.2.1.1 Puertos

En la ficha **Puertos** puede definir el número de puertos utilizados para la comunicación HTTP. De forma predeterminada, los números de puerto 80, 8080 y 3128 ya están definidos.

7.2.1.2 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.

7.2.2 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, el programa 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 es conveniente confiar a ciegas en los mensajes con etiquetas, ya que pueden omitirse en mensajes HTML problemáticos o ser falsificadas por algunos virus. Están disponibles las siguientes opciones:

- **Nunca**: no se agregará ningún mensaje de etiqueta.
- **Solo al correo electrónico infectado**: únicamente se marcarán como analizados los mensajes que contengan software malintencionado.
- **A todos los correos electrónicos analizados**: el programa agregará mensajes 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: edite esta plantilla para modificar el formato del prefijo del asunto de un mensaje infectado.

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

- Comprobación del protocolo POP3 28
- Comprobación del protocolo IMAP 29

7.2.2.1 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 Antivirus 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.

7.2.2.2 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 Antivirus 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.

7.3 Anti-Phishing

El término *phishing* define una actividad delictiva que usa la ingeniería social (manipulación de usuarios para obtener información confidencial). Con frecuencia se utiliza para obtener datos confidenciales como números de cuentas bancarias, de tarjetas de crédito, códigos PIN, o nombres de usuario y contraseñas.

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

8. Control de dispositivos

ESET Endpoint Antivirus 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 opción puede resultar útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

Dispositivos externos admitidos:
- Almacenamiento en disco (unidad de disco duro, 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 Antivirus en **Herramientas** > **Archivos de registro** 32.

8.1 Editor de reglas

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

Al hacer clic en **Activar el control de dispositivos** se activa la función de control de dispositivos de ESET Endpoint Antivirus. 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 Antivirus 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

Escriba la 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.

NOTA: 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 del control de dispositivos 32.

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.
Alerta: registra errores graves y mensajes de alerta.
Ninguno: no se registra nada.

Lista de usuarios

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios agregándolos a la lista de usuarios:
Modificar...: 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.

NOTA: 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).

9. Herramientas

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

9.1 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 Antivirus, donde también se pueden archivar registros.

Se puede acceder a los archivos de registro desde el menú principal de ESET Endpoint Antivirus 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 Antivirus 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. **Sitios web filtrados**: esta lista es útil si desea ver una lista de sitios web bloqueados por Protección del acceso a la Web 27. 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.

9.1.1 Mantenimiento de registros

La configuración de registros de ESET Endpoint Antivirus 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: Editar**: le permite guardar registros con la siguiente información:

- Sucesos como *Nombre de usuario y contraseña no válidos*, *No se pueden actualizar los módulos*, etc. se escriben 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

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 33.

