ESET Smart Security 4

Guía del usuario

Microsoft® Windows® Vista / XP / 2000 / 2003 / 2008

we protect your digital worlds

ESET Smart Security 4

Servicio de atención al cliente mundial: www.eset.eu/support
Servicio de atención al cliente en Norteamérica: www.eset.com/support

REV.20090123-001

Índice

1. ESET Smart Security 4

ESET Smart Security 4 es el primer representante del nuevo enfoque hacia la seguridad informática plenamente integrada. Utiliza la velocidad y la precisión del antivirus ESET NOD32, garantizadas gracias a la versión más reciente del motor de análisis ThreatSense®, junto con el cortafuegos personal personalizado y los módulos contra correo no deseado. El resultado es un sistema inteligente que está constantemente en alerta frente a ataques y software malintencionado que puedan poner en peligro su equipo.

ESET Smart Security no es un burdo conglomerado de varios productos en un paquete, como ofrecen otros proveedores. Es el resultado de un esfuerzo a largo plazo para combinar la máxima protección con el mínimo de impacto en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial son capaces de eliminar proactivamente la penetración de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques que proceden de Internet sin entorpecer el rendimiento del sistema ni perturbar el equipo.

1.1 Novedades

La experiencia de desarrollo a largo plazo de nuestros expertos se demuestra mediante la arquitectura completamente nueva del programa ESET Smart Security, que garantiza la detección máxima con unos requisitos del sistema mínimos. La compleja solución de seguridad contiene módulos con varias opciones avanzadas. La siguiente lista ofrece una breve descripción general de estos módulos.

- **Antivirus y antiespía**

Este módulo se basa en el núcleo de análisis ThreatSense®, que se utilizó por primera vez en el galardonado sistema antivirus NOD 32. El núcleo ThreatSense® se ha optimizado y mejorado con la nueva arquitectura de ESET Smart Security.

Característica	Descripción
Desinfección mejorada	El sistema antivirus desinfecta y elimina de forma inteligente la mayoría de las amenazas detectadas sin requerir la intervención del usuario.
Modo de análisis en segundo plano	El análisis del equipo se puede iniciar en segundo plano sin ralentizar el rendimiento.
Archivos de actualización más pequeños	Los procesos de optimización del núcleo generan archivos de actualización de menor tamaño que en la versión 2.7. Además, se ha mejorado la protección de los archivos de actualización contra daños.
Protección de los clientes de correo más conocidos	Ahora es posible analizar el correo entrante no sólo en MS Outlook, sino también en Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird.
Diversas mejoras secundarias	– Acceso directo a sistemas de archivos para lograr una gran velocidad y un excelente rendimiento. – Bloqueo del acceso a los archivos infectados. – Optimización para el Centro de seguridad de Windows, incluido Vista.

- **Cortafuegos personal**

El cortafuegos personal supervisa todo el tráfico entre un equipo protegido y otros equipos de la red. El cortafuegos personal de ESET contiene las funciones avanzadas indicadas en la siguiente lista.

Característica	Descripción
Análisis de comunicación de red de capa baja	El análisis de comunicación de red en la capa del vínculo de datos permite al cortafuegos personal de ESET superar una serie de ataques que, de otra forma, no se podrían detectar.
Compatibilidad con IPv6	El cortafuegos personal de ESET muestra las direcciones IPv6 y permite a los usuarios crear reglas para ellas.
Supervisión de archivos ejecutables	Supervisión de los cambios en los archivos ejecutables para superar la infección. Se puede permitir la modificación de archivos de aplicaciones firmadas.
Análisis de archivos integrado con HTTP y POP3	Análisis de archivos integrado en los protocolos de aplicación HTTP y POP3. Los usuarios estarán protegidos cuando naveguen por Internet o descarguen mensajes de correo electrónico.
Sistema de detección de intrusiones	Capacidad para reconocer el carácter de la comunicación de red y diversos tipos de ataques de red y una opción para prohibir automáticamente dicha comunicación.
Compatibilidad con los modos automático, de aprendizaje, basado en las directrices, interactivo y automático con excepciones.	Los usuarios pueden seleccionar si las acciones del cortafuegos se ejecutarán automáticamente o si desean establecer reglas interactivamente. La comunicación en el modo basado en las directrices se administra según las reglas definidas por el usuario o por el administrador de red. En el modo de aprendizaje, se pueden crear y guardar automáticamente las reglas; este modo se recomienda para la configuración inicial del cortafuegos.
Sustitución del cortafuegos de Windows integrado	Sustituye al cortafuegos de Windows integrado y también interactúa con el Centro de seguridad de Windows de modo que el usuario siempre está informado sobre su estado de seguridad. La instalación de ESET Smart Security desactiva el cortafuegos de Windows de forma predeterminada.

- **Contra correo no deseado**

El módulo contra correo no deseado de ESET filtra el correo electrónico no solicitado y, por tanto, aumenta la seguridad y la comodidad de la comunicación electrónica.

Característica	Descripción
Puntuación del correo entrante	Se asigna una puntuación a todo el correo entrante, que va desde 0 (mensaje que no es correo no deseado) hasta 100 (mensaje que es correo no deseado) y se transfiere en función de la misma a la carpeta de la papelera o a una carpeta personalizada creada por el usuario. Se puede realizar un análisis paralelo de los mensajes de correo electrónico entrantes.
Compatibilidad con una serie de técnicas de análisis	– Análisis Bayesiano – Análisis basado en reglas – Comprobación global de la base de datos de huellas
Plena integración con los clientes de correo electrónico	La protección contra correo no deseado está disponible para los usuarios de los clientes Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird.
Posibilidad de seleccionar manualmente el correo no deseado	Existe una opción para seleccionar/deseleccionar manualmente un mensaje de correo electrónico como correo no deseado.

1.2 Requisitos del sistema

Para un funcionamiento óptimo de ESET Smart Security y ESET Smart Security Business Edition, el sistema debe cumplir los siguientes requisitos de hardware y software:

ESET Smart Security:

Windows 2000 o XP	400 MHz 32 bits/64 bits (x86/x64) 128 MB de RAM de memoria del sistema 35 MB de espacio disponible Super VGA (800 × 600)
Windows Vista	1 GHz 32 bits/64 bits (x86/x64) 512 MB de RAM de memoria del sistema 35 MB de espacio disponible Super VGA (800 × 600)

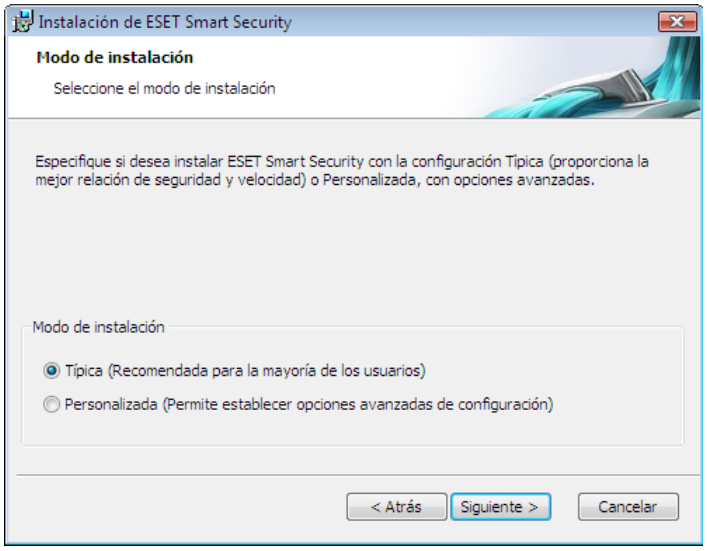
ESET Smart Security Business Edition:

Windows 2000, 2000 Server, XP o 2003 Server	400 MHz 32 bits/64 bits (x86/x64) 128 MB de RAM de memoria del sistema 35 MB de espacio disponible Super VGA (800 × 600)
Windows Vista o Windows Server 2008	1 GHz 32 bits/64 bits (x86/x64) 512 MB de RAM de memoria del sistema 35 MB de espacio disponible Super VGA (800 × 600)

2. Instalación

Tras la compra, se puede descargar el instalador de ESET Smart Security del sitio web de ESET. Viene como paquete ess_nt**_***.msi (ESET Smart Security) o essbe_nt**_***.msi (ESET Smart Security Business Edition). Ejecute el instalador; el asistente de instalación le proporcionará instrucciones para realizar la configuración básica. Existen dos tipos de instalación disponibles con distintos niveles de detalles de configuración:

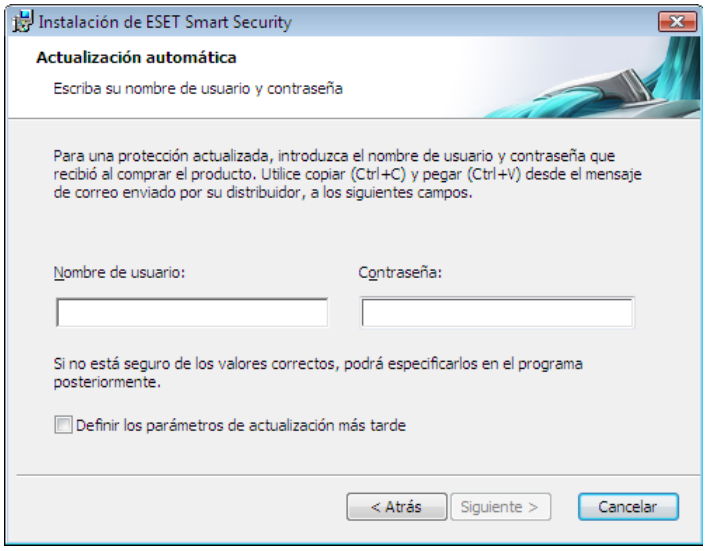
1. Instalación típica
2. Instalación personalizada



2.1 Instalación típica

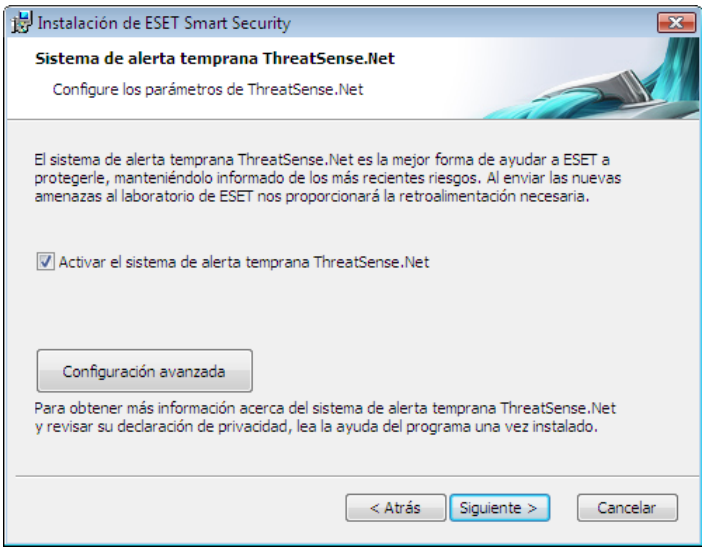
La instalación típica se recomienda para usuarios que deseen instalar ESET Smart Security con la configuración predeterminada, que proporciona el máximo nivel de protección, aspecto que valoran los usuarios que no desean realizar una configuración detallada.

El primer (y muy importante) paso es escribir el nombre de usuario y la contraseña para la actualización automática del programa. Esta tarea desempeña una función muy significativa que proporciona la protección constante del sistema.



Escriba su **Nombre de usuario** y **Contraseña**, es decir, los datos de autentificación que haya recibido tras la adquisición o el registro del producto en los campos correspondientes. Si no dispone actualmente de su nombre de usuario y contraseña, seleccione la opción **Definir Usuario y Contraseña más tarde**. Los datos de autentificación se pueden introducir más adelante en cualquier momento, directamente desde el programa.

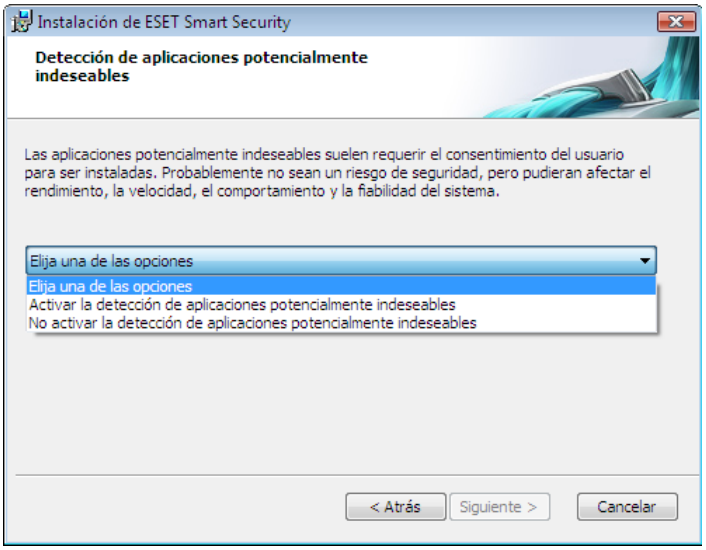
El paso siguiente de la instalación es la configuración del sistema de alerta temprana ThreatSense.Net. El sistema de alerta temprana ThreatSense.Net ayuda a garantizar que ESET se mantenga informado de forma continua e inmediata acerca de las nuevas amenazas con el fin de proteger rápidamente a sus clientes. El sistema permite el envío de nuevas amenazas al laboratorio de virus de ESET, en el que se analizan, procesan y agregan a las bases de firmas de virus.



De forma predeterminada, está seleccionada la casilla de verificación **Activar el sistema de alerta temprana ThreatSense.Net**, que activará esta función. Haga clic en **Configuración avanzada** para modificar la configuración detallada del envío de archivos sospechosos.

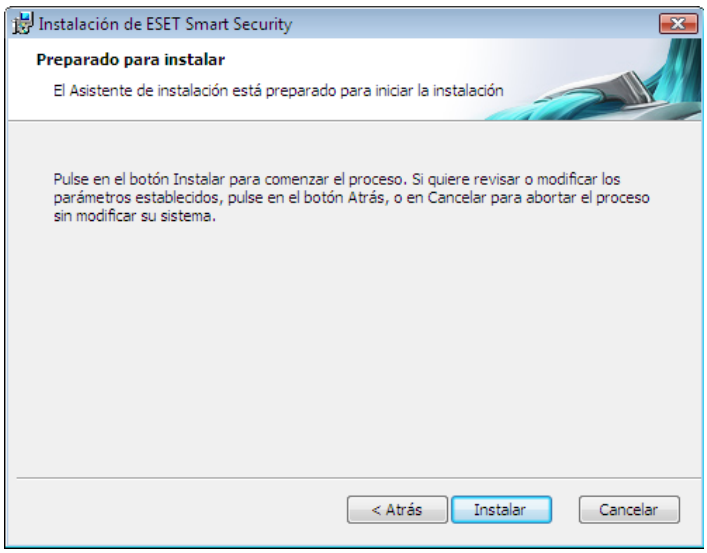
El paso siguiente del proceso de instalación es configurar la **Detección de aplicaciones potencialmente indeseables**. Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden influir negativamente en el comportamiento del sistema operativo.

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.



Active la opción **Activar la detección de aplicaciones potencialmente indeseables** para permitir que ESET Smart Security detecte este tipo de amenaza (recomendado).

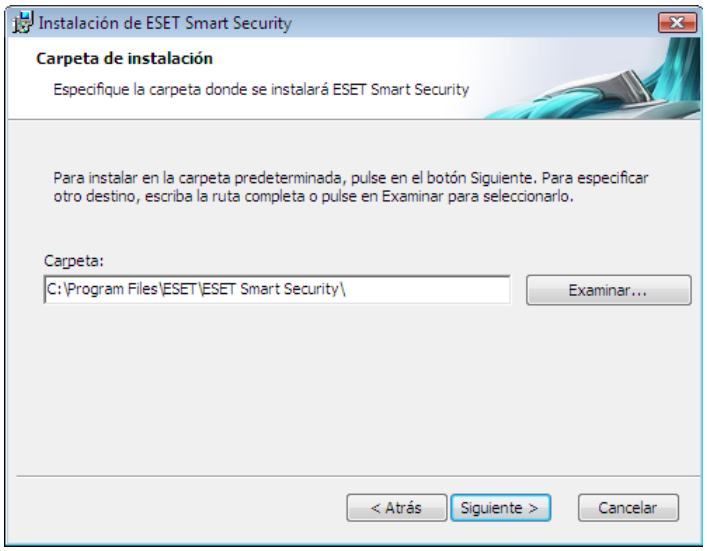
El último paso de la instalación típica es la confirmación de la instalación, para lo que debe hacer clic en el botón **Instalar**.



2.2 Instalación personalizada

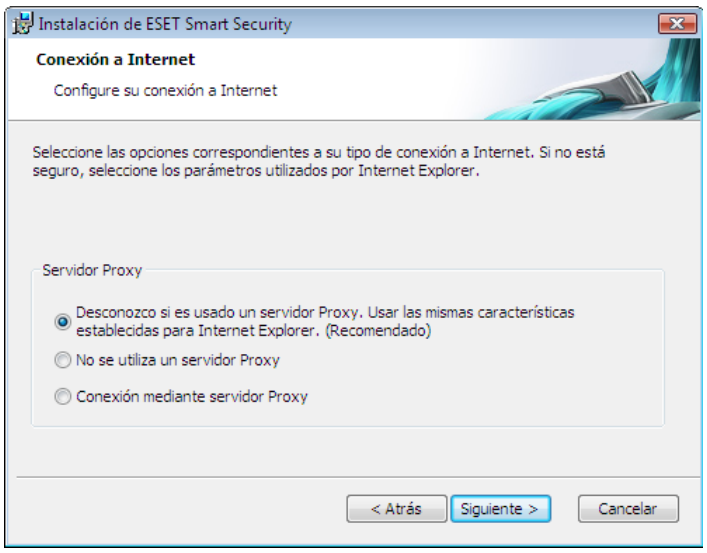
La instalación **personalizada** está diseñada para usuarios que tienen experiencia a la hora de ajustar programas y que desean modificar opciones avanzadas durante la instalación.

El primer paso es seleccionar la ubicación de destino para la instalación. De forma predeterminada, el programa se instala en la carpeta C:\Archivos de programa\ESET\ESET Smart Security\. Haga clic en **Examinar...** para cambiar la ubicación (no recomendado).