9.1.2 Filtrado de registros

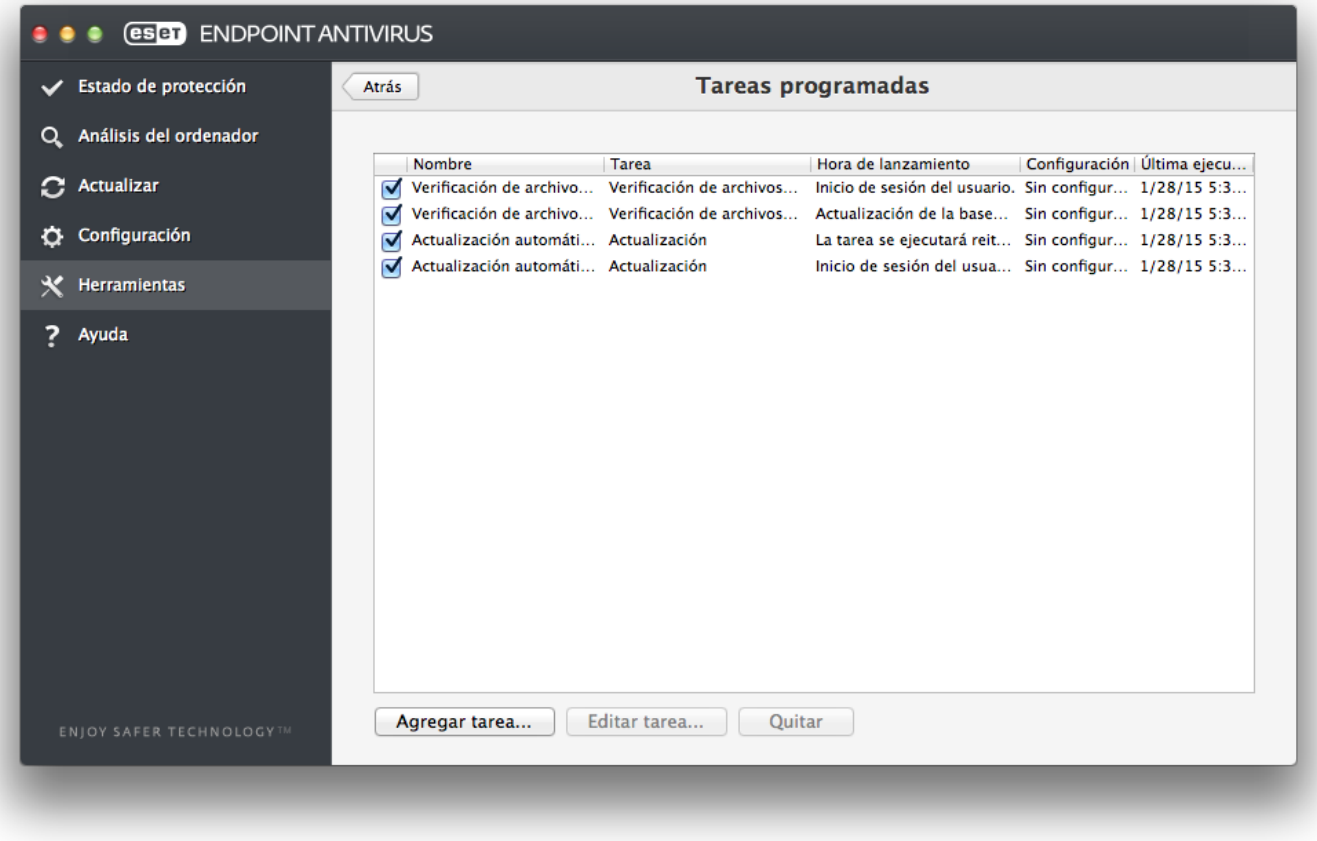
Los registros guardan información sobre sucesos importantes del sistema. La función de filtrado de registros permite ver los registros de sucesos determinados.

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.

9.2 Tareas programadas

La opción **Tareas programadas** está disponible en el menú principal de ESET Endpoint Antivirus, 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 el 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...**.

9.2.1 Creación de tareas nuevas

Para crear una nueva tarea en el Planificador de tareas, haga clic en **Agregar tarea** o haga Ctrl + clic en el espacio en blanco y seleccione **Agregar** en el menú contextual. Existen cinco tipos de tareas programadas disponibles:

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

NOTA: si selecciona **Ejecutar aplicación**, puede ejecutar programas como un usuario del sistema llamado "nadie". Los permisos para la ejecución de aplicaciones a través del Planificador de tareas vienen definidos por macOS.

En el ejemplo siguiente se utiliza el Planificador de tareas para añadir una nueva tarea de actualización, dado que esta es una de las tareas programadas más frecuentes:

1. Seleccione **Actualización** en el menú desplegable **Tarea programad**.
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 la 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 35).
4. En el siguiente paso, defina la acción que deba llevarse a cabo 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 Antivirus contiene tareas programadas predefinidas para garantizar el correcto funcionamiento del producto. Estas tareas no se deben modificar, por lo que están ocultas de forma predeterminada. Para que estas tareas estén visibles, diríjase al menú principal, haga clic en **Configuración** > **Introducir preferencias de aplicación** > **Tareas programadas** y seleccione **Mostrar tareas de sistema**.

9.2.2 Creación de una tarea definida 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)
```

Por 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 diagonal (`/`): define los incrementos de los rangos; por ejemplo, `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).

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

9.3 Live Grid

El sistema de alerta temprana Live Grid informa a ESET de las nuevas amenazas de forma inmediata y continua. El sistema de alerta temprana Live Grid bidireccional tiene un único objetivo: mejorar la protección que le ofrecemos. La mejor manera de garantizar la detección de nuevas amenazas en cuanto aparecen es "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 Live Grid:

1. Puede optar por no activar el sistema de alerta temprana Live Grid. El software no perderá funcionalidad, pero en algunos casos ESET Endpoint Antivirus puede responder más rápido a nuevas amenazas que una actualización de los módulos de detección.
2. Puede configurar el sistema de alerta temprana Live Grid para que envíe información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso. Esta información se puede enviar a ESET para que realice un análisis detallado. El 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 Live Grid recopilará información acerca de su ordenador que esté relacionada con amenazas detectadas recientemente. Esta información puede incluir una muestra o una copia del archivo en el que haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la fecha y la hora, el proceso mediante el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

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

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

9.3.1 Archivos sospechosos

De forma predeterminada, ESET Endpoint Antivirus 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** > **Live Grid** > **Configuración**).

Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio para su análisis. Para ello, haga clic en **Herramientas** > **Enviar archivo para su análisis** 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 alerta temprana ESET Live Grid 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.

A continuación se muestra un ejemplo de paquete de información estadística enviado:

```
# 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.

9.4 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 Antivirus 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 Antivirus. Los archivos en cuarentena se guardan en un formato cifrado seguro y se pueden restaurar tras la instalación de ESET Endpoint Antivirus.

9.4.1 Poner archivos en cuarentena

ESET Endpoint Antivirus 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 Antivirus - Agregar archivos a la carpeta Cuarentena para enviar el archivo a cuarentena.

9.4.2 Restauración de un archivo en 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.

9.4.3 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.

9.5 Privilegios

La configuración de ESET Endpoint Antivirus 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**.

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

9.6 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 Antivirus se volverá naranja y mostrará un signo de alerta.

9.7 Procesos en ejecución

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

- **Proceso**: nombre del proceso que se está ejecutando actualmente en el ordenador. 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 Antivirus y la tecnología ESET Live Grid asignan un nivel de riesgo a los objetos (archivos, procesos, etc.) mediante una serie de reglas heurísticas que examinan las características de cada uno de ellos y, después, estiman el potencial de actividad maliciosa. De acuerdo con esta heurística, se asigna un nivel de riesgo a los diferentes objetos. Las aplicaciones conocidas marcadas en verde son totalmente seguras (incluidas en lista blanca) y 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 Live Grid se encarga de recopilar esta información.
- **Hora de la detección**: periodo de tiempo transcurrido desde que la tecnología ESET Live Grid 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.

10. 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 Antivirus 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 Antivirus en el Dock del macOS, así como alternar ESET Endpoint Antivirus y otras aplicaciones en ejecución pulsando *cmd+tab*. Los cambios se aplican tras reiniciar ESET Endpoint Antivirus (normalmente se activa con el reinicio del sistema).
- **Utilizar menú estándar** le permite utilizar determinados accesos directos del teclado (consulte Accesos directos del teclado 16) 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 Antivirus.
- **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 Antivirus 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 Antivirus (normalmente se activa con el reinicio del sistema).

10.1 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 Antivirus.

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 40.

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

Desde la versión 6.2 de ESET Endpoint Antivirus puede impedir que determinados **Estados de protección** se muestren en la pantalla principal del programa (ventana **Estado de protección**). Para obtener más información sobre esta cuestión, consulte el apartado Estados de protección 41.

10.1.1 Mostrar alertas

ESET Endpoint Antivirus 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 la opción **No volver a mostrar este cuadro de diálogo** para suprimir cada notificación por separado.

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 Antivirus. Para activar o suprimir cada notificación, active la casilla de verificación que aparece a la izquierda del **Nombre del cuadro de diálogo**. También puede definir las **Condiciones de visualización** bajo las que se mostrarán las notificaciones sobre nuevas actualizaciones del dispositivo y el sistema operativo.

10.1.2 Estados de protección

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

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

- Anti-Phishing
- Protección del tráfico de Internet
- Protección del cliente de correo electrónico
- Modo Presentación
- Actualización del sistema operativo
- Caducidad de la licencia
- Es necesario reiniciar el ordenador

10.2 Menú contextual

Para que las funciones de ESET Endpoint Antivirus 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.