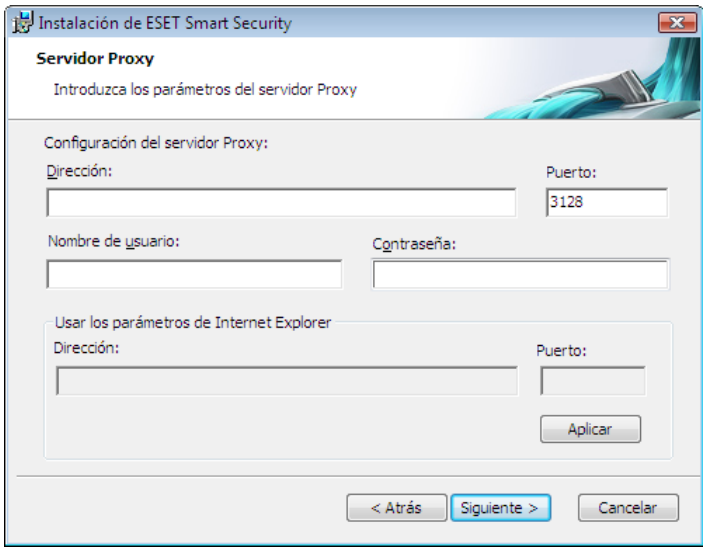


A continuación, **escriba su nombre de usuario y contraseña**. Este paso es el mismo que en la Instalación típica (consulte la página 5).

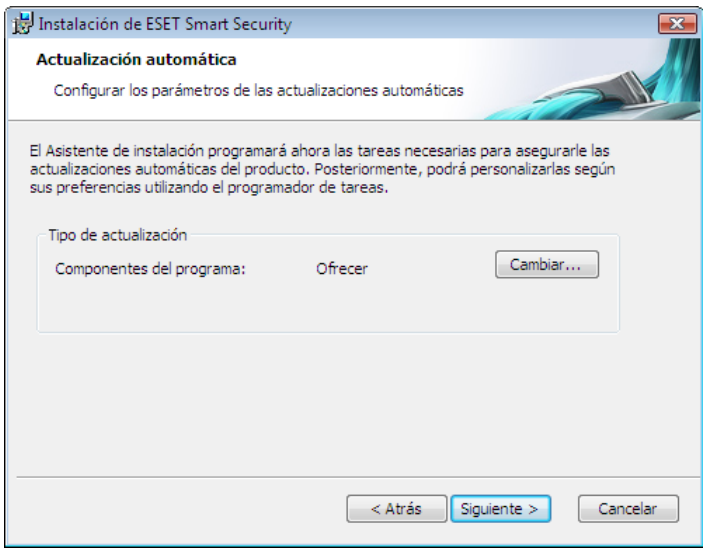
Una vez introducido su nombre de usuario y contraseña, haga clic en **Siguiente** para **Configurar su conexión a Internet**.



Si utiliza un servidor Proxy, éste debe estar correctamente configurado para que las actualizaciones de firmas de virus funcionen de forma adecuada. Si no está seguro de si utiliza un servidor Proxy para conectarse a Internet, deje la opción predeterminada **Desconozco si es usado un servidor Proxy. Usar las mismas características establecidas para Internet Explorer** y haga clic en **Siguiente**. Si no utiliza un servidor Proxy, seleccione la opción correspondiente.

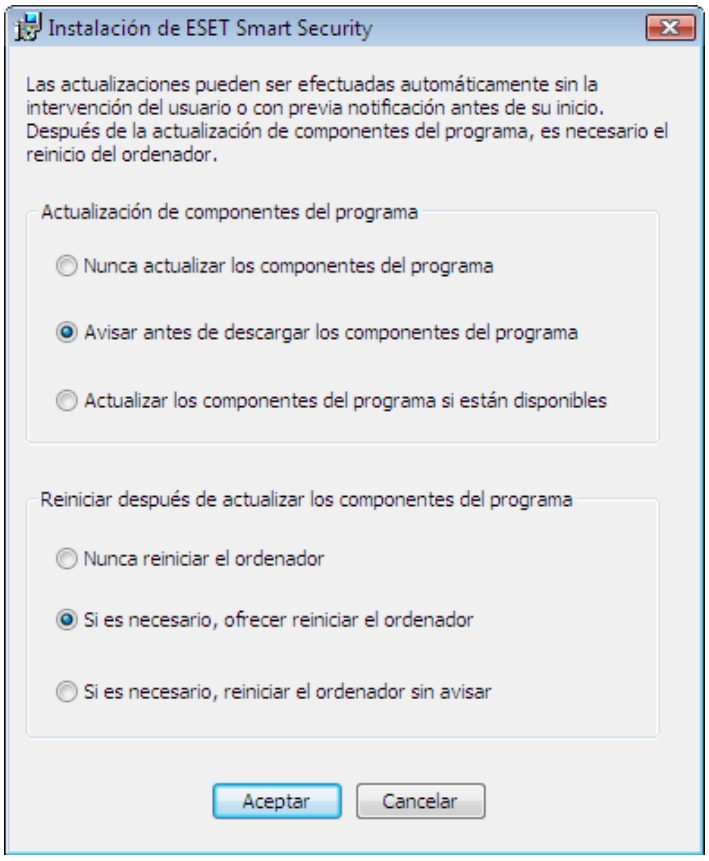


Para configurar su servidor Proxy, seleccione **Conexión mediante servidor Proxy** y haga clic en **Siguiente**. Introduzca la dirección IP o URL de su servidor Proxy en el **campo Dirección.** La opción **Puerto** permite especificar el puerto en el que el servidor Proxy acepta las conexiones (3128 de forma predeterminada). En el caso de que el servidor Proxy requiera autentificación, debe introducir un nombre de usuario y una contraseña válidos que permitan obtener acceso al servidor Proxy. La configuración del servidor Proxy también se puede copiar de Internet Explorer si lo desea. Para ello, haga clic en **Aplicar** y confirme la selección.



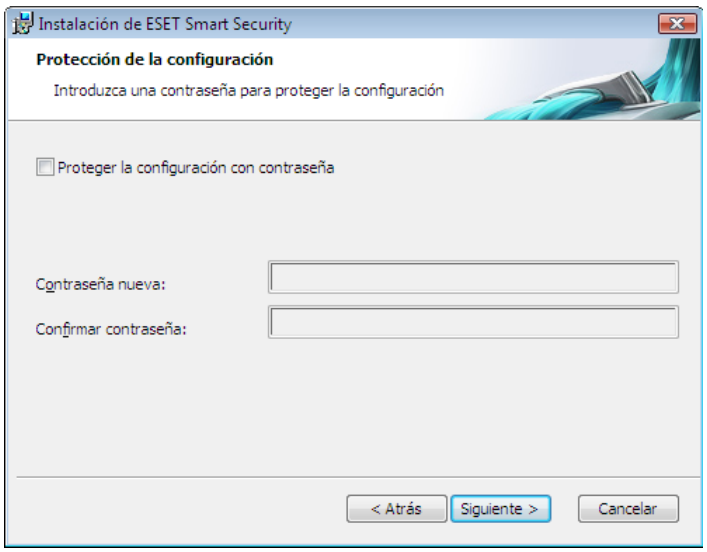
Haga clic en **Siguiente** para pasar a la ventana **Configurar los parámetros de las actualizaciones automáticas**. Este paso permite designar cómo se administrarán las actualizaciones automáticas de componentes del programa en su sistema. Haga clic en **Cambiar...** para obtener acceso a la configuración avanzada.

Si no desea que se actualicen los componentes del programa, seleccione **Nunca actualizar los componentes del programa**. Al activar la opción **Avisar antes de descargar los componentes del programa** aparecerá una ventana de confirmación antes de descargar los componentes del programa. Para activar la actualización automática de componentes del programa sin preguntar, seleccione la opción **Actualizar los componentes del programa si están disponibles**.



NOTA: tras una actualización de componentes del programa, suele ser necesario reiniciar el equipo. La configuración recomendada es: **Si es necesario, reiniciar el ordenador sin avisar**.

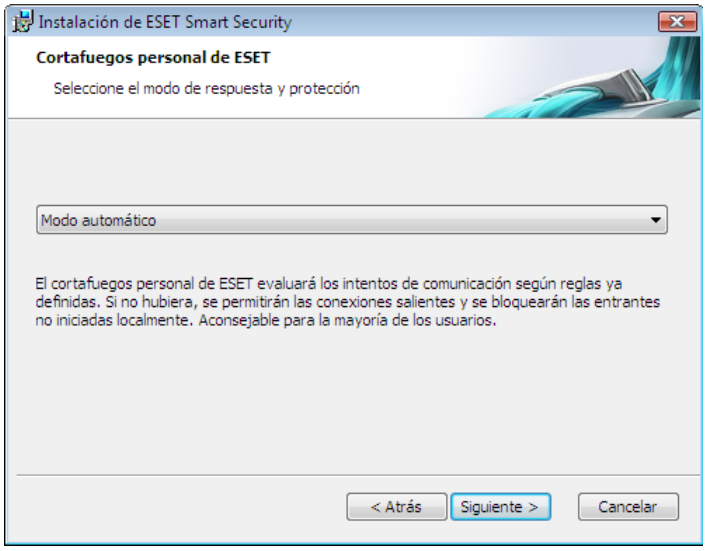
El siguiente paso de la instalación es introducir una contraseña para proteger los parámetros del programa. Elija la contraseña con la que desee proteger el programa. Vuelva a escribir la contraseña para confirmarla.



Los pasos **Activar el sistema de alerta temprana ThreatSense.Net** y **Detección de aplicaciones potencialmente indeseables** son los mismos que en la instalación típica y no se indican aquí (consulte la página 5).

El último paso del modo de instalación personalizada es seleccionar el modo de filtro del cortafuegos personal de ESET. Dispone de cinco modos:

- Automático
- Automático con excepciones (reglas definidas por el usuario)
- Interactivo
- Basado en las directrices
- Aprendizaje



Automático es aconsejable para la mayoría de los usuarios. Todas las conexiones salientes estándar están activadas (analizadas automáticamente mediante la configuración predefinida). Las conexiones entrantes no solicitadas se bloquean automáticamente.

Modo automático con excepciones (reglas definidas por el usuario). Como complemento del modo automático, le permite agregar reglas personalizadas.

Interactivo se recomienda para usuarios avanzados. Las comunicaciones se administran mediante reglas definidas por el usuario. Si no existe una regla definida para una comunicación, el programa pregunta al usuario si desea permitir o denegar la comunicación.

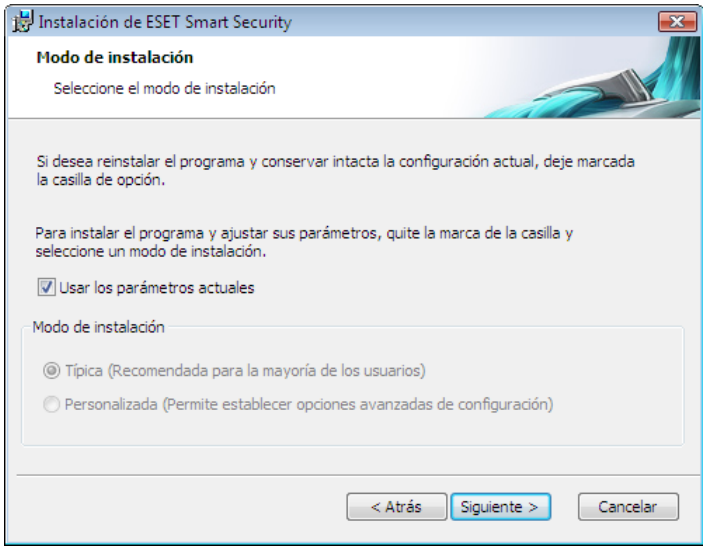
Basado en las directrices analiza las comunicaciones basadas en reglas predefinidas creadas por el administrador. Si no existen reglas disponibles, la conexión se bloquea automáticamente y no aparece ningún mensaje de alerta. Se recomienda que seleccione este modo sólo si es un administrador que tiene intención de configurar la comunicación de red.

Modo de aprendizaje permite crear y guardar automáticamente las reglas y se recomienda para la configuración inicial del cortafuegos personal. No es necesaria la intervención del usuario, ya que ESET Smart Security guarda las reglas de acuerdo con los parámetros predefinidos. Este modo no es seguro y sólo debe utilizarse hasta que se hayan creado todas las reglas de comunicaciones necesarias.

El último paso muestra una ventana que solicita su aprobación para realizar la instalación.

2.3 Uso de valores originales

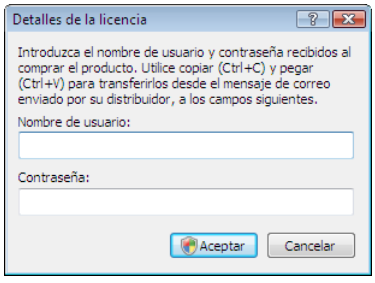
Si reinstala ESET Smart Security, se muestra la opción **Usar los parámetros actuales**. Seleccione esta opción para transferir parámetros de configuración de la instalación original a la nueva.



2.4 Introducción del nombre de usuario y la contraseña

Para optimizar la funcionalidad, es importante que el programa se actualice automáticamente. Esto sólo es posible si se introducen el nombre de usuario y la contraseña correctos en la configuración de actualizaciones.

Si no ha especificado un nombre de usuario y una contraseña durante la instalación, puede hacerlo ahora. En la ventana principal del programa, haga clic en **Actualizar** y, a continuación, en **Configuración del nombre de usuario y contraseña**. Introduzca los datos que haya recibido con la licencia del producto en la ventana **Detalles de la licencia**.



2.5 Análisis del equipo a petición

Después de la instalación de ESET Smart Security, debería llevarse a cabo un análisis del equipo para determinar la posible existencia de un código malicioso. Para iniciar el análisis rápidamente, seleccione **Análisis del equipo** en el menú principal y, a continuación, **Análisis estándar** en la ventana principal del programa. Para obtener más información acerca de la característica de análisis del equipo, consulte el capítulo "Análisis del equipo".

3. Guía para principiantes

Este capítulo proporciona una descripción general inicial de ESET Smart Security y su configuración básica.

3.1 Introducción del diseño de la interfaz de usuario: modos

La ventana principal de ESET Smart Security está dividida en dos secciones principales. La columna izquierda proporciona acceso al menú principal de fácil uso. La ventana principal del programa de la derecha está destinada fundamentalmente a mostrar información correspondiente a la opción seleccionada en el menú principal.

A continuación, se muestra una descripción de los botones del menú principal:

Estado de la protección: proporciona información fácil de consultar acerca del estado de la protección de ESET Smart Security. Si está activado el modo avanzado, se muestra el estado de todos los módulos de protección. Haga clic en un módulo para ver su estado actual.

Análisis del equipo: esta opción permite al usuario configurar e iniciar el análisis del equipo a petición.

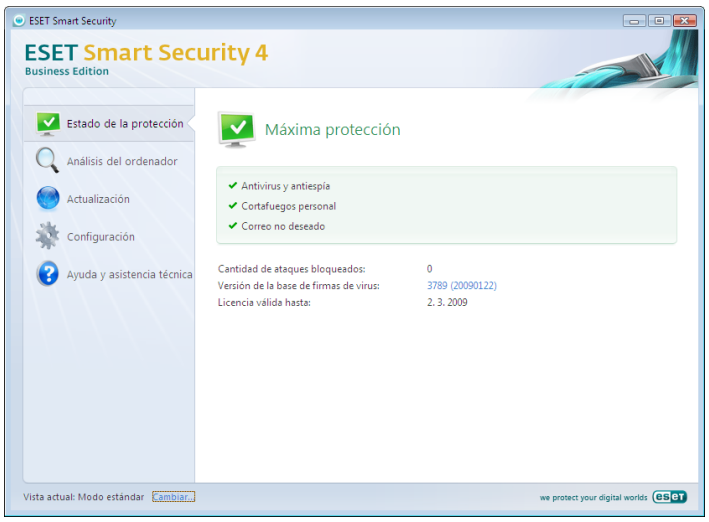
Actualización: seleccione esta opción para tener acceso al módulo de actualización que administra las actualizaciones en la base de firmas de virus.

Configuración: seleccione esta opción para ajustar el nivel de seguridad del equipo. Si está activado el modo avanzado, aparecerán los submenús Protección antivirus y antiespía, Cortafuegos personal y Módulo contra correo no deseado.

Herramientas: esta opción sólo está disponible en el modo avanzado. Proporciona acceso a Archivos de registro, Cuarentena y Tareas programadas.

Ayuda y asistencia técnica: seleccione esta opción para obtener acceso a los archivos de ayuda, el sitio web de ESET, la Base de conocimientos de ESET y a la solicitud de atención al cliente.

La interfaz de usuario de ESET Smart Security permite a los usuarios alternar entre los modos estándar y avanzado. Para cambiar entre un modo y otro, consulte el vínculo **Vista actual** ubicado en la esquina inferior izquierda de la ventana principal de ESET Smart Security. Haga clic en este botón para seleccionar el modo de visualización que desee.



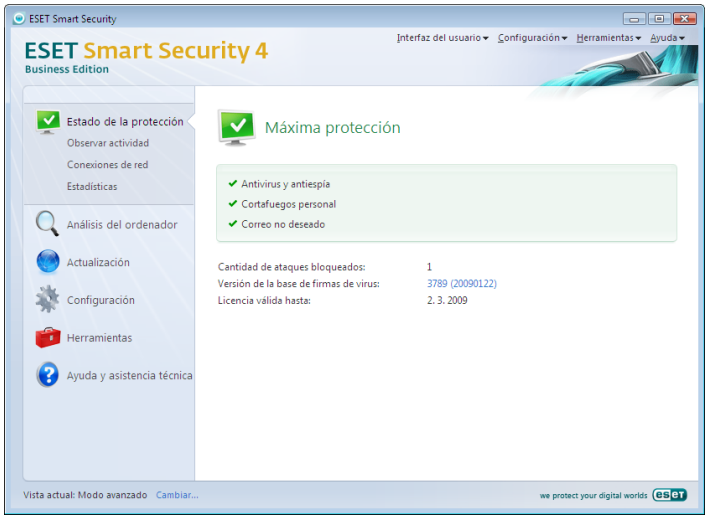
El modo estándar proporciona acceso a las características necesarias para realizar operaciones habituales. No muestra ninguna de las opciones avanzadas.

Al cambiar al modo avanzado, aparece la opción **Herramientas** en el menú principal. La opción Herramientas permite al usuario obtener acceso a Tareas programadas o Cuarentena, o ver los archivos de registro de ESET Smart Security.

NOTA: todas las instrucciones restantes de esta guía se llevarán a cabo en el modo avanzado.

3.1.1 Comprobación del funcionamiento del sistema

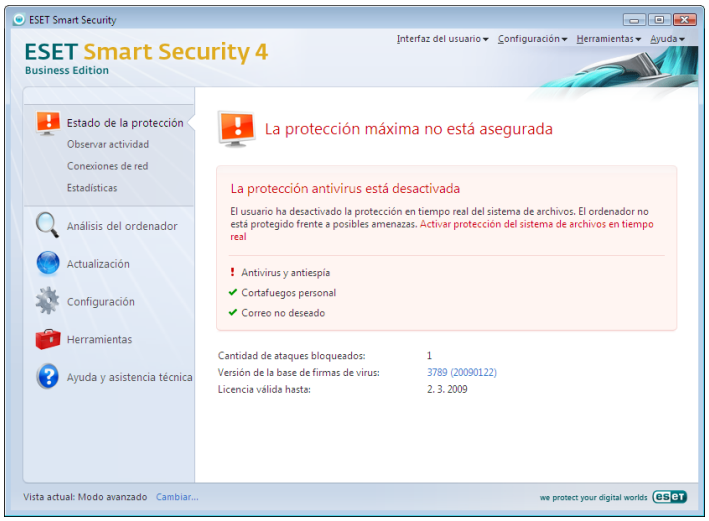
Para ver el **estado de la protección**, haga clic en esta opción ubicada en la parte superior del menú principal. Aparecerá un resumen del estado acerca del funcionamiento de ESET Smart Security en el lateral derecho de la ventana, así como un submenú con tres elementos: **Protección antivirus y antiespía**, **Cortafuegos personal** y **Módulo contra correo no deseado**. Seleccione uno de ellos para ver información detallada acerca del módulo de protección en cuestión.



Si los módulos activados funcionan correctamente, se les asigna una marca verde. En caso contrario, se muestra un signo de exclamación rojo o un icono de notificación naranja, además de información adicional acerca del módulo en la parte superior de la ventana. También se muestra una sugerencia de solución para reparar el módulo. Para cambiar el estado de los módulos individuales, haga clic en **Configuración** en el menú principal y, a continuación, en el módulo deseado.

3.1.2 Qué hacer si el programa no funciona correctamente

Si ESET Smart Security detecta un problema en algunos de sus módulos de protección, aparecerá en la ventana **Estado de la protección**. Aquí se ofrece igualmente una posible solución para el problema.

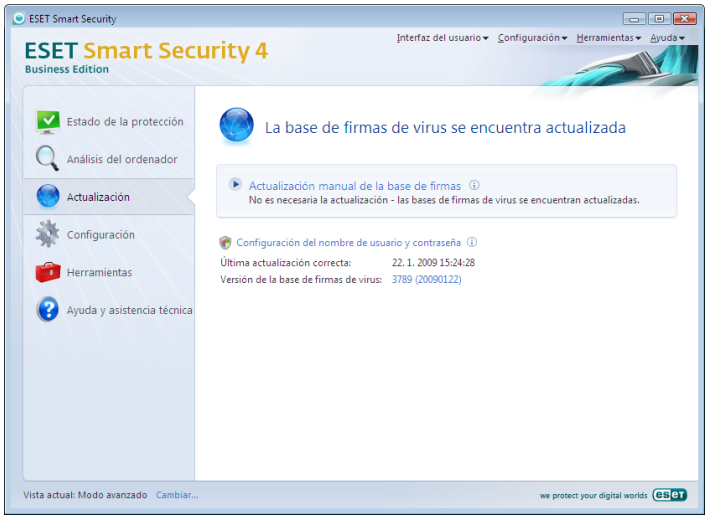


Si no se puede resolver mediante la lista de soluciones y problemas conocidos, haga clic en **Ayuda y asistencia técnica** para obtener acceso a los archivos de ayuda o realizar una búsqueda en la Base de conocimientos. Si aún no se puede encontrar una solución, envíe una solicitud de asistencia al Servicio de atención al cliente de ESET. Según los comentarios proporcionados, nuestros especialistas pueden responder rápidamente a las preguntas y aconsejarle eficazmente sobre el problema.

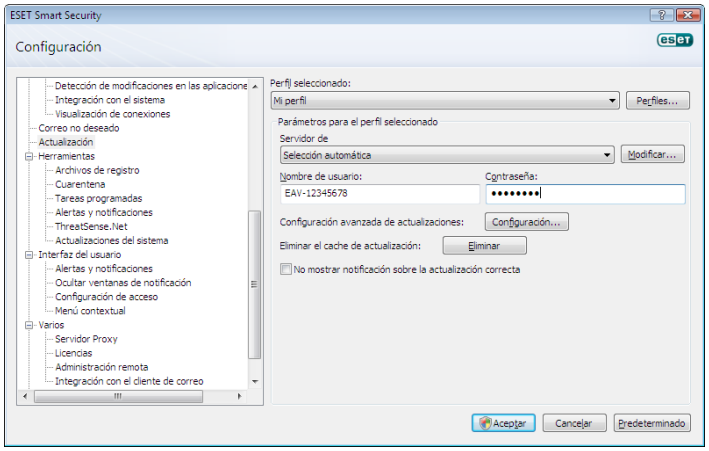
3.2 Configuración de actualizaciones

La actualización de la base de firmas de virus y de los componentes del programa son partes importantes a la hora de proporcionar total protección contra código malicioso. Preste especial atención a su configuración y funcionamiento. En el menú principal, seleccione **Actualización** y, a continuación, haga clic en **Actualización manual de la base de firmas de virus** en la ventana principal del programa para comprobar al instante la disponibilidad de la actualización más reciente de la base de datos. **Nombre de usuario y contraseña...** abre un cuadro de diálogo en el que se deben introducir el nombre de usuario y la contraseña recibidos en el momento de la compra.

Si éstos se han facilitado durante la instalación de ESET Smart Security, no se le solicitarán en este momento.



La ventana **Configuración avanzada** (pulse F5 para abrirla) contiene otras opciones de actualización más detalladas. **Servidor de actualización:** el menú desplegable se debe establecer en **Selección automática**. Para configurar las opciones de actualización avanzadas como el modo de actualización, el servidor Proxy, el acceso a las actualizaciones en un servidor local y la creación de copias de firmas de virus (ESET Smart Security Business Edition), haga clic en el botón **Configuración...**.



3.3 Configuración de zonas de confianza

La configuración de una zona de confianza es un paso importante de la protección del equipo en un entorno de red. Puede permitir a otros usuarios obtener acceso a su equipo mediante la configuración de la zona de confianza para permitir el uso compartido. Haga clic en **Configuración > Cortafuegos personal > Cambiar el modo de protección de su ordenador en la red...** Se mostrará una ventana que le permite configurar los parámetros del modo de protección del equipo en la misma red o zona.

La detección de zonas de confianza se lleva a cabo después de la instalación de ESET Smart Security o al conectar el equipo a una nueva red. Por tanto, no es necesario definir la zona de confianza en la mayoría de los casos. De forma predeterminada, se muestra un cuadro de diálogo tras la detección de una nueva zona, que permite establecer el nivel de protección de la misma.

Advertencia: la configuración incorrecta de una zona de confianza puede exponer su equipo a determinados riesgos.

NOTA: de forma predeterminada, se concede acceso a las estaciones de trabajo de una zona de confianza para compartir archivos e impresoras, la comunicación RPC entrante está activada y el uso compartido de escritorio remoto está disponible.

3.4 Configuración del servidor Proxy

Si utiliza un servidor Proxy para realizar la conexión a Internet en un sistema que utilice ESET Smart Security, es necesario especificarlo en la configuración avanzada (F5). Para obtener acceso a la ventana de configuración del **servidor Proxy**, haga clic en **Varios > Servidor Proxy** desde el árbol de configuración avanzada. Seleccione la casilla de verificación **Conexión mediante servidor Proxy** y escriba la dirección IP y el puerto del servidor Proxy, junto con sus datos de autentificación.

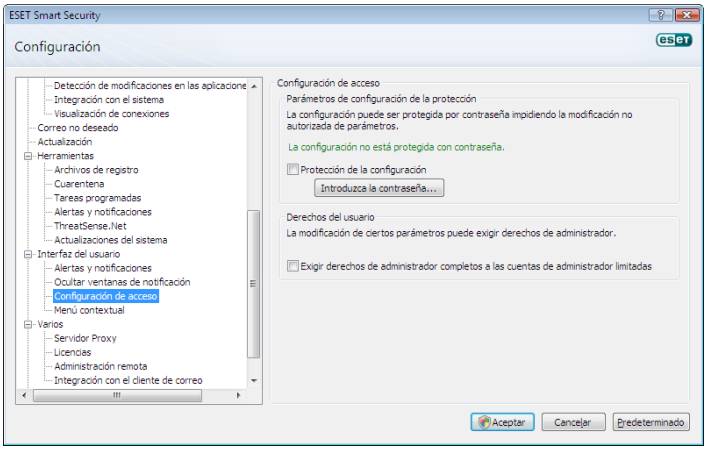
Si esta información no está disponible, puede intentar detectar automáticamente la configuración del servidor Proxy para ESET Smart Security haciendo clic en el botón **Detectar servidor Proxy** .

NOTA: las opciones del servidor Proxy pueden ser diferentes para los distintos perfiles de actualización. En este caso, configure el servidor Proxy en la configuración avanzada de actualizaciones.

3.5 Protección de la configuración

La configuración de ESET Smart Security puede ser muy importante desde el punto de vista de la directiva de seguridad de su organización. Las modificaciones no autorizadas pueden poner en peligro potencialmente la estabilidad y la protección del sistema. Para establecer una contraseña que proteja los parámetros de configuración, comience en el menú principal y haga clic en **Configuración > Escriba el árbol completo de la configuración avanzada... > Interfaz del usuario > Protección de parámetros** y haga clic en el botón **Introduzca la contraseña...**.

Introduzca una contraseña, confírmela escribiéndola de nuevo y haga clic en **Aceptar**. Esta contraseña se solicitará para cualquier modificación futura en los parámetros de ESET Smart Security.



4. Uso de ESET Smart Security

4.1 Protección antivirus y antiespía

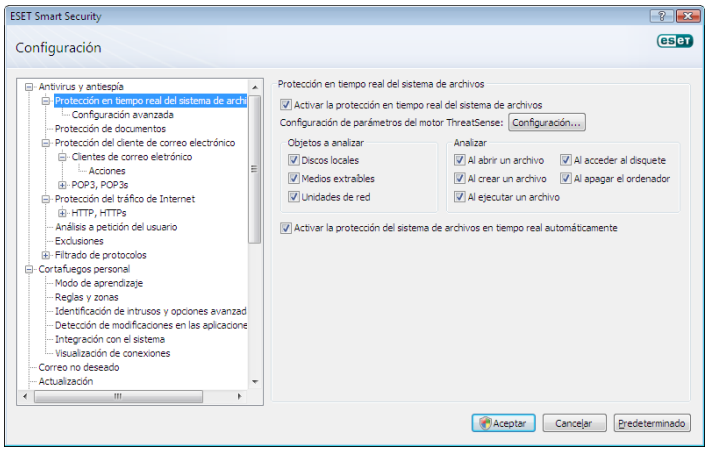
La protección antivirus protege contra ataques maliciosos al sistema, controlando las comunicaciones por Internet, el correo electrónico y los archivos. Si se detecta una amenaza con código malicioso, el módulo antivirus puede eliminarlo bloqueándolo primero y, a continuación, desinfectándolo, eliminándolo o poniéndolo en cuarentena.

4.1.1 Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con el antivirus en el sistema. Todos los archivos se analizan en busca de código malicioso en el momento en el que se abren, crean o ejecutan en el equipo. La protección del sistema de archivos en tiempo real se inicia al arrancar el sistema.

4.1.1.1 Configuración del control

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y varios sucesos activan el control, que utiliza los métodos de detección de la tecnología ThreatSense (tal como se describe en "Configuración de parámetros del motor ThreatSense"). El comportamiento del control puede variar para los archivos existentes y los creados recientemente. Para estos últimos, se puede aplicar un nivel de control más exhaustivo.



4.1.1.1.1 Medios que se van a analizar

De forma predeterminada, todos los tipos de medios se analizan en busca de amenazas.

Discos locales: controla todas las unidades del sistema.

Medios extraíbles: disquetes, dispositivos de almacenamiento USB, etc.

Unidades de red: analiza todas las unidades asignadas.

Recomendamos que mantenga la configuración predeterminada y sólo la modifique en casos específicos como, por ejemplo, cuando el análisis de ciertos medios ralentice significativamente las transferencias de datos.

4.1.1.1.2 Analizar (Análisis cuando se cumpla la condición)

De forma predeterminada, todos los archivos se analizan cuando se abren, ejecutan o crean. Recomendamos que mantenga la configuración predeterminada que ofrece el máximo nivel de protección en tiempo real para su equipo.

La opción **Al acceder al disquete** ofrece control del sector de arranque del disquete cuando se obtiene acceso a esta unidad. La opción **Al apagar el ordenador** ofrece control de los sectores de arranque del disco duro durante el apagado del equipo. Aunque los virus de arranque son escasos hoy en día, recomendamos que deje estas opciones activadas, ya que aún existe la posibilidad de infección por virus de arranque de fuentes alternativas.

4.1.1.1.3 Parámetros adicionales de ThreatSense para archivos nuevos o modificados

La probabilidad de infección en archivos creados o modificados recientemente es proporcionalmente mayor que en archivos existentes. Éste es el motivo por el que el programa analiza estos archivos con parámetros de análisis adicionales. Junto con los métodos de análisis basados en firmas comunes, se utiliza la heurística avanzada, que mejora en gran medida los índices de detección. Además de los archivos creados recientemente, el análisis también se realiza en archivos de auto extracción (SFX) y empaquetadores en tiempo real (archivos ejecutables comprimidos internamente). De forma predeterminada, los archivos se analizan hasta el décimo nivel de anidamiento y se verifican independientemente de su tamaño real. Anule la selección de la opción ***Usar parámetros predeterminados para archivos comprimidos*** para modificar la configuración de análisis de archivos.

4.1.1.1.4 Configuración avanzada

Para reducir al mínimo el consumo de recursos del sistema cuando se utiliza la protección en tiempo real, los archivos que ya se han analizado no se analizarán reiteradamente (a menos que se hayan modificado). Los archivos se vuelven a analizar inmediatamente después de cada actualización de la base de firmas de virus. Este comportamiento se configura utilizando la opción **Análisis optimizado**. Si está desactivada, todos los archivos se analizarán cada vez que se obtenga acceso a ellos.

La protección en tiempo real comienza de forma predeterminada en el momento de iniciarse el sistema operativo, proporcionando un análisis ininterrumpido. En casos especiales, (por ejemplo, si hay un conflicto con otro análisis en tiempo real), la protección en tiempo real se puede detener desactivando la opción **Iniciar la protección automática del sistema de archivos en tiempo real**.

De forma predeterminada, no se utiliza la heurística avanzada al ejecutar los archivos. No obstante, en algunos casos, es posible que desee activar esta opción (activando la opción **Heurística avanzada al ejecutar un archivo**). Tenga en cuenta que la heurística avanzada puede ralentizar la ejecución de algunos programas debido a la necesidad de requisitos del sistema adicionales.

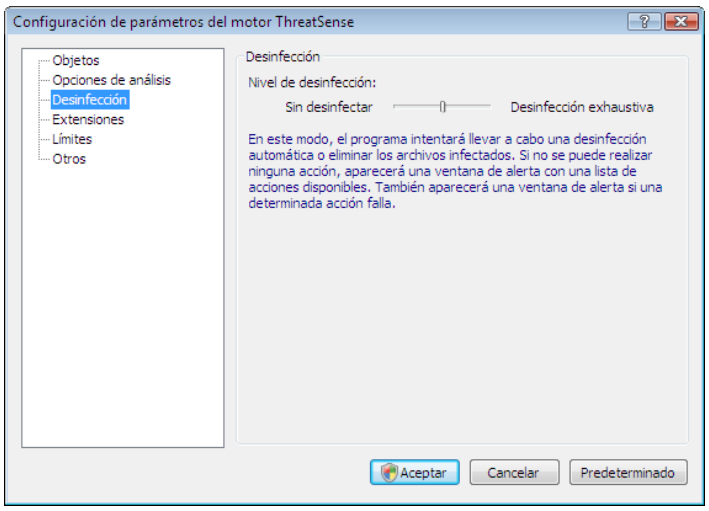
4.1.1.2 Niveles de desinfección

La protección en tiempo real tiene tres niveles de desinfección (para obtener acceso a ellos, haga clic en el botón **Configuración...** en la sección **Protección del sistema de archivos en tiempo real** y, a continuación, en el apartado **Desinfección**).

- En el primer nivel, se muestra una ventana de alerta con opciones disponibles para cada amenaza encontrada. El usuario debe elegir una acción para cada amenaza individualmente. Este nivel está diseñado para usuarios más avanzados que saben los pasos que hay que seguir en caso de una amenaza.

- El nivel predeterminado elige y realiza automáticamente una acción predefinida (dependiendo del tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante un mensaje de información ubicado en la esquina inferior derecha de la pantalla. Sin embargo, no se realiza ninguna acción automática si la amenaza se localiza dentro de un archivo comprimido que también contiene archivos desinfectados ni en objetos para los que no hay acciones predefinidas.

- El tercer nivel es el más "agresivo"; ya que todos los objetos infectados se desinfectan. Como este nivel puede provocar la pérdida de archivos válidos, recomendamos que se utilice sólo en situaciones específicas.



4.1.1.3 Modificación de la configuración de protección en tiempo real

La protección en tiempo real es el componente más esencial de mantenimiento de un sistema seguro. Por tanto, debe tener cuidado cuando modifique los parámetros correspondientes. 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 Smart Security, se optimizará toda la configuración para proporcionar el nivel máximo de seguridad del sistema a los usuarios. Para restaurar la configuración predeterminada, haga clic en el botón **Predeterminado** ubicado en la parte inferior derecha de la ventana **Protección del sistema de archivos en tiempo real** (**Configuración avanzada > Antivirus y antiespía > Protección del sistema de archivos en tiempo real**).

4.1.1.4 Análisis de protección en tiempo real

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

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

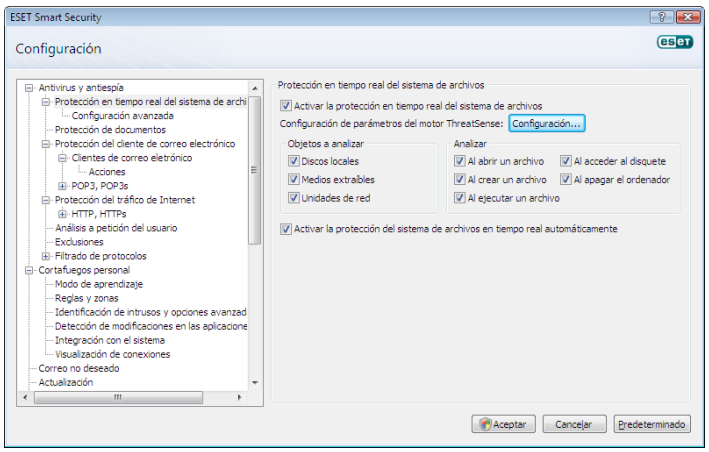
4.1.1.5 ¿Qué debo hacer si la protección en tiempo real no funciona?

En el próximo capítulo, describimos las situaciones en las que puede surgir un problema cuando se utiliza la protección en tiempo real y cómo resolverlas.

Protección en tiempo real desactivada

Si un usuario ha desactivado la protección en tiempo real sin darse cuenta, será necesario volver a activarla. Para ello, vaya a **Configuración>Antivirus y antiespía** y haga clic en **Activar** en la sección **Protección del sistema de archivos en tiempo real** de la ventana principal del programa.