11. Actualización

Es necesario actualizar ESET Endpoint Antivirus 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.

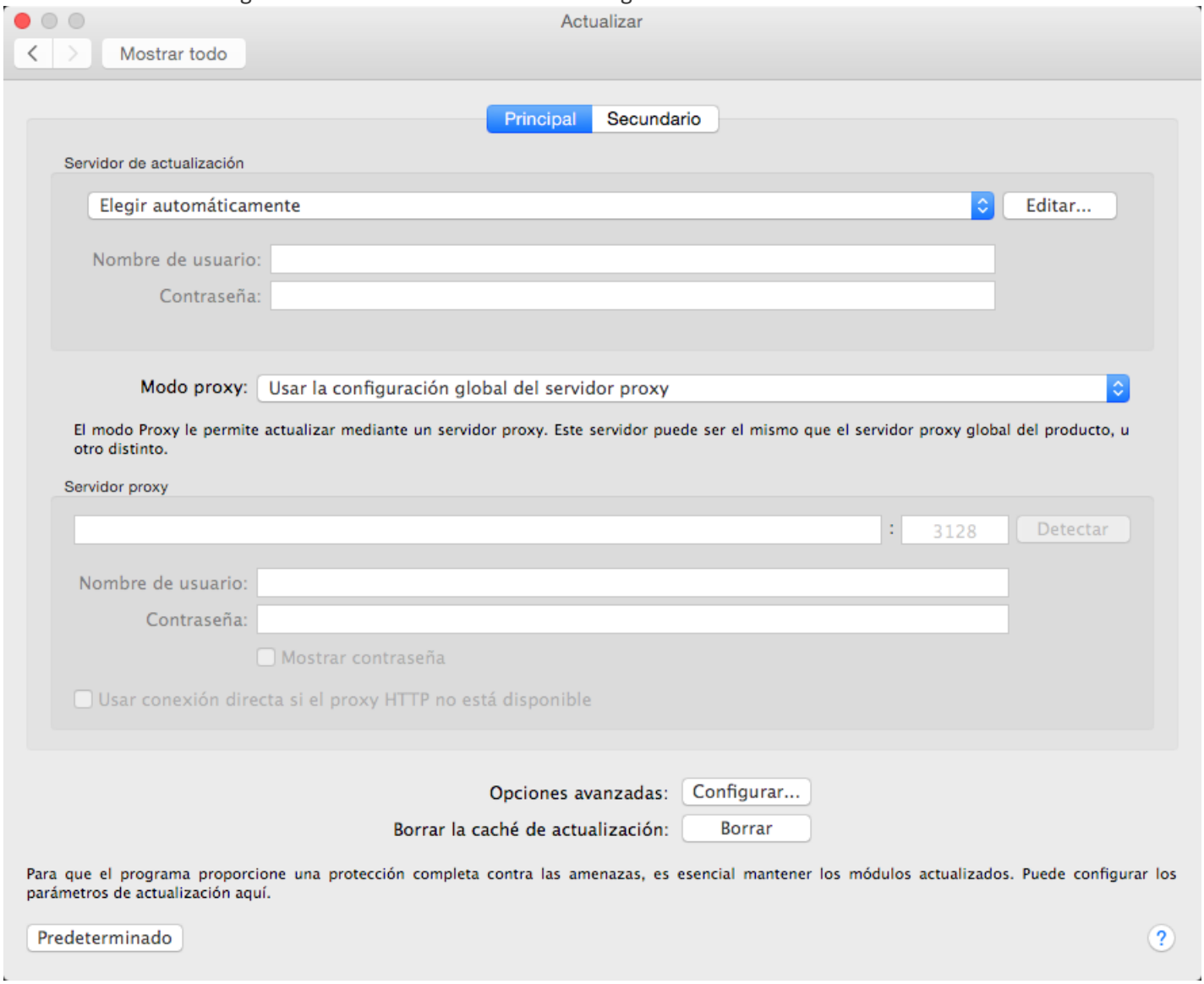
Haga clic en **Actualización** en el menú principal para comprobar el estado de la actualización actual, incluidas la fecha y la hora de la última actualización, y compruebe si es necesario actualizar el programa. Haga clic en **Actualizar módulos** para iniciar el proceso de actualización manualmente.