Si la protección en tiempo real no se activa al iniciar el sistema, probablemente se deba a que la opción **Iniciar la protección automática del sistema de archivos en tiempo real** se encuentra desactivada. Para activar esta opción, vaya a **Configuración avanzada** (F5) y haga clic en **Protección del sistema de archivos en tiempo real** en el árbol de configuración avanzada. En la sección **Configuración avanzada** de la parte inferior de la ventana, asegúrese de que esté seleccionada la casilla de verificación **Iniciar la protección automática del sistema de archivos en tiempo real**.



Si la protección en tiempo real no detecta ni desinfecta amenazas

Asegúrese de que no tiene instalados otros programas antivirus en el equipo. Si están activadas dos protecciones en tiempo real al mismo tiempo, pueden entrar en conflicto. Recomendamos que desinstale uno de los programas antivirus de su sistema.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y la opción **Iniciar la protección automática del sistema de archivos en tiempo real** está activada), es posible que se deba a la existencia de conflictos con otros programas. Si éste es el caso, consulte a los especialistas de Atención al cliente de ESET.

4.1.2 El Sistema de Prevencion de Intrusos (SPI)

El Sistema de Prevencion de Intrusos (SPI) protege su sistema de los códigos maliciosos o de cualquier actividad no autorizada que intente afectar negativamente a la seguridad de su ordenador. Utiliza un análisis avanzado del comportamiento, unido a las capacidades de detección del filtrado de redes, para supervisar los procesos en funcionamiento, archivos y llaves del registro, bloqueando e impidiendo activamente cualquier intento de causar daño.

4.1.3 Protección de clientes de correo electrónico

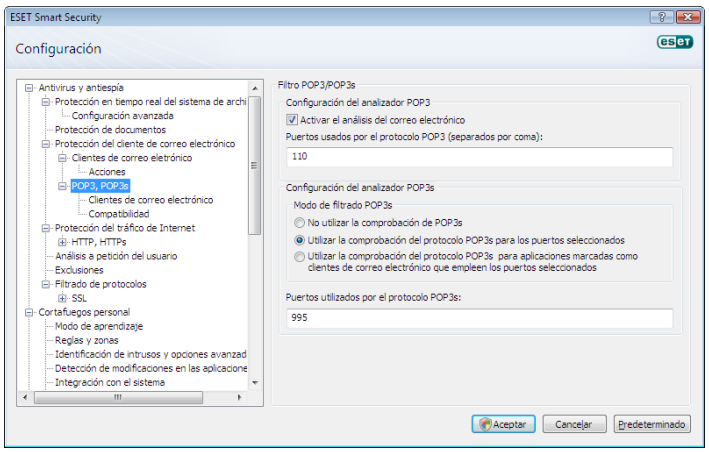
La protección de correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través del protocolo POP3. Con el programa de complemento para Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird, ESET Smart Security ofrece control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP y HTTP). Al examinar los mensajes entrantes, el programa utiliza todos los métodos de análisis avanzados proporcionados por el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con la base de firmas de virus. El análisis de las comunicaciones del protocolo POP3 es independiente del cliente de correo electrónico utilizado.

4.1.3.1 Análisis POP3

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

El módulo que proporciona este control se inicia automáticamente al arrancar el sistema operativo y está activo en la memoria. Para que el módulo funcione correctamente, asegúrese de que está activado; el análisis POP3 se realiza automáticamente sin necesidad de reconfigurar el cliente de correo electrónico. De forma predeterminada, se analizan todas las comunicaciones en el puerto 110, pero se pueden agregar otros puertos de comunicación si es necesario. Los números de puerto deben delimitarse por una coma.

Las comunicaciones cifradas no se controlan.



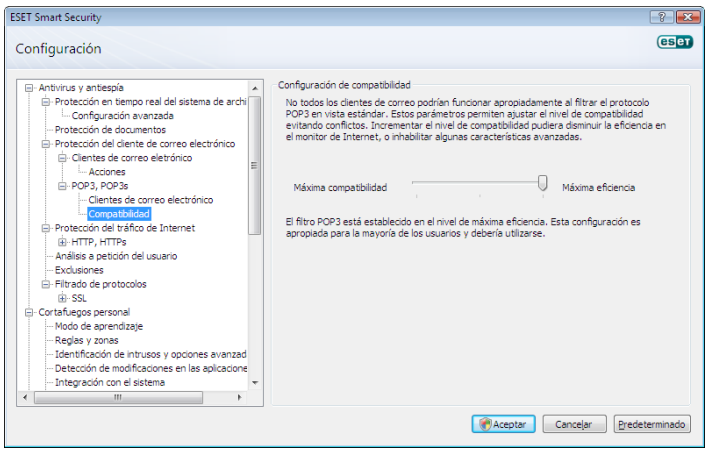
4.1.3.1.1 Compatibilidad

Con determinados programas de correo electrónico, puede experimentar problemas al filtrar el protocolo POP3 (por ejemplo, si recibe mensajes con una conexión de Internet lenta, pueden producirse tiempos de espera debido al análisis). Si éste es el caso, intente modificar la forma en la que se realiza el control. La reducción del nivel de control puede mejorar la velocidad del proceso de desinfección. Para ajustar el nivel de control del filtrado del protocolo POP3, vaya a **Antivirus y antiespía > Protección de correo electrónico > POP3 > Compatibilidad**.

Si está activado el modo de **máxima eficiencia**, las amenazas se eliminan de los mensajes infectados y la información sobre la amenaza se inserta antes del asunto original del correo electrónico (deben estar activadas las opciones **Eliminar** o **Desinfectar**, o debe estar activado el nivel de desinfección **Estricta** o **Predeterminado**).

Compatibilidad media modifica la forma en la que se reciben los mensajes. Los mensajes se envían gradualmente al cliente de correo electrónico; una vez transferida la última parte del mensaje, se analizará en busca de amenazas. Sin embargo, el riesgo de infección aumenta con este nivel de control. El nivel de desinfección y el tratamiento de los mensajes con etiquetas (alertas de notificación agregadas a la línea del asunto y al cuerpo de los mensajes de correo electrónico) son idénticos a la configuración de máxima eficiencia.

Con el nivel de **compatibilidad máxima**, una ventana de alerta informa al usuario sobre la recepción de un mensaje infectado. No se agregará ninguna información sobre archivos infectados a la línea del asunto o al cuerpo de los mensajes de correo electrónico enviados y las amenazas no se eliminarán automáticamente. La eliminación de las amenazas debe realizarla el usuario del cliente de correo electrónico.

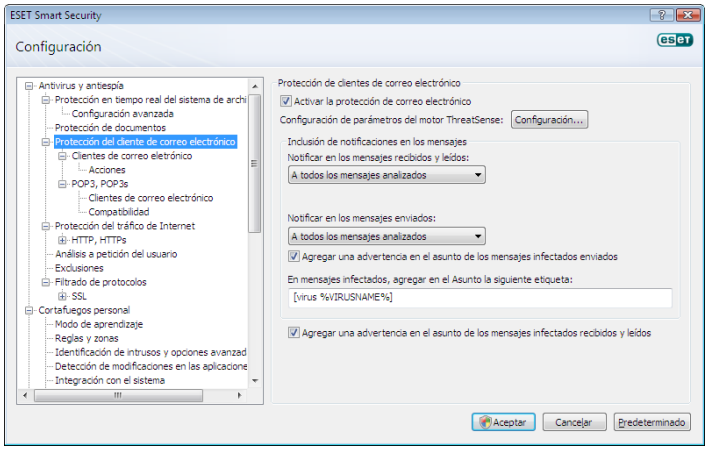


4.1.3.2 Integración con clientes de correo electrónico

La integración de ESET Smart Security con clientes de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si se admite su cliente de correo electrónico, esta integración se puede activar en ESET Smart Security. Si está activada la integración, la barra de herramientas contra correo no deseado de ESET Smart Security se inserta directamente en el cliente de correo electrónico, contribuyendo a que la protección de las comunicaciones por correo electrónico sea más eficaz. Las opciones de integración están disponibles en **Configuración > Escriba el árbol completo de la configuración avanzada... > Varios > Integración con el cliente de correo electrónico**. Este cuadro de diálogo le permite activar la integración con los clientes de correo electrónico compatibles. Entre los clientes de correo electrónico compatibles actualmente, se incluyen Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird.

Seleccione la opción ***Desactivar el análisis de cambios de contenido de la bandeja de entrada*** si se ha producido una ralentización del sistema al trabajar con su cliente de correo electrónico. Esta situación puede producirse al descargar correo electrónico de Kerio Outlook Connector Store.

La protección de correo electrónico comienza con la activación de la casilla de verificación **Activar la protección de correo electrónico** en **Configuración avanzada (F5) > Antivirus y antiespía > Protección de correo electrónico**.



4.1.3.2.1 Adición de mensajes con etiquetas al cuerpo del correo electrónico

Se puede marcar cada mensaje de correo electrónico controlado por ESET Smart Security si se agrega un mensaje con etiqueta al asunto o cuerpo del mensaje. Esta función aumenta el nivel de credibilidad del destinatario y, si se detecta una amenaza, proporciona información valiosa sobre el nivel de amenaza del remitente/mensaje de correo electrónico específico.

Las opciones de esta funcionalidad están disponibles en **Configuración avanzada > Antivirus y antiespía > Protección de correo electrónico**. El programa puede **agregar mensajes con etiquetas a correo electrónico leído y recibido**, así como **a correo enviado**. Los usuarios también tienen la capacidad de decidir si los mensajes con etiquetas deben agregarse a todo el correo electrónico, sólo al correo electrónico infectado o a ningún mensaje de correo electrónico. ESET Smart Security permite también al usuario agregar mensajes al asunto original de los mensajes infectados. Para permitir esta adición al asunto, utilice las opciones **Agregar una advertencia en el asunto de los mensajes infectados recibidos y leídos** y **Agregar una advertencia en el asunto de los mensajes infectados enviados.**

El contenido de las notificaciones se puede modificar en el campo Etiqueta y agregar en el asunto de los mensajes infectados.

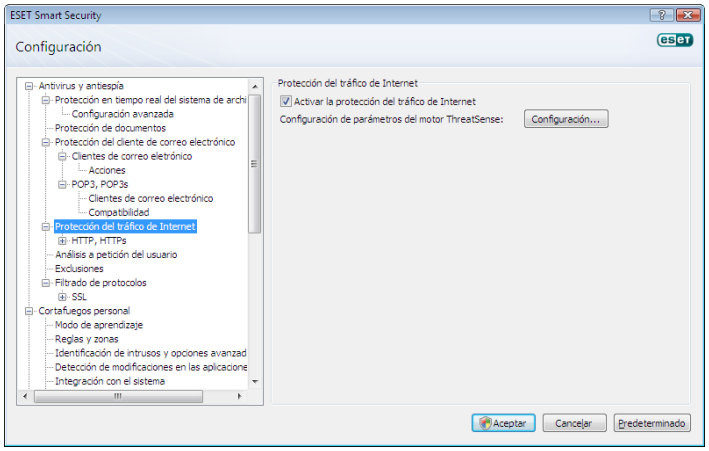
Las modificaciones anteriormente mencionadas pueden ayudar a automatizar el proceso de filtrado de correo electrónico infectado, ya que permiten filtrar correo electrónico con un asunto específico (si se admite en su cliente de correo electrónico) a una carpeta individual.

4.1.3.3 Eliminación de amenazas

Si se recibe un mensaje de correo electrónico infectado, aparecerá una ventana de alerta, que muestra el nombre del remitente, el correo electrónico y el nombre de la amenaza. En la parte inferior de la ventana, están disponibles las opciones **Desinfectar**, **Eliminar** o **Sin acciones** para el objeto detectado. En casi todos los casos, recomendamos que seleccione **Desinfectar** o **Eliminar**. En situaciones especiales, cuando desee recibir el archivo infectado, seleccione **Sin acciones**. Si está activada la **Desinfección estricta**, aparecerá una ventana de información sin opciones disponibles para objetos infectados.

4.1.4 Protección del tráfico de Internet

La conectividad a Internet es una característica estándar de un ordenador personal. Desafortunadamente, se ha convertido también en el principal medio de transferencia de código malicioso. Por esta razón, es esencial que analice detenidamente su protección de acceso a Internet. Recomendamos que esté activada la opción **Activar la protección del tráfico de Internet** que se encuentra en **Configuración avanzada (F5) > Antivirus y antiespía > Protección del tráfico de Internet**.



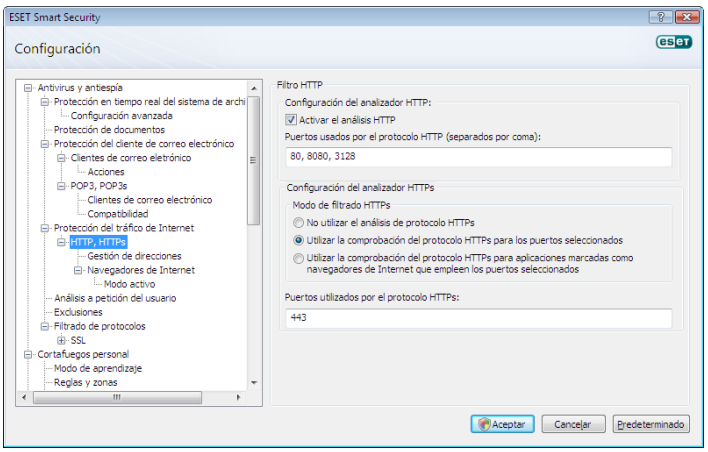
4.1.4.1 HTTP, HTTPs

La protección del tráfico de Internet se ocupa de supervisar la comunicación entre los navegadores de Internet y los servidores remotos, cumpliendo con las reglas de los protocolos HTTP (Protocolo de transferencia de hipertexto) y HTTPs (comunicación cifrada). De forma predeterminada, ESET Smart Security se configura para utilizar los estándares de la mayoría de los navegadores de Internet. No obstante, las opciones de configuración de análisis HTTP se pueden modificar en Protección del tráfico de Internet> HTTP, HTTPs. En la ventana principal del filtro HTTP, se puede seleccionar la opción **Activar el análisis HTTP**. También se pueden definir los números de los puertos utilizados para la comunicación HTTP. De forma predeterminada, los números de puerto 80, 8080 y 3128 se encuentran predefinidos. El análisis HTTPs se puede llevar a cabo de las formas siguientes:

No utilizar el análisis de protocolo HTTPs
No se analizará la comunicación cifrada.

Utilizar la comprobación del protocolo HTTPs para los puertos seleccionados
Sólo se realizará el análisis HTTPs para los puertos definidos en Puertos usados por el protocolo HTTPs.

Utilizar la comprobación del protocolo HTTPs para aplicaciones marcadas como navegadores de Internet que empleen los puertos seleccionados
Sólo se analizarán las aplicaciones especificadas en la sección de navegadores y se utilizarán los puertos definidos en ***Puertos usados por el protocolo HTTPs***.

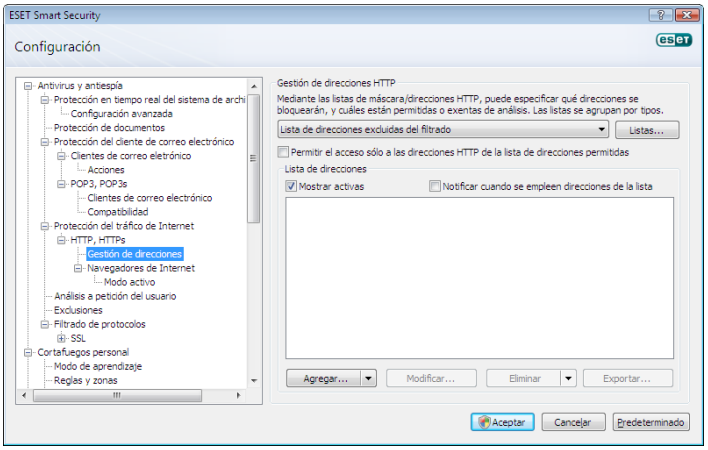


4.1.4.1.1 Administración de direcciones

Esta sección le permite especificar las direcciones HTTP para bloquear, incluir o excluir el análisis de las mismas.

Los botones **Agregar, Cambiar, Eliminar** y **Exportar** se utilizan para administrar las listas de direcciones. No se podrá obtener acceso a los sitios web de la lista de direcciones bloqueadas. Se puede tener acceso a los sitios web de la lista de direcciones excluidas sin necesidad de analizarlos en busca de código maliciosos. Si se activa la opción ***Permitir el acceso sólo a las direcciones HTTP de la lista de direcciones permitidas***, se podrá obtener acceso únicamente a las direcciones que se encuentren en la lista de direcciones permitidas y el resto de direcciones HTTP quedará bloqueado.

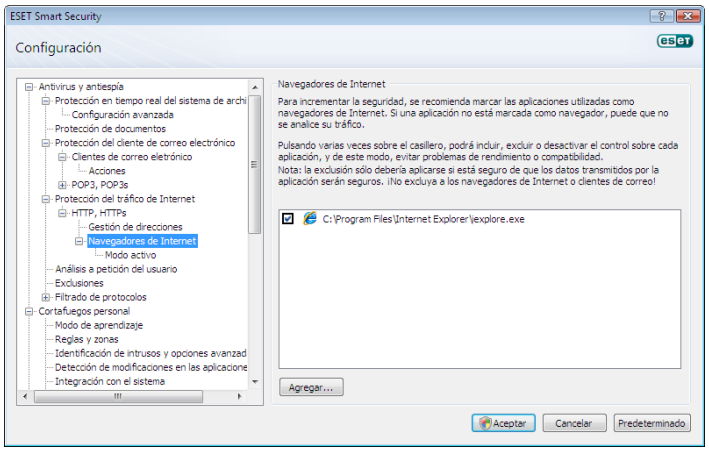
En todas las listas, se pueden utilizar los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista sólo debe contener direcciones seguras y de confianza. del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista. Para activar una lista, seleccione la opción ***Lista activa***. Si desea recibir una notificación cuando se introduzca una dirección de la lista actual, seleccione ***Notificar cuando se empleen direcciones de la lista***



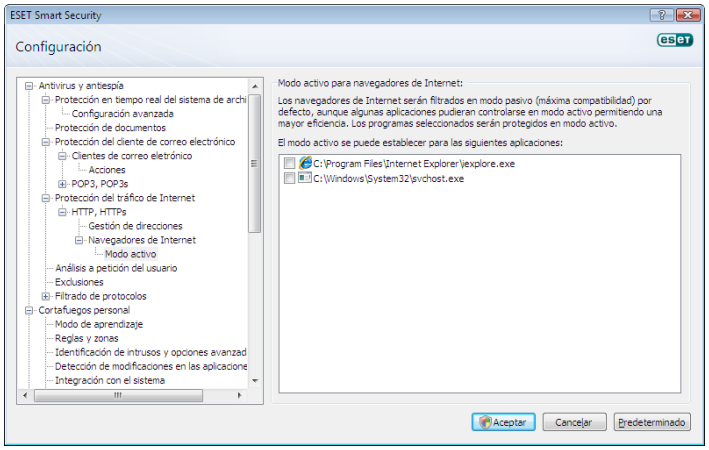
4.1.4.1.2 Navegadores de Internet

ESET Smart Security incluye también la función de **navegadores de Internet**, que permite al usuario definir si la aplicación específica es un navegador o no. Si el usuario marca una aplicación como navegador, toda la comunicación desde esta aplicación se supervisa independientemente de los números de puerto que participen en la comunicación.

La función de navegadores de Internet sirve de complemento a la función de análisis HTTP, ya que ésta sólo se utiliza en puertos predefinidos. Sin embargo, muchos servicios de Internet utilizan números de puerto desconocidos o que cambian dinámicamente. Para ello, la función de navegador de Internet puede establecer el control de las comunicaciones de puerto independientemente de los parámetros de conexión.



Se puede obtener acceso directamente a la lista de aplicaciones marcadas como navegadores desde el submenú **Navegadores de Internet** del apartado **HTTP**. En esta sección, también se incluye el submenú **Modo activo** , que define el modo de análisis de los navegadores de Internet. El **modo activo** resulta útil porque examina los datos transferidos en conjunto. Si no está activado, la comunicación de las aplicaciones se supervisa gradualmente en lotes. Esto reduce la eficacia del proceso de verificación de datos, pero también ofrece mayor compatibilidad para las aplicaciones enumeradas. Si no se producen problemas durante su utilización, recomendamos que active el modo de comprobación activa seleccionando la casilla de verificación junto a la aplicación deseada.



4.1.5 Análisis del equipo

Si sospecha que su equipo está infectado (se comporta de manera anormal), ejecute un análisis del equipo a petición para examinar si existen amenazas en su sistema. Desde el punto de vista de la seguridad, es esencial que los análisis del equipo no sólo se ejecuten cuando se sospecha de la presencia de una infección, sino también con regularidad, como parte de las medidas de seguridad rutinarias. Los análisis regulares ayudan a detectar amenazas que no se detectaron durante el análisis en tiempo real en el momento en el que se guardaron en el disco. Esto puede ocurrir si se ha desactivado el análisis en tiempo real en el momento de la infección o la base de firmas de virus no estaba actualizada.

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**.

4.1.5.1 Tipo de análisis

Hay dos tipos disponibles. En el **análisis estándar**, se analiza rápidamente el sistema sin necesidad de realizar una configuración adicional de los parámetros de análisis. El **análisis personalizado** permite al usuario seleccionar cualquier perfil de análisis predefinido, además de elegir los objetos de análisis de la estructura de árbol.

4.1.5.1.1 Análisis estándar

El análisis estándar es un método fácil de usar que permite al usuario iniciar rápidamente un análisis del equipo y limpiar archivos infectados sin necesidad de que el usuario intervenga. Su principal ventaja es su funcionamiento sencillo sin ninguna configuración de análisis detallado. El análisis estándar comprueba todos los archivos en las unidades locales y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece automáticamente en el valor predeterminado. Para obtener más información sobre los tipos de desinfección, consulte "Desinfección" (véase la página 18).

El perfil de análisis estándar está diseñado para usuarios que desean analizar rápida y fácilmente sus equipos. Ofrece una solución de análisis y desinfección eficaz sin necesidad de un proceso de configuración amplio.

4.1.5.1.2 Análisis personalizado

El análisis personalizado es una solución óptima si desea especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del análisis personalizado es la capacidad para configurar los parámetros detalladamente. Las 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, use el menú desplegable de la función de selección rápida de objetos o seleccione los objetos desde la estructura de árbol que aparece en todos los dispositivos disponibles en el equipo. Además, puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración... > Desinfección**. Si sólo está interesado en analizar el sistema sin realizar acciones adicionales, seleccione la casilla de verificación **Analizar sin desinfectar**.

La realización de análisis del equipo en el modo de análisis personalizado es adecuado para usuarios avanzados con experiencia previa en la utilización de programas antivirus.

4.1.5.2 Analizar objetos

En el menú desplegable Analizar objetos, se pueden seleccionar archivos, carpetas y dispositivos (discos) que se analizarán en busca de virus.

Con la opción de menú de análisis de objetos rápido, puede seleccionar los siguientes objetos:

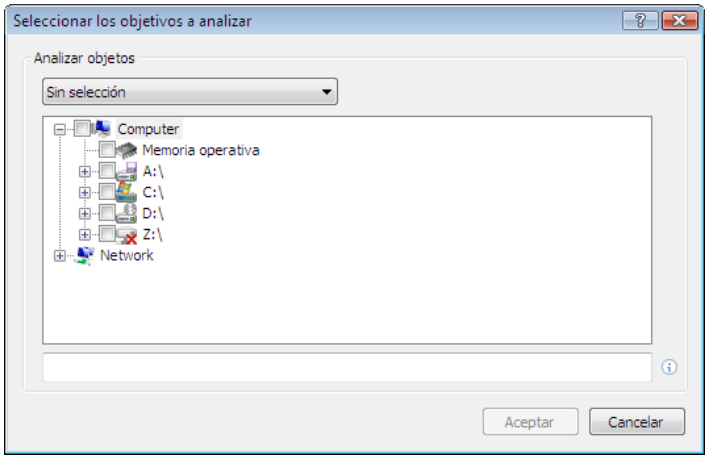
Parámetros según perfil: controla los objetos definidos en el perfil de análisis seleccionado.

Medios extraíbles: disquetes, dispositivos de almacenamiento USB y CD/DVD.

Discos locales: controla todas las unidades del sistema.

Unidades de red: todas las unidades asignadas.

Sin selección: cancela todas las selecciones.



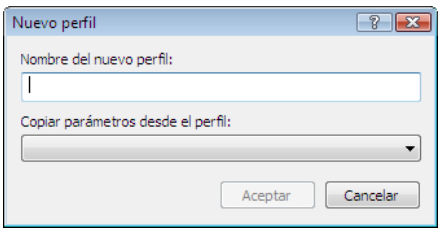
También se puede especificar con más precisión un objeto de análisis introduciendo la ruta a la carpeta o archivo(s) que desea incluir en el análisis. Seleccione los objetos en la estructura de árbol que aparece con todos los dispositivos disponibles en el equipo.

4.1.5.3 Perfiles de análisis

Los parámetros preferidos de análisis del equipo se pueden guardar en perfiles. La ventaja de la creación de perfiles de análisis es que se pueden utilizar regularmente para el análisis en el futuro. Recomendamos que cree tantos perfiles (con varios objetos de análisis, métodos de análisis y otros parámetros) como el usuario utiliza regularmente.

Para crear un nuevo perfil que se pueda utilizar repetidamente para análisis futuros, vaya a **Configuración avanzada** (F5) **> Análisis del equipo a petición**. Haga clic en el botón **Perfiles...** a la derecha para ver la lista de perfiles de análisis existentes y la opción para crear uno nuevo. En la opción **Configuración de parámetros del motor ThreatSense**, se describe cada parámetro de la configuración del análisis. Esto le ayudará a crear un perfil de análisis que se ajuste a sus necesidades.

Ejemplo:
Suponga que desea crear su propio perfil de análisis y la configuración asignada al perfil **Análisis inteligente** es parcialmente adecuada. Sin embargo, no desea analizar empaquetadores en tiempo real o aplicaciones potencialmente peligrosas y, además, quiere aplicar una **desinfección estricta**. En la ventana **Perfiles de configuración**, haga clic en el botón **Agregar...**. Escriba el nombre del nuevo perfil en el campo **Nombre del perfil** y seleccione **Análisis inteligente** en el menú desplegable **Copiar parámetros desde el perfil:** A continuación, ajuste los parámetros restantes para que cumplan sus requisitos.



4.1.6 Filtrado de protocolos

El motor de análisis ThreatSense proporciona la protección antivirus para los protocolos POP3 y HTTP utilizados por la aplicación. Este motor integra a la perfección todas las técnicas avanzadas de análisis de códigos maliciosos. El control funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizado. a continuación, se indican las opciones disponibles para el filtrado de protocolos (si la opción **Activar filtro de protocolos de la aplicación** está activada).

Puertos HTTP y POP3: limita el análisis de la comunicación a los puertos HTTP y POP3 conocidos.

Aplicaciones marcadas como navegadores de Internet y clientes de correo electrónico: active esta opción para filtrar solamente la comunicación de las aplicaciones marcada como navegadores (Protección del tráfico de Internet > HTTP, HTTPS > Navegadores de Internet) y los clientes de correo electrónico (Protección del cliente de correo electrónico > POP3, POP3S > Clientes de correo electrónico).

Puertos y aplicaciones marcados como usados por navegadores de Internet y clientes de correo electrónico: ambos puertos y navegadores se analizan para buscar códigos maliciosos.

Nota:
A partir de las versiones Windows Vista Service Pack 1 y Windows Server 2008, se usa un nuevo filtro de comunicación. Por ello, la sección de filtrado de protocolos no se encuentra disponible.

4.1.6.1 SSL

ESET Smart Security 4 le permite analizar los protocolos encapsulados en el protocolo SSL. Puede utilizar varios modos de análisis para las comunicaciones protegidas mediante el protocolo SSL gracias a los certificados de confianza, a los certificados desconocidos y a los certificados que se excluyen del análisis de estas comunicaciones.

Analizar siempre el protocolo SSL (los certificados excluidos y de confianza seguirán siendo válidos): seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL, excepto aquellas que estén protegidas por los certificados excluidos del análisis. Si se establece una comunicación nueva mediante un certificado firmado que sea desconocido, el usuario no recibirá ninguna notificación al respecto y la comunicación se filtrará automáticamente. Cuando un usuario obtiene acceso a un servidor con un certificado que no es de confianza y que el usuario ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permitirá la comunicación con el servidor y se filtrará el contenido del canal de la comunicación.

Preguntar sobre sitios no visitados (certificados desconocidos): si entra en un nuevo sitio protegido mediante el protocolo SSL (con un certificado desconocido), le aparecerá un cuadro de diálogo de selección. Gracias a este modo, puede crear una lista de certificados SSL que se excluirán del análisis.

No analizar el protocolo SSL: si selecciona esta opción, el programa no analizará las comunicaciones establecidas a través del protocolo SSL.

Si el certificado no se puede comprobar mediante el Archivo de Autoridades Certificadores de Confianza:

Preguntar sobre la validez del certificado: solicita al usuario que seleccione una acción para llevarla a cabo.

Bloquear la comunicación que utiliza el certificado: finaliza la conexión con el sitio que utiliza el certificado.

Si el certificado no es válido o está dañado:

Preguntar sobre la validez del certificado: solicita al usuario que seleccione una acción para llevarla a cabo.

Bloquear la comunicación que utiliza el certificado: finaliza la conexión con el sitio que utiliza el certificado.

4.1.6.1.1 Certificados de confianza

Además de contar con el Archivo de Autoridades Certificadoras de Confianza integrado, en el que ESET Smart Security 4 almacena los certificados de confianza, puede crear una lista de certificados de confianza personalizada que puede visualizar a través de **Configuración** (F5) **> Filtrado de protocolos > SSL > Certificados de confianza**.

4.1.6.1.2 Certificados excluidos

La sección Certificados excluidos contiene certificados que se consideran seguros. El programa no analizará el contenido de las comunicaciones cifradas que utilizan certificados de esta lista. Recomendamos instalar sólo los certificados web cuya seguridad esté garantizada y para los que no sea necesario realizar el filtrado de contenido.

4.1.7 Configuración de parámetros del motor ThreatSense

ThreatSense es el nombre de la tecnología que consta de complejos métodos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de diferentes métodos (análisis de código, emulación de código, firmas genéricas y firmas de virus) que funcionan de forma conjunta para mejorar la seguridad del sistema en gran medida. El motor de búsqueda 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.

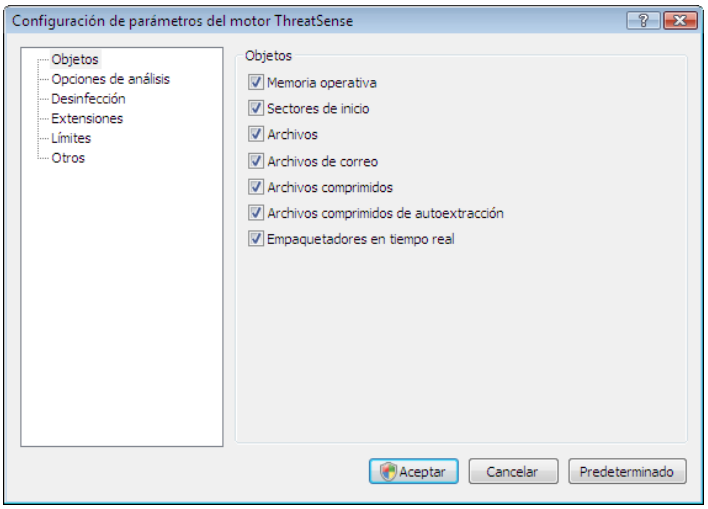
Para obtener acceso a la ventana de configuración, haga clic en el botón **Configuración...** ubicado en la ventana de configuración de cualquier módulo que utilice la tecnología ThreatSense (ver a continuación). Es posible que escenarios de seguridad distintos requieran configuraciones diferentes. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Verificación de la ejecución de archivos en el inicio del sistema
- Protección de correo electrónico
- Protección del tráfico de Internet
- Análisis del equipo a petición

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre ejecuten empaquetadores en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real, podrían implicar la ralentización del sistema (normalmente, sólo se analizan archivos recién creados mediante estos métodos). Por este motivo, se recomienda que no modifique los parámetros predeterminados de ThreatSense de todos los módulos, a excepción del Análisis del equipo.

4.1.7.1 Configuración de objetos

La sección **Objetos** le permite definir los componentes y archivos del equipo que se analizarán en busca de amenazas.



Memoria operativa: analiza en busca de amenazas que atacan a la memoria operativa del sistema.

Sectores de inicio: analiza los sectores de inicio en busca de virus en el registro de inicio principal

Archivos: proporciona análisis de todos los tipos de archivo comunes (programas, fotografías, audio, archivos de vídeo, archivos de base de datos, etc.).

Archivos de correo electrónico: analiza archivos especiales donde hay mensajes de correo.

Archivos comprimidos: proporciona análisis de archivos comprimidos en archivos (.rar, .zip, .arj, .tar, etc.).

Archivos comprimidos de auto extracción: analiza archivos incluidos en archivos comprimidos de auto extracción, pero que se suelen aparecer con la extensión .exe.

Empaquetadores en tiempo real: los empaquetadores en tiempo real (a diferencia de los tipos de archivo estándar) se descomprimen en la memoria, además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FGS, etc.).

4.1.7.2 Opciones

En la sección Opciones, el usuario puede seleccionar los métodos que va a utilizar para analizar el sistema en busca de amenazas. Las siguientes opciones están disponibles:

Firmas: las firmas pueden detectar amenazas de manera exacta y fiable e identificarlas por nombre mediante firmas de virus.

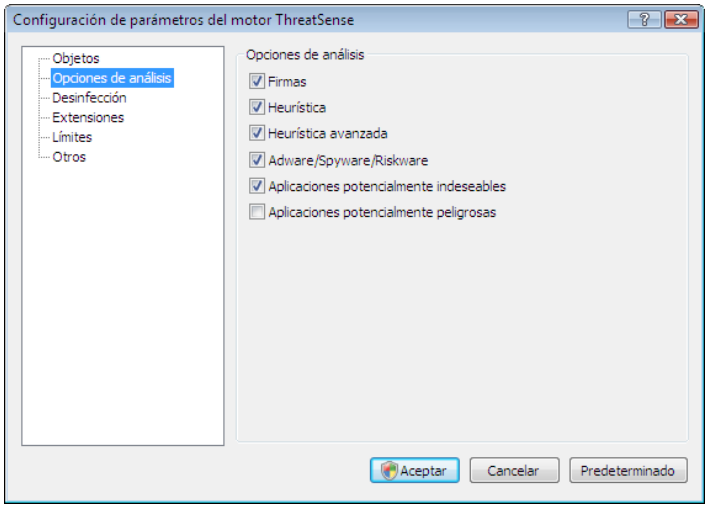
Heurística: la heurística hace referencia a un algoritmo que analiza la actividad (maliciosa) de los programas. Su principal ventaja es la habilidad para detectar nuevo software malicioso que no existía anteriormente o que no estaba incluido en la lista de virus conocidos (base de firmas de virus).

Heurística avanzada: la heurística avanzada consiste en un algoritmo heurístico exclusivo desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que estén escritos en lenguajes de programación de alto nivel. Gracias a la heurística avanzada, las capacidades de detección del programa son significativamente superiores.

Adware/Spyware/Riskware: esta categoría incluye software que recopila información importante sobre usuarios sin su consentimiento expreso, así como software que muestra material publicitario.

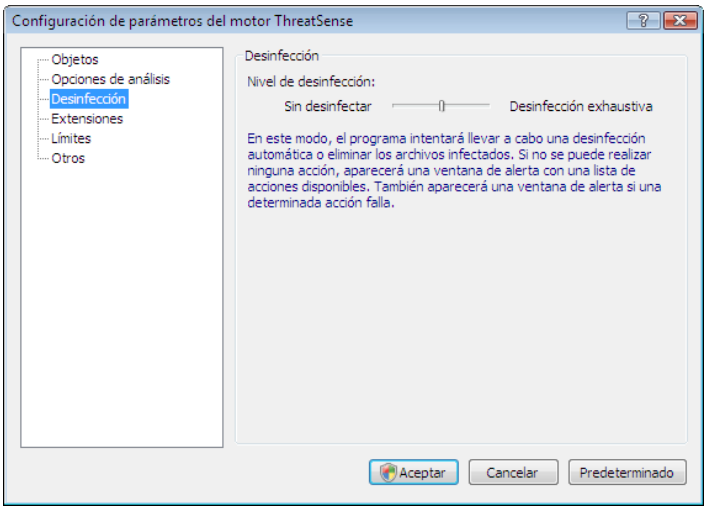
Aplicaciones potencialmente peligrosas: aplicaciones potencialmente peligrosas es la clasificación utilizada para el software comercial legítimo. Incluye programas como, por ejemplo, herramientas de acceso remoto, que es el motivo por el que esta opción está desactivada de forma predeterminada.

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



4.1.7.3 Desinfección

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



No desinfectar
Los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción.