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 42; el motivo más habitual de este error es introducir incorrectamente los datos de licencia 13 o la configuración de conexión 46.

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.

11.1 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 Antivirus 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 el servidor de actualización secundario, ni el nombre de usuario y la 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 Antivirus elija automáticamente el mejor servidor de actualización para utilizarlo.

Modo proxy le permite actualizar los módulos de detección utilizando 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 46.

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 Antivirus 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 Antivirus detecta la configuración del proxy a partir de las Preferencias del Sistema de macOS. La configuración puede definirse en macOS desde > **Preferencias del Sistema** > **Red** > **Avanzado** > **Proxies**.

Si activa **Usar conexión directa si el proxy HTTP no está disponible**, ESET Endpoint Antivirus 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.

11.1.1 Opciones avanzadas

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

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 Antivirus 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 Antivirus 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.

11.2 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 Antivirus:

- **Actualización automática de rutina**
- **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 34.

11.3 Actualización a una nueva compilación

Utilice la compilación más reciente de ESET Endpoint Antivirus para disfrutar de la máxima protección posible. Para buscar una versión nueva, haga clic en **Actualizar** en el menú principal de la izquierda. Si está disponible una nueva compilación, se mostrará una notificación en la parte inferior de la ventana. Haga clic en **Más información** para abrir una ventana nueva con el número de versión de la nueva compilación y el registro de cambios.

Al hacer clic en **Descargar** el archivo se guarda en la carpeta de descargas (o la carpeta predeterminada que indique el navegador). Cuando finalice la descarga, abra el archivo y siga las instrucciones de instalación. La información de la licencia se transferirá automáticamente a la nueva instalación.

Se recomienda comprobar periódicamente si hay actualizaciones disponibles, especialmente cuando ESET Endpoint Antivirus se instala desde un CD/DVD.

11.4 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 Antivirus 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 Antivirus 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.

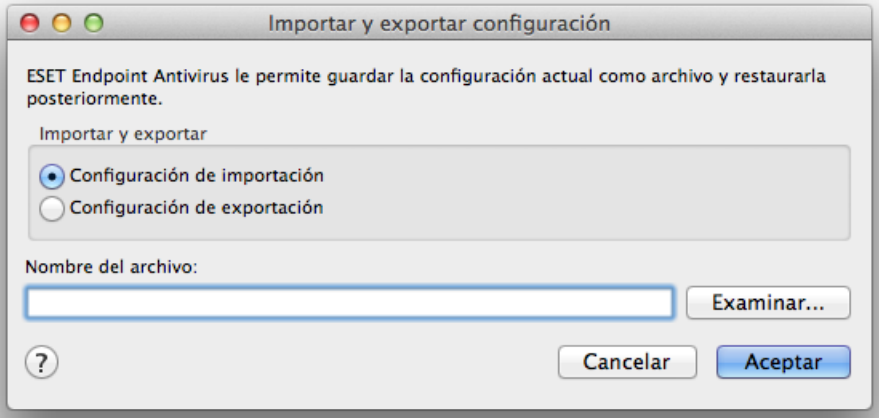
En la ventana de notificación se muestran las actualizaciones recuperadas mediante la herramienta de la línea de comandos "softwareupdate". Las actualizaciones recuperadas con esta herramienta varían en función de las actualizaciones que muestra la aplicación "Actualizaciones de Software". Si desea instalar 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**. Esta opción solo se recomienda a usuarios avanzados.

12. Varios

12.1 Importar y exportar configuración

Si desea importar una configuración existente o exportar la configuración de ESET Endpoint Antivirus, 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 Antivirus y utilizarlas más adelante. Exportar configuración también es útil para los usuarios que desean utilizar su configuración preferida de ESET Endpoint Antivirus 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.

12.2 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 Antivirus. Los parámetros definidos aquí los utilizarán todos los módulos que necesiten conexión a Internet. ESET Endpoint Antivirus 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.

12.3 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 Antivirus 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).

NOTA: 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).