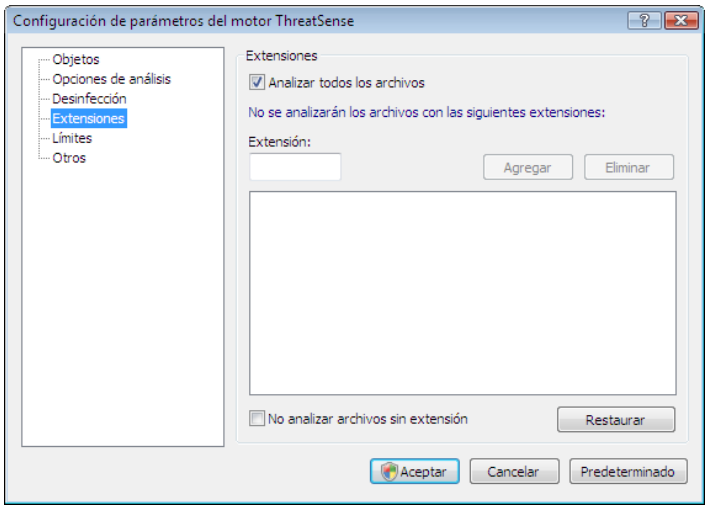
Nivel predeterminado
El programa intentará desinfectar o eliminar automáticamente un archivo infectado. Si no se puede seleccionar la acción correcta de manera automática, el programa ofrece una selección de acciones que se pueden seguir. La selección de acciones que se pueden seguir también aparecerá si una acción predefinida no puede completarse.

Desinfección estricta
El programa desinfectará o eliminará todos los archivos infectados (incluidos los archivos comprimidos). Las únicas excepciones son los archivos del sistema. Si no se pueden desinfectar, se le ofrece al usuario la opción de realizar una acción indicada en una ventana de alerta.

Advertencia:
En el modo predeterminado, se elimina todo el archivo comprimido sólo si todos los archivos que contiene están infectados. Si el archivo comprimido también contiene archivos legítimos, no se eliminará. Si se detecta un archivo comprimido infectado en el modo de desinfección estricta, se eliminará todo el archivo comprimido, incluso si contiene archivos desinfectados.

4.1.7.4 Extensiones

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



De forma predeterminada, todos los archivos se analizan independientemente de su extensión. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis. Si no está seleccionada la opción **Analizar todos los archivos**, la lista cambia para mostrar todas las extensiones de los archivos analizados actualmente. Con los botones **Agregar** y **Quitar**, puede activar o prohibir el análisis de las extensiones deseadas.

Para activar el análisis de archivos sin extensión, marque la opción **Analizar archivos sin extensión**.

La exclusión de archivos del análisis cumple su objetivo si el análisis de determinados tipos de archivos provoca un funcionamiento incorrecto del programa que utiliza las extensiones. Por ejemplo, quizás sea aconsejable excluir las extensiones .edb, .eml y .tmp cuando se utilice el servidor MS Exchange.

4.1.7.5 Límites

La sección Límites le permite especificar el tamaño máximo de los objetos y niveles de los archivos comprimidos anidados que se van a analizar:

Tamaño máximo del objeto (bytes)
Define el tamaño máximo de los objetos que se van a analizar. a continuación, el módulo antivirus establecido analizará únicamente los objetos con un tamaño inferior al especificado. No se recomienda cambiar el valor predeterminado, ya que no suele existir un motivo para su modificación. Esta opción sólo deben cambiarla usuarios avanzados con motivos específicos para excluir objetos de mayor tamaño del análisis.

Tiempo máximo de análisis para el objeto (seg.)
Define el valor del tiempo máximo para analizar un objeto. Si se ha introducido un valor definido por el usuario en esta opción, el módulo antivirus detendrá el análisis de un objeto cuando haya transcurrido ese tiempo, independientemente de si el análisis ha finalizado o no.

Nivel de anidamiento de archivos
Especifica la profundidad máxima del análisis de archivos comprimidos. No se recomienda cambiar el valor predeterminado de 10. En circunstancias normales, no existen motivos para modificarlo. Si el análisis finaliza antes de tiempo debido al número de archivos comprimidos anidados, el archivo comprimido quedará sin analizar.

Tamaño máx. de archivo en el archivo comprimido (bytes)
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 de un archivo comprimido finaliza antes de tiempo por ese motivo, éste quedará sin analizar.

4.1.7.6 Otros

Analizar secuencias de datos alternativas (ADS)
Las secuencias de datos alternativas (ADS) utilizadas por el sistema de archivos NTFS son asociaciones de carpetas y archivos invisibles con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por secuencias de datos alternativas.

Ejecutar análisis en segundo plano y con baja prioridad
Cada secuencia de análisis consume una cierta cantidad de recursos del sistema. Si trabaja con programas que colocan una gran carga en los recursos del sistema, puede activar el análisis en segundo plano con prioridad baja y ahorrar recursos para sus aplicaciones.

Registrar todos los objetos
Si se selecciona esta opción, el archivo de registro mostrará todos los archivos analizados, incluso aquéllos que no están infectados.

Conservar hora del último acceso
Active esta opción para mantener el tiempo de acceso original de los archivos analizados, en lugar de actualizarlo (por ejemplo, para su uso con sistemas de copia de seguridad de datos).

La Optimización Inteligente
La Optimización Inteligente está diseñada para potenciar el análisis de su sistema en búsqueda de códigos maliciosos. Cuando se encuentra activada, incrementa la velocidad del análisis, sin disminuir o afectar negativamente a la seguridad de su sistema.

Desplazar el registro de análisis
Esta opción le permite activar o desactivar el desplazamiento del registro. Si la selecciona, la información se desplaza hacia arriba dentro de la ventana de visualización.

Al finalizar el análisis mostrar una notificación en una nueva ventana
Abre una ventana independiente que contiene información sobre los resultados del análisis.

4.1.8 Detección de una amenaza

Las amenazas pueden obtener acceso al sistema desde varios puntos de entrada: páginas web, carpetas compartidas, a través del correo electrónico o desde dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Si el equipo muestra señales de infección por malware (por ejemplo, se ralentiza, se bloquea con frecuencia, etc.), recomendamos que haga lo siguiente:

- Abra ESET Smart Security y haga clic en **Análisis del equipo**
- Haga clic en **Análisis estándar** (para obtener más información, consulte"Análisis estándar").
- Una vez finalizado el análisis, consulte el registro para conocer el número de archivos analizados, infectados y desinfectados.

Si sólo desea analizar una parte específica del disco, seleccione **Análisis personalizado** y los objetos que se van a analizar en busca de virus.

Como ejemplo general de cómo se administran las amenazas en ESET Smart Security, suponga que el supervisor del sistema de archivos en tiempo real detecta una amenaza que utiliza el nivel de desinfección predeterminado. Intentará desinfectar o eliminar el archivo. Si no hay que realizar ninguna tarea predefinida para el

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

Desinfección y eliminación
Aplique esta opción si un archivo limpio ha sido infectado por un virus que ha agregado un código malicioso al archivo desinfectado. Si es el caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo se compone exclusivamente de código malicioso, se eliminará.

Si un proceso del sistema "bloquea" o está utilizando un archivo infectado, por lo general, sólo se eliminará una vez liberado (normalmente tras reiniciar el sistema).

Eliminación de amenazas en archivos comprimidos
En el modo de desinfección predeterminado, el archivo comprimido completo se eliminará sólo si contiene archivos infectados y ningún archivo limpio. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos desinfectados inofensivos. Sin embargo, tenga cuidado cuando realice un análisis con desinfección estricta, ya que el archivo se eliminará si contiene, como mínimo, un archivo infectado, sin tener en cuenta el estado de los otros archivos.

4.2 Cortafuegos personal

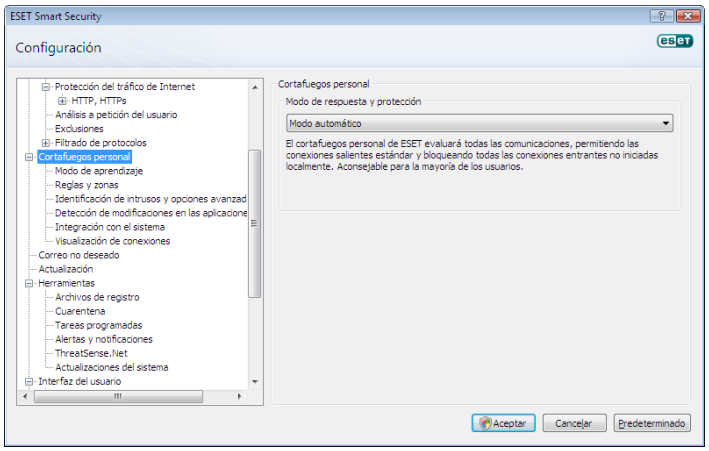
El cortafuegos personal se encarga de controlar todo el tráfico de red entrante y saliente del sistema. Esta tarea se lleva a cabo permitiendo o denegando conexiones de red individuales basadas en reglas de filtrado especificadas. Proporciona protección frente a ataques procedentes de equipos remotos y activa el bloqueo de determinados servicios. También ofrece protección antivirus para los protocolos HTTP y POP3. Esta funcionalidad representa un elemento muy importante para la seguridad del equipo.

4.2.1 Modos de filtrado

Existen tres modos de filtrado disponibles para el cortafuegos personal de ESET Smart Security. El comportamiento del cortafuegos cambia según el modo seleccionado. Los modos de filtrado influyen igualmente en el nivel de interacción del usuario.

El filtrado se puede realizar mediante uno de los siguiente cinco modos:

- El modo de filtrado automático es el modo predeterminado. Es aconsejable para usuarios que optan por un uso sencillo y cómodo del cortafuegos sin necesidad de definir reglas. Permite todo el tráfico saliente para el sistema en cuestión y bloquea todas las conexiones nuevas iniciadas desde la red.
- Modo automático con excepciones (reglas definidas por el usuario). Como complemento del modo automático, le permite agregar reglas personalizadas.
- El modo de filtrado interactivo permite crear una configuración personalizada para su cortafuegos personal. Cuando se detecta una comunicación y no existen reglas que se apliquen a la misma, aparece un cuadro de diálogo que notifica la existencia de una conexión desconocida El cuadro de diálogo ofrece la opción de permitir o denegar la comunicación; la decisión de permitir o denegar la misma se puede recordar como una regla nueva para el cortafuegos personal. Si el usuario opta por crear una nueva regla en este momento, todas las conexiones futuras de este tipo se permitirán o bloquearán de acuerdo con dicha regla.
- El modo basado en las directrices permite bloquear todas las conexiones que no se hayan definido en una regla específica que las permita. Este modo permite a todos los usuarios avanzados definir reglas que permitan únicamente las conexiones especificadas y seguras. El cortafuegos personal bloqueará el resto de conexiones no especificadas.
- El modo de aprendizaje permite crear y guardar automáticamente las reglas y se recomienda para la configuración inicial del cortafuegos personal. No es necesaria la intervención del usuario, ya que ESET Smart Security guarda las reglas de acuerdo con los parámetros predefinidos. El modo de aprendizaje no es seguro y sólo debe utilizarse hasta que se hayan creado todas las reglas de comunicaciones necesarias.



4.2.2 Bloquear todo el tráfico de red e impedir conexiones

La única forma de bloquear todo el tráfico de red por completo es utilizar la opción **Bloquear todo el tráfico de red e impedir conexiones**. De este modo, el cortafuegos personal bloqueará toda comunicación entrante o saliente sin mostrar ninguna ventana de alerta. Utilice esta opción de bloqueo si considera que existen riesgos de seguridad graves que requieran la desconexión del sistema de la red.

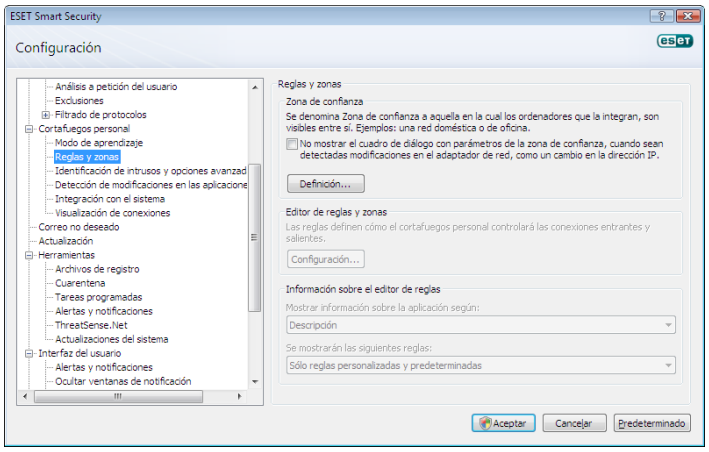
4.2.3 Desactivar filtro: permitir todo el tráfico

La opción para desactivar el filtro es la configuración opuesta a la mencionada anteriormente para bloquear todas las comunicaciones. Si se selecciona esta opción, todas las opciones de filtrado del cortafuegos personal se desactivan y se permiten todas las conexiones entrantes y salientes. En lo que respecta a la red, esta opción se comporta como si no hubiera ningún cortafuegos presente.

4.2.4 Configuración y uso de reglas

Las reglas representan un conjunto de condiciones que se utilizan para probar de manera significativa todas las conexiones de red y acciones asignadas a estas condiciones. En el cortafuegos personal, puede definir la acción que desee siempre que se haya establecido una conexión definida por una regla.

Para obtener acceso a la configuración del filtro de reglas, vaya a **Configuración avanzada** (F5) **> Cortafuegos personal > Reglas y zonas**. Para ver la configuración actual, haga clic en **Configuración...** en la sección **Editor de zonas y reglas** (si el cortafuegos personal se ha configurado en **Modo de respuesta y protección: Automático**, estas opciones no están disponibles).



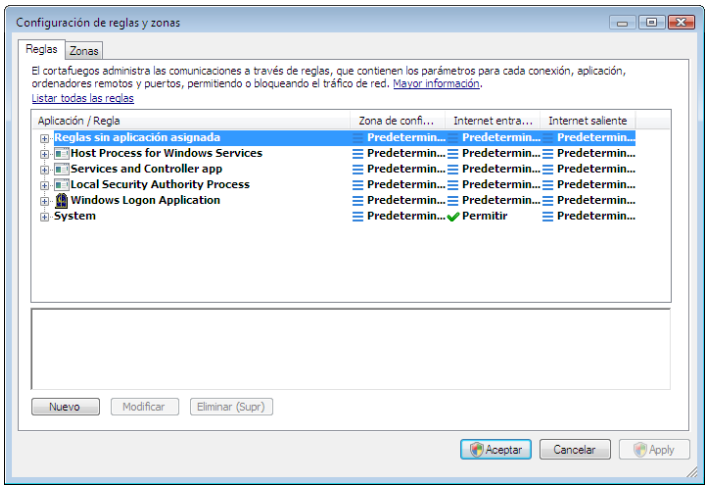
En la ventana **Configuración de reglas y zonas**, se muestra información general acerca de las reglas o las zonas (en función de la pestaña seleccionada actualmente). La ventana se divide en dos secciones. En la sección superior, se enumeran todas las reglas en una vista abreviada. En la sección inferior, se muestra información detallada acerca de la regla seleccionada actualmente en la sección superior. En la parte de abajo, se encuentran los botones **Nuevo**, **Modificar**, y **Eliminar**, que permiten al usuario configurar las reglas.

Si se tiene en cuenta la dirección de comunicación, se pueden dividir las conexiones en entrantes y salientes. Las conexiones entrantes se inician en equipos remotos que intentan establecer una conexión con el sistema local. Las conexiones salientes funcionan de la forma opuesta, es decir, la ubicación local se comunica con el equipo remoto.

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

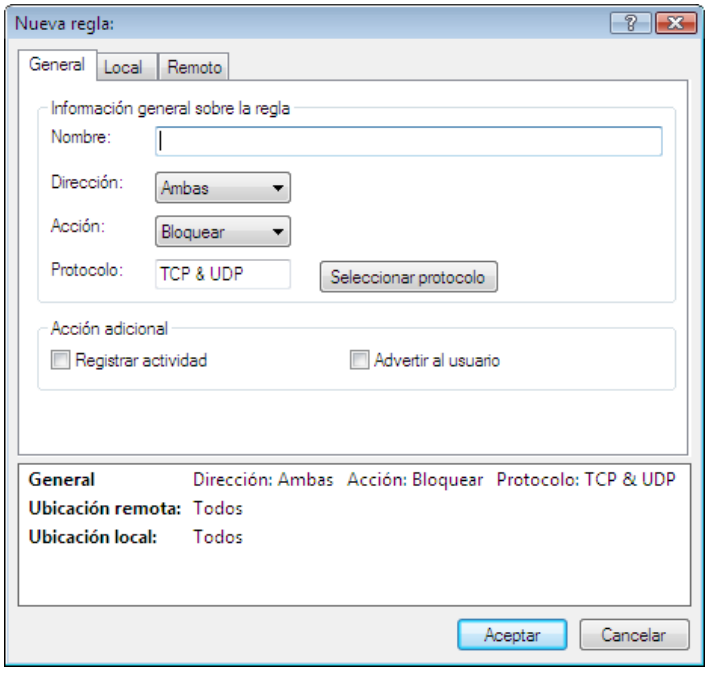
4.2.4.1 Creación de nuevas reglas

Cuando se instala una nueva aplicación que puede obtener acceso a la red o si se lleva a cabo una modificación en una conexión existente (ubicación remota, número de puerto, etc.), es necesario crear una regla nueva.



Para agregar una nueva regla, verifique que la pestaña **Reglas** está seleccionada. A continuación, haga clic en el botón **Nuevo** en la ventana de configuración de **reglas y zonas**. Al hacer clic en este botón, se abre un nuevo cuadro de diálogo que permite especificar una regla nueva. La parte superior del cuadro contiene las tres pestañas siguientes:

- General: especifica el nombre de la regla, la dirección, la acción y el protocolo. La dirección puede ser de entrada o de salida (o ambas). La acción implica el hecho de permitir o denegar la conexión en sí.
- Local: muestra información acerca de la ubicación local de la conexión, incluido el número del puerto local o el intervalo de puertos y el nombre de la aplicación que intenta establecer la comunicación.
- Remoto: esta pestaña contiene información acerca del puerto remoto (o rango de puertos). También permite al usuario definir una lista de direcciones IP remotas o zonas para una regla determinada.



Un buen ejemplo de la adición de una nueva regla es la acción de permitir a su navegador de Internet obtener acceso a la red. En este caso, es necesario realizar la siguiente configuración:

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

4.2.4.2 Modificación de reglas

Para modificar una regla existente, haga clic en el botón **Modificar**. Se pueden modificar todos los parámetros mencionados anteriormente (que se describen en el capítulo "Creación de nuevas reglas").

Esta modificación es necesaria cada vez que se cambia alguno de los parámetros controlados. Como resultado, la regla no cumple las condiciones y la acción especificada no se puede aplicar. Finalmente, es probable que se rechace la conexión en cuestión, lo que puede conllevar problemas relacionados con el funcionamiento de la aplicación correspondiente. Un ejemplo de este caso sería la modificación de la dirección de red o del número de puerto de la ubicación remota.

4.2.5 Configuración de zonas

Una zona representa un grupo de direcciones de red que crea un grupo lógico.Consecuentemente, a cada dirección del grupo concreto se asignan reglas similares definidas de manera centralizada para todo el grupo. Un ejemplo de dicho grupo es la Zona de confianza, que representa un grupo de direcciones de red en las que el usuario puede confiar completamente y que no están bloqueadas de forma alguna por el cortafuegos personal.

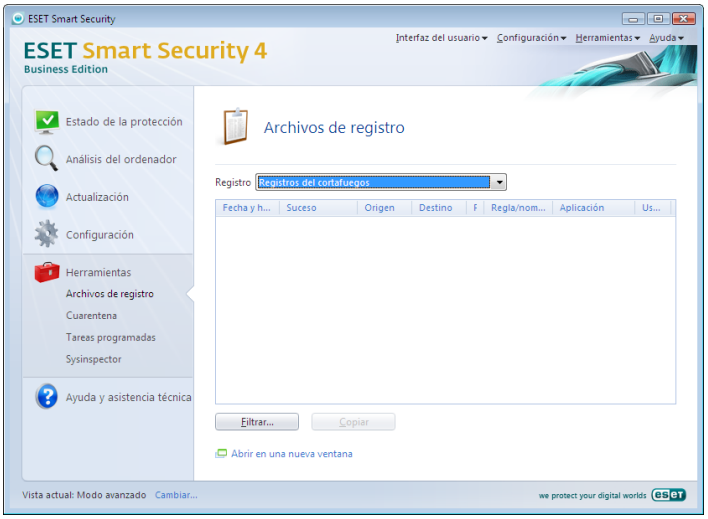
Puede configurar estas zonas utilizando la pestaña **Zonas** que aparece en la ventana **Configuración de reglas y zonas** haciendo clic en el botón **Nuevo**. Escriba el nombre de la zona, su descripción y la lista de direcciones de red en la ventana que acaba de abrir.

4.2.6 Establecimiento de una conexión: detección

El cortafuegos personal detecta cualquier conexión de red nueva. El modo del cortafuegos activo (automático, interactivo o basado en las directrices) determina las acciones que se deben realizar para la nueva regla. Al activar el modo automático o basado en las directrices, el cortafuegos personal llevará a cabo las acciones predefinidas sin necesidad de que intervenga el usuario. En el modo interactivo, se muestra una ventana informativa que notifica la detección de una nueva conexión de red, con información adicional acerca de dicha conexión. El usuario tiene la opción de permitir la conexión o de rechazarla (bloquearla). Si el usuario permite en repetidas ocasiones la misma conexión en el cuadro de diálogo, se recomienda que cree una regla nueva para la conexión. Para realizar esta tarea, seleccione la opción **Recordar acción** (crear regla) y guárdela como una nueva regla para el cortafuegos personal. Si el cortafuegos reconoce la misma conexión en el futuro, se aplicará la regla existente.

Tenga cuidado cuando cree reglas nuevas y permita únicamente las conexiones que sean seguras. Si se permiten todas las conexiones, el cortafuegos personal no podrá cumplir su finalidad. a continuación, se indica una serie de parámetros importantes para las conexiones:

- **Ubicación remota:** sólo se permiten las conexiones a direcciones conocidas y de confianza.
- **Aplicación local:** no es recomendable permitir conexiones de aplicaciones y procesos desconocidos.
- **Número de puertos:** la comunicación en puertos comunes (por ejemplo, Internet: número de puerto 80) suele ser segura.



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

4.2.7 Registro

El cortafuegos personal que incluye ESET Smart Security guarda sucesos importantes en un archivo de registro que se puede consultar directamente en el menú principal. Haga clic en **Herramientas > Archivos de registro** y, a continuación, seleccione **Registros del cortafuegos personal de ESET** en el menú desplegable **Registro**.

Los archivos de registro constituyen una herramienta muy valiosa para la detección de errores y el descubrimiento de amenazas, por lo que debe tenerlos en cuenta. Los registros del cortafuegos personal de ESET contienen los siguientes datos:

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

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

4.3 Protección contra correo no deseado

Hoy en día, el correo electrónico no deseado (spam) es uno de los problemas más graves de la comunicación electrónica. Representa hasta el 80% de todas las comunicaciones por correo electrónico. La protección contra correo no deseado sirve para protegerse frente a este problema. Combinando varios principios muy eficaces, el módulo contra correo no deseado ofrece un filtrado superior.

Un principio importante en la detección del correo no deseado es la capacidad de reconocer correo electrónico no solicitado basándose en direcciones de confianza predefinidas (lista blanca) y direcciones de correo no deseado (lista negra). Todas las direcciones de su cliente de correo electrónico se agregan automáticamente a la lista blanca, además del resto de direcciones marcadas por el usuario como seguras.

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

El filtro Bayesiano también se utiliza para filtrar. Al marcar los mensajes como *no deseados* y *deseados*, el usuario crea una base de datos de palabras utilizadas en la categoría correspondiente. Cuanto mayor sea la base de datos, más precisos serán los resultados.

Una combinación de los métodos mencionados anteriormente aporta un alto índice de detección de correo no deseado.

ESET Smart Security admite la protección contra correo no deseado para Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail y Mozilla Thunderbird.

4.3.1 Autoaprendizaje contra correo no deseado

El autoaprendizaje contra correo no deseado está relacionado con el filtro Bayesiano anteriormente mencionado. La importancia de palabras individuales cambia durante el proceso de "aprendizaje" para marcar mensajes individuales como deseados o no deseados. En consecuencia, cuantos más mensajes se clasifiquen (marcados como deseados o no deseados), más precisos serán los resultados obtenidos con el filtro Bayesiano.

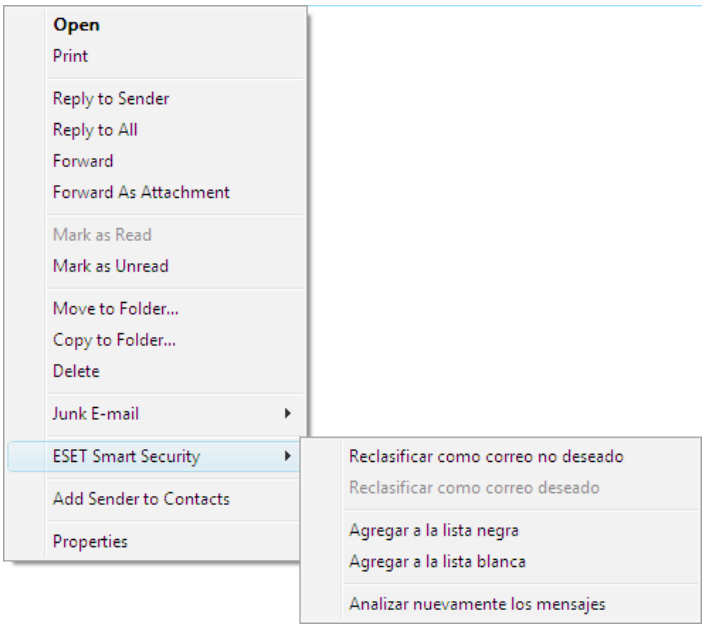
Agregue direcciones conocidas a la lista blanca para excluir del filtrado los mensajes enviados desde estas direcciones.

4.3.1.1 Adición de direcciones a la lista blanca

Las direcciones de correo electrónico que pertenecen a personas con las que el usuario se comunica frecuentemente se pueden agregar a la lista de direcciones "seguras", es decir, la lista blanca. De esta manera, se garantiza que ningún mensaje que proceda de una dirección de la lista blanca se clasifique como correo no deseado. Para agregar una nueva dirección a la lista blanca, haga clic con el botón secundario en el mensaje de correo electrónico deseado y seleccione **Agregar a la lista blanca** en la opción del menú contextual de ESET Smart Security, o haga clic en **Direcciones de confianza** en la barra de herramientas contra correo no deseado de ESET Smart Security en la parte superior de su programa de correo electrónico. Este proceso también se aplica a direcciones de correo no deseado. Si una dirección de correo electrónico aparece en la lista negra, cada mensaje de correo electrónico enviado desde esa dirección se clasifica como no deseado.

4.3.1.2 Marcado de mensajes como correo no deseado

Cualquier mensaje que aparezca en su cliente de correo electrónico puede marcarse como correo no deseado. Para ello, utilice el menú contextual (haga clic con el botón secundario en **ESET Smart Security > Reclasificar como correo no deseado**), o haga clic en **Correo no deseado** en la barra de herramientas contra correo no deseado de ESET Smart Security ubicada en su cliente de correo electrónico.



Los mensajes reclasificados se mueven automáticamente a la carpeta SPAM, pero la dirección de correo electrónico del remitente no se agregará a la lista negra. del mismo modo, los mensajes se pueden

clasificar como "deseados". Si los mensajes de la carpeta de **correo basura** se clasifican como deseados, se moverán a la carpeta original. Al marcar un mensaje como deseado, no se agrega automáticamente la dirección del remitente a la lista blanca.

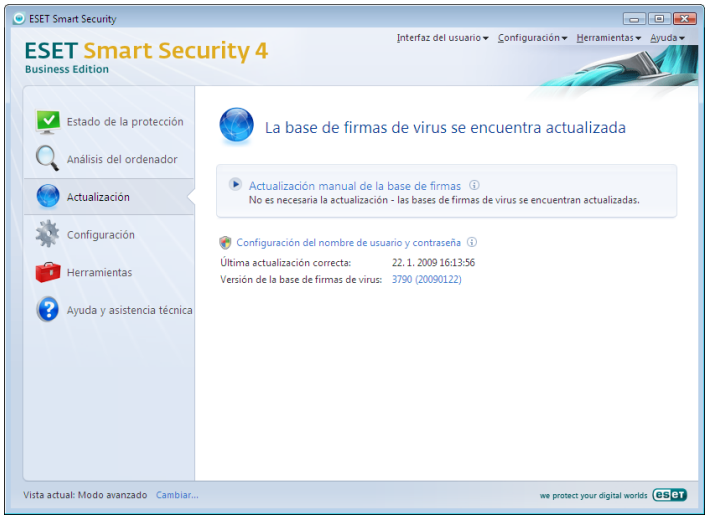
4.4 Actualización del programa

La actualización regular del sistema es la condición básica para obtener el nivel máximo de seguridad que proporciona ESET Smart Security. El módulo de actualización garantiza que el programa esté siempre actualizado. Esta tarea se lleva a cabo de dos formas: mediante la actualización de la base de firmas de virus y la actualización de los componentes del sistema.

Puede consultar información acerca del estado actual de actualización haciendo clic en **Actualizar**, como la versión actual de la base de firmas de virus donde, además, se especifica si es necesario actualizarla. También está disponible la opción que permite activar el proceso de actualización inmediatamente, (**Actualización manual de la base de firmas de virus**), así como las opciones de configuración de actualizaciones básicas, como el nombre de usuario y la contraseña para obtener acceso a los servidores de actualización de ESET.

La ventana de información también contiene detalles como la fecha y la hora de la última actualización realizada correctamente y el número de la base de firmas de virus. Esta indicación numérica es un vínculo activo al sitio web de ESET en el que se muestran todas las firmas agregadas en la actualización correspondiente.

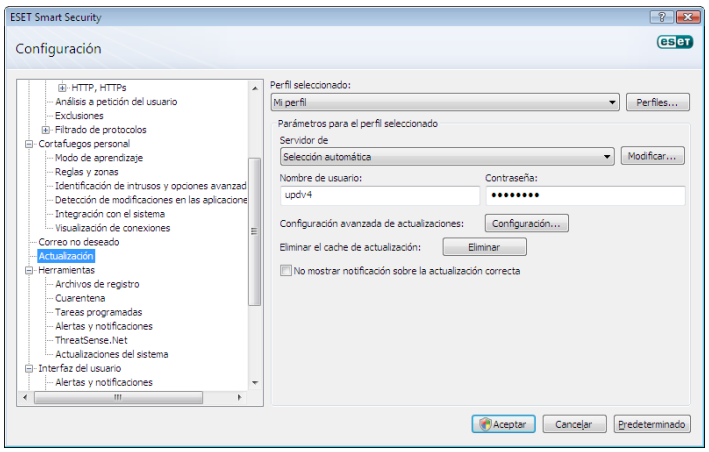
Utilice el vínculo **Registrar** para abrir el formulario de registro que le permitirá registrar su nueva licencia con ESET y, a continuación, recibirá sus datos de autentificación por correo electrónico.



NOTA: ESET facilita el nombre de usuario y la contraseña tras la compra de ESET Smart Security.

4.4.1 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 los datos de autentificación para los mismos. De forma predeterminada, el campo **Servidor de actualización:** está establecido en **Selección automática**. Este valor garantiza que los archivos actualizados se descargarán automáticamente del servidor ESET con la menor carga de tráfico de red. Las opciones de configuración de actualización están disponibles en el árbol Configuración avanzada (F5) en **Actualizar**.



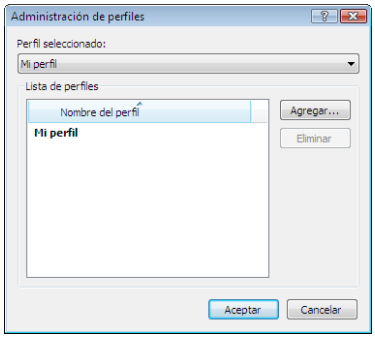
Puede desplazarse a la lista de servidores de actualización existentes actualmente a través del menú desplegable **Servidor de actualización:** Para agregar un nuevo servidor de actualización, haga clic en **Modificar...** en la sección **Parámetros para el perfil seleccionado** y, a continuación, haga clic en el botón **Agregar**.

La autentificación en los servidores de actualización se lleva a cabo mediante el **Nombre de usuario** y la **Contraseña** generados y enviados al usuario por ESET tras la adquisición de la licencia del producto.

4.4.1.1 Perfiles de actualización

Es posible crear perfiles de actualización definidos por el usuario, que se pueden utilizar para una tarea de actualización determinada para distintas configuraciones de actualización. La creación de varios perfiles de actualización resulta especialmente útil para usuarios móviles, ya que las propiedades de conexión a Internet cambian con frecuencia. Mediante la modificación de la tarea de actualización, los usuarios móviles pueden determinar que, si no es posible actualizar el programa con la configuración especificada en **Mi perfil**, la actualización se realizará mediante el uso de un perfil alternativo.

En el menú desplegable **Perfil seleccionado**, se muestra el perfil seleccionado actualmente. De forma predeterminada, esta entrada se establece en la opción **Mi perfil**. Para crear un perfil nuevo, haga clic en el botón **Perfiles...** y, a continuación, en el botón **Agregar...** e introduzca su **Nombre de perfil**. Durante la creación de un perfil nuevo, puede copiar parámetros de uno existente seleccionándolo en el menú desplegable **Copiar parámetros desde el perfil:**



En la configuración del perfil, se puede especificar el servidor de actualización al que se conectará el programa y descargar las actualizaciones; se puede utilizar cualquier servidor de la lista de servidores disponibles o agregar un servidor nuevo. Puede desplazarse a la lista de servidores de actualización existentes a través del menú desplegable **Servidor de actualización:** Para agregar un nuevo servidor de actualización, haga clic en **Modificar...** en la sección **Parámetros para el perfil seleccionado** y, a continuación, en el botón **Agregar**.

4.4.1.2 Configuración avanzada de actualizaciones

Para ver la **Configuración avanzada de actualizaciones**, haga clic en el botón **Configuración...**. Entre las opciones de la configuración avanzada de actualizaciones, se incluyen la configuración de **Tipo de actualización, Servidor Proxy HTTP, LAN** y **Servidor local de actualización**.

4.2.1.2.1 Tipo de actualización

La pestaña **Tipo de actualización** contiene las opciones relacionadas con la actualización de componentes del programa.

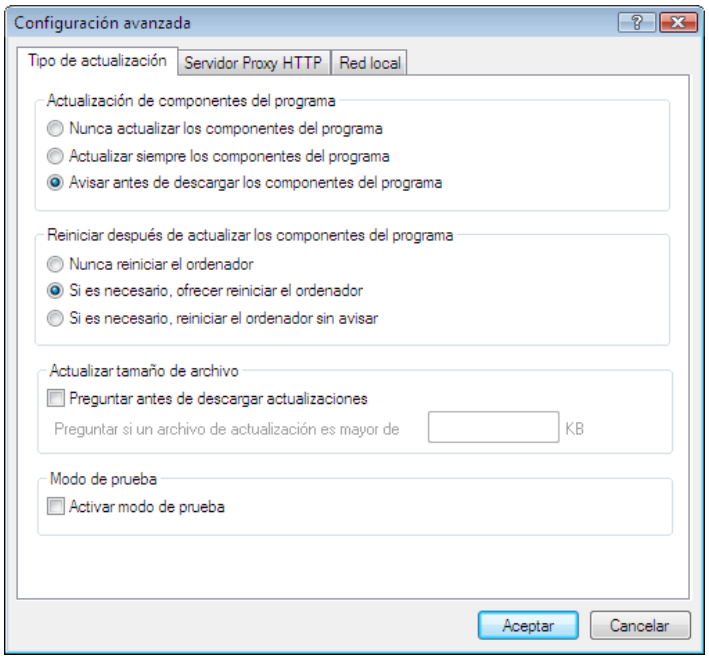
En la sección **Actualización de componentes del programa**, hay tres opciones disponibles:

- **Nunca actualizar los componentes del programa**
- **Actualizar siempre los componentes del programa**
- **Avisar antes de descargar los componentes del programa**

Si selecciona la opción **Nunca actualizar los componentes del programa**, se asegura de que no se descargarán nuevas actualizaciones de componentes del programa publicadas por ESET y de que no se llevará a cabo actualización de componentes del programa alguna en la estación de trabajo en cuestión. La opción **Actualizar siempre los componentes del programa** implica que las actualizaciones de componentes del programa se realizarán cada vez que esté disponible una nueva actualización en los servidores de actualización de ESET y que los componentes del programa se actualizarán a la versión descargada.

Seleccione la tercera opción, **Avisar antes de descargar los componentes del programa**, para asegurarse de que el programa confirme la descarga de actualizaciones de componentes del programa en el momento en el que estén disponibles las mismas. En este caso, aparecerá un cuadro de diálogo con información acerca de las actualizaciones de componentes del programa disponibles con la opción para confirmar o denegar. En caso de que confirme, se descargarán las actualizaciones y se instalarán los nuevos componentes del programa.

La opción predeterminada para una actualización de componentes del programa es **Avisar antes de descargar los componentes del programa**.



Tras la instalación de una actualización de componentes del programa, es necesario reiniciar el sistema para disponer de todas las funciones de los módulos. La sección **Reiniciar después de actualizar los componentes del programa** permite al usuario seleccionar unas de las tres opciones siguientes:

- **Nunca reiniciar el ordenador**
- **Si es necesario, ofrecer reiniciar el ordenador**
- **Si es necesario, reiniciar el ordenador sin avisar**

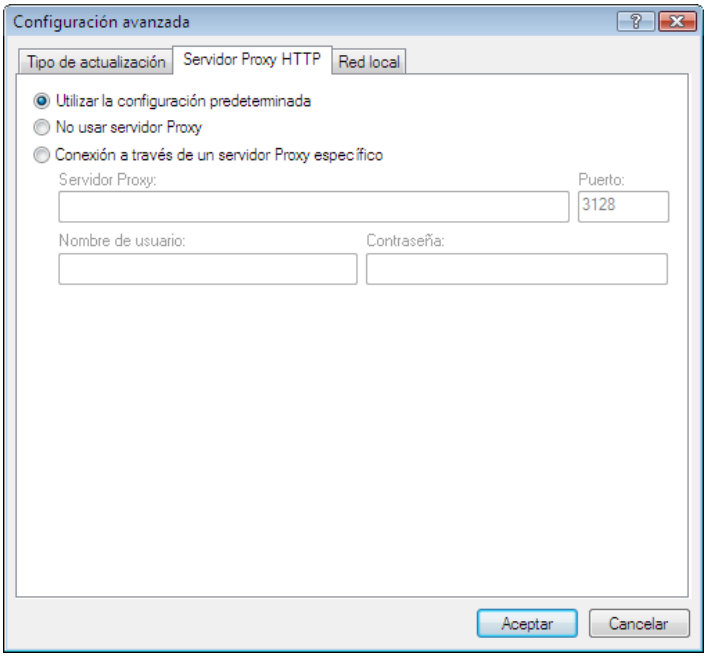
La opción predeterminada para reiniciar es **Si es necesario, ofrecer reiniciar el ordenador**. La selección de las opciones más adecuadas para las actualizaciones de componentes del programa en la pestaña **Tipo de actualización** depende de cada estación de trabajo individual, ya que es en ésta donde se debe aplicar la configuración. Tenga en cuenta que existen ciertas diferencias entre estaciones de trabajo y servidores, por ejemplo, el reinicio automático del servidor tras una actualización del programa podría causar daños graves.

4.4.1.2.2 Servidor Proxy

Para obtener acceso a las opciones de configuración del servidor Proxy para un perfil de actualización especificado: Haga clic en **Actualizar** en el árbol Configuración avanzada (F5) y, a continuación, en el botón **Configuración...** a la derecha de **Configuración avanzada de actualizaciones.** Haga clic en la pestaña **Servidor Proxy HTTP** y seleccione una de las tres opciones siguientes:

- **Utilizar la configuración predeterminada**
- **No usar servidor Proxy**
- **Conexión a través de un servidor Proxy específico** (conexión definida por las propiedades de conexión)

Si selecciona la opción **Utilizar la configuración predeterminada**, se utilizarán las opciones de configuración del servidor Proxy ya especificadas en el apartado **Varios > Servidor Proxy** del árbol Configuración avanzada.



Seleccione la opción **No usar servidor Proxy** para definir de forma explícita que no se utilice ningún servidor Proxy para actualizar ESET Smart Security.

Debe seleccionarse la opción **Conexión a través de un servidor Proxy específico** si se va a utilizar un servidor Proxy para actualizar ESET Smart Security diferente del especificado en la configuración global (**Varios > Servidor Proxy**). En este caso, será necesario especificar la configuración aquí: Dirección de **Servidor Proxy**, **Puerto** de comunicación, junto con **Nombre de usuario** y **Contraseña** para el servidor Proxy si es necesario.

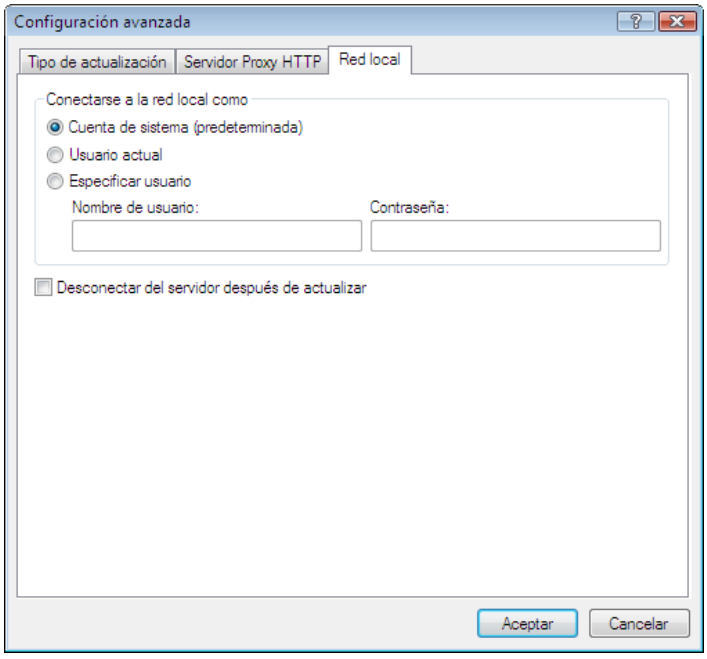
Esta opción también se debe seleccionar si la configuración del servidor Proxy no se ha establecido globalmente, pero, aún así, ESET Smart Security establecerá una conexión con un servidor Proxy en busca de actualizaciones.

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

4.4.1.2.3 Conexión a la red local

Para realizar una actualización desde un servidor local en el que se ejecute un sistema operativo basado en NT, es necesario autenticar todas las conexiones de red de forma predeterminada. En la mayoría de los casos, una cuenta de sistema local no dispone de los derechos suficientes para obtener acceso a la carpeta Servidor local de actualización (que contiene copias de archivos actualizados). En este caso, escriba su nombre de usuario y contraseña en la sección de configuración de actualizaciones o especifique una cuenta existente con la que el programa pueda obtener acceso al servidor de actualización (Servidor local de actualización).

Para configurar esta cuenta, haga clic en la pestaña **Red local**. La sección **Conectarse a la red local como** ofrece las opciones **Cuenta de sistema (predeterminada)**, **Usuario actual** y **Especificar usuario**.



Seleccione la opción **Cuenta de sistema (predeterminada)** para utilizar la cuenta de sistema para la autentificación. Normalmente, no tiene lugar ningún proceso de autentificación si no se proporcionan datos para ésta en la sección de configuración de actualizaciones.

Para garantizar que el programa se autorice a sí mismo a utilizar la cuenta de un usuario registrado actualmente, seleccione **Usuario actual**. El inconveniente de esta solución es que el programa no puede conectarse al servidor de actualizaciones si no hay ningún usuario registrado actualmente.

Seleccione **Especificar usuario** si desea que el programa utilice una cuenta de usuario específica para la autentificación.

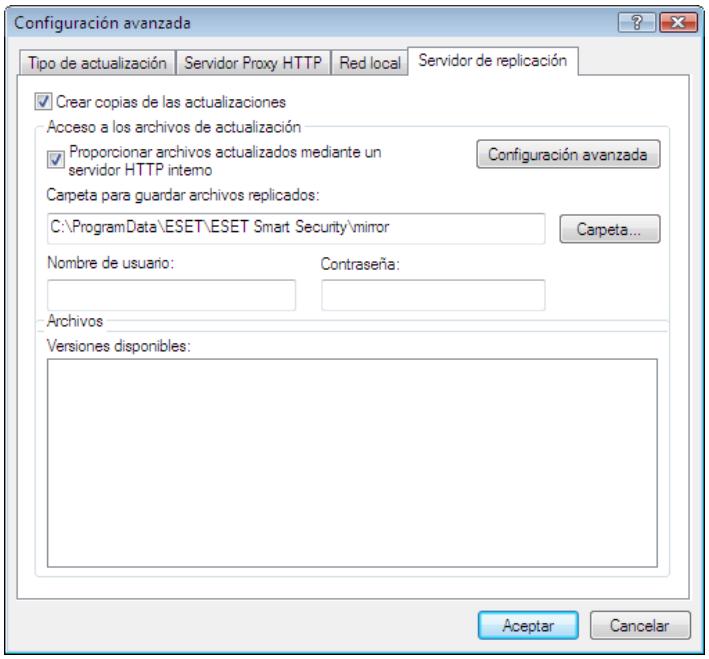
La opción predeterminada de la conexión de red local es **Cuenta de sistema**.

Advertencia:
Cuando se activa la opción **Usuario actual** o **Especificar usuario**, puede producirse un error al cambiar la identidad del programa al usuario deseado. Por este motivo, se recomienda que inserte los datos de autentificación de la red local en la sección principal de configuración de actualizaciones, donde los datos de autentificación se deben introducir de la forma siguiente: nombre_dominio\usuario (si es un grupo de trabajo, escriba nombre_grupo de trabajo\nombre) y la contraseña del usuario. Cuando se actualiza desde la versión HTTP del servidor local, no es necesaria ninguna autentificación.

4.4.1.2.4 Creación de copias de actualización: servidor local de actualización

ESET Smart Security Business Edition permite al usuario crear copias de archivos actualizados que se pueden utilizar para actualizar otras estaciones de trabajo ubicadas en la red. La actualización de estaciones de trabajo cliente desde un servidor local de actualización optimiza el equilibrio de carga de la red y ahorra ancho de banda de conexión a Internet.

Las opciones de configuración del servidor local de actualización están disponibles (tras agregar una clave de licencia válida en el administrador de licencias, ubicado en la sección Configuración avanzada de ESET Smart Security Business Edition) en la sección **Configuración avanzada de actualizaciones:** (para obtener acceso a esta sección, pulse F5 y haga clic en **Actualizar** en el árbol Configuración avanzada. Haga clic en el botón **Configuración** junto a **Configuración avanzada de actualizaciones:** y seleccione la pestaña **Servidor local de actualización**).



El primer paso para configurar el servidor local de actualización es seleccionar la casilla de verificación **Crear copias de las actualizaciones**. Al seleccionar dicha opción, se activan otras opciones de configuración de servidor local de actualización, como la forma de obtener acceso a los archivos actualizados y la ruta de actualización a los archivos replicados.

Los métodos de activación del servidor local de actualización se describen en el siguiente capítulo, "Otras formas de acceso al servidor local de actualización". En estos momentos, tenga en cuenta que existen dos formas básicas de obtener acceso al servidor local de actualización: la carpeta con los archivos actualizados se puede presentar como una carpeta de red compartida o como un servidor HTTP.

La carpeta destinada a almacenar los archivos actualizados para el servidor local de actualización se define en la sección **Carpeta para guardar archivos replicados**. Haga clic en **Carpeta...** para buscar la carpeta deseada en el equipo local o en la carpeta de red compartida. Si es necesaria una autorización para la carpeta especificada, deberá proporcionar los datos de autentificación en los campos **Nombre de usuario** y **Contraseña**. El nombre de usuario y la contraseña se deben introducir con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. No olvide que debe introducir las contraseñas correspondientes.

Cuando se especifique la configuración detallada del servidor local de actualización, el usuario también puede establecer las versiones de idiomas en las que desee descargar las copias de actualización. La configuración de la versión de idioma se encuentra en la sección **Archivos > Versiones disponibles:**

4.4.1.2.4.1 Actualización desde el servidor local de actualización

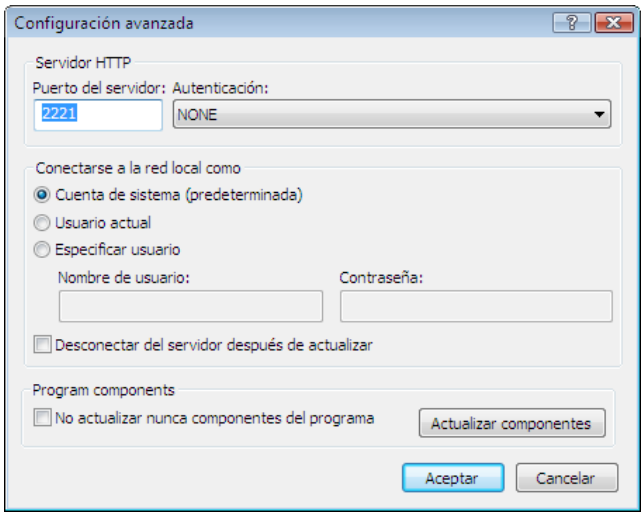
Existen dos formas básicas de obtener acceso al servidor local de actualización: la carpeta con los archivos actualizados se puede presentar como una carpeta de red compartida o como un servidor HTTP.

Acceso al servidor local de actualización mediante un servidor HTTP interno

Esta configuración es la predeterminada, especificada en la configuración del programa predefinida. Para obtener acceso al servidor local de actualización utilizando el servidor HTTP, vaya a **Configuración avanzada de actualizaciones** (la pestaña **Servidor local de actualización**) y seleccione la opción **Crear copias de las actualizaciones**.

En la sección **Configuración avanzada** de la pestaña **Servidor local de actualización**, puede especificar el **Puerto del servidor** en el que se encontrará en escucha el servidor HTTP, además del tipo de **Autentificación** que debe utilizar dicho servidor. De forma predeterminada, el puerto del servidor se establece en el valor **2221**. La opción **Autentificación** define el método de autentificación utilizado para obtener acceso a los archivos actualizados. Las siguientes opciones están disponibles: **NONE, Basic,** y **NTLM**. Seleccione **Basic** para utilizar la codificación base64 con la autentificación básica de nombre de usuario y contraseña. La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autentificación, se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados. La configuración predeterminada es **NONE** que concede acceso a los archivos actualizados sin necesidad de autentificación.

Advertencia:
Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta del servidor local de actualización debe encontrarse en el mismo equipo que la instancia de ESET Smart Security que vaya a crearla.



Una vez finalizada la configuración del servidor local de actualización, vaya a las estaciones de trabajo y agregue un nuevo servidor de actualizaciones con el formato **http://dirección_IP_de_su_servidor:2221**. Para realizar esta tarea, siga estos pasos:

- Abra **Configuración avanzada de ESET Smart Security** y haga clic en el apartado **Actualizar**.
- Haga clic en **Modificar...** a la derecha del menú desplegable **Servidor de actualización** y agregue un nuevo servidor utilizando el siguiente formato: http://dirección_IP_de_su_servidor:2221
- Seleccione el servidor que acaba de agregar en la lista de servidores de actualización.

Acceso al servidor local de actualización mediante el uso compartido del sistema

En primer lugar, se debe crear una carpeta compartida en un dispositivo local o de red. a la hora de crear el servidor local de actualización, es necesario proporcionar el acceso de "escritura" para el usuario que va a guardar los archivos en la carpeta y el acceso de "lectura" para todos los usuarios que van a actualizar ESET Smart Security desde la carpeta del servidor local de actualización.

A continuación, configure el acceso al servidor local de actualización en la sección **Configuración avanzada de actualizaciones** (la pestaña **Servidor local de actualización**) desactivando la opción **Proporcionar archivos actualizados mediante un servidor HTTP interno**. Esta opción se activa de forma predeterminada en el paquete de instalación del programa.

Si la carpeta compartida se encuentra en otro equipo de la red, es necesario especificar los datos de autentificación para obtener acceso al otro equipo. Para especificar los datos de autentificación, abra Configuración avanzada de ESET Smart Security (F5) y haga clic en el apartado **Actualizar**. Haga clic en el botón **Configuración...** y, a continuación, en la pestaña **Red local**. Esta configuración es la misma que se aplica a las actualizaciones, como se describe en el capítulo "Conexión a la red local".

Una vez finalizada la configuración del servidor local de actualización, continúe con las estaciones de trabajo y establezca \\UNC\RUTA como servidor de actualización. Esta operación se puede completar mediante los siguientes pasos:

- Abra la Configuración avanzada de ESET Smart Security y haga clic en **Actualizar**
- Haga clic en **Modificar...** junto a Servidor de actualización y agregue un nuevo servidor con el formato \\UNC\RUTA.
- Seleccione el servidor que acaba de agregar en la lista de servidores de actualización.

NOTA: para un correcto funcionamiento, es necesario especificar la ruta a la carpeta del servidor local de actualización como una ruta UNC. Es posible que no funcionen las actualizaciones de las unidades asignadas.

4.4.1.2.4.2 Resolución de problemas con actualizaciones del servidor local de actualización

En función de la forma de acceso a la carpeta del servidor local de actualización, se pueden producir distintos tipos de problemas. En la mayoría de los casos, los problemas causados durante la actualización desde un servidor local de actualización se deben a: la especificación incorrecta de las opciones de la carpeta del servidor local de actualización, la introducción de datos de autentificación no válidos para la carpeta del servidor local de actualización, la configuración incorrecta de las estaciones de trabajo locales que intentan descargar archivos de actualización del servidor local de actualización o una combinación de los casos anteriores. a continuación, se ofrece información general acerca de los problemas más frecuentes durante la actualización desde el servidor local de actualización:

- **ESET Smart Security notifica un error al conectarse al servidor local de actualización:** suele deberse a la especificación incorrecta del servidor de actualización (ruta de red a la carpeta del servidor local de actualización) desde donde se actualizan las descargas de las estaciones de trabajo locales. Para verificar la carpeta, haga clic en el **menú Inicio** de Windows, a continuación, en **Ejecutar**, inserte el nombre de la carpeta y haga clic en **Aceptar**. A continuación, debe aparecer el contenido de la carpeta.

- **ESET Smart Security requiere un nombre de usuario y una contraseña:** suele producirse por la introducción de datos de autentificación no válidos (nombre de usuario y contraseña) en la sección de actualización. El nombre de usuario y la contraseña se utilizan para conceder acceso al servidor de actualización, desde el que se actualiza el programa. Asegúrese de que los datos de autentificación sean correctos y se introduzcan con el formato adecuado. Por ejemplo, *Dominio/Nombre de usuario* o *Grupo de trabajo/Nombre de usuario*, junto con las contraseñas correspondientes. Si "Todos" pueden obtener acceso al servidor local de actualización, debe ser consciente de que esto no quiere decir que cualquier usuario tenga acceso. "Todos" no hace referencia a cualquier usuario no autorizado, tan sólo significa que todos los usuarios del dominio pueden tener acceso a la carpeta. Como resultado, si "Todos" pueden tener acceso a la misma, será igualmente necesario introducir un nombre de usuario y una contraseña en la sección de configuración de actualizaciones.

- **ESET Smart Security notifica un error al conectarse al servidor local de actualización:** la comunicación del puerto definida para obtener acceso a la versión HTTP del servidor local de actualización está bloqueada.

4.4.2 Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente haciendo clic en **Actualización manual de la base de firmas de virus** en la ventana de información que aparece tras hacer clic en **Actualizar** en el menú principal**.**

Las actualizaciones también se pueden ejecutar como tareas programadas: para configurar una tarea programada, haga clic en **Herramientas > Tareas programadas**. Las siguientes tareas se activan en ESET Smart Security de forma predeterminada:

- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**

Cada una de las tareas mencionadas anteriormente se puede modificar para cumplir sus necesidades. Además de las tareas de actualización predeterminadas, puede crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más información acerca de la creación y la configuración de tareas de actualización, consulte el capítulo "Tareas programadas".

4.5 Tareas programadas

La característica Tareas programadas está disponible si está activado el modo avanzado en ESET Smart Security. **Tareas programadas** puede encontrarse en el menú principal de ESET Smart Security en **Herramientas**. Esta característica contiene una lista resumida de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

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

- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**
- **Verificación de la ejecución de archivos en el inicio después del registro del usuario**
- **Verificación automática de la ejecución de archivos en el inicio después de actualizar correctamente la base de firmas de virus**

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón secundario en la tarea y seleccione **Modificar...** o bien, seleccione la tarea que desea modificar y haga clic en el botón **Modificar...**.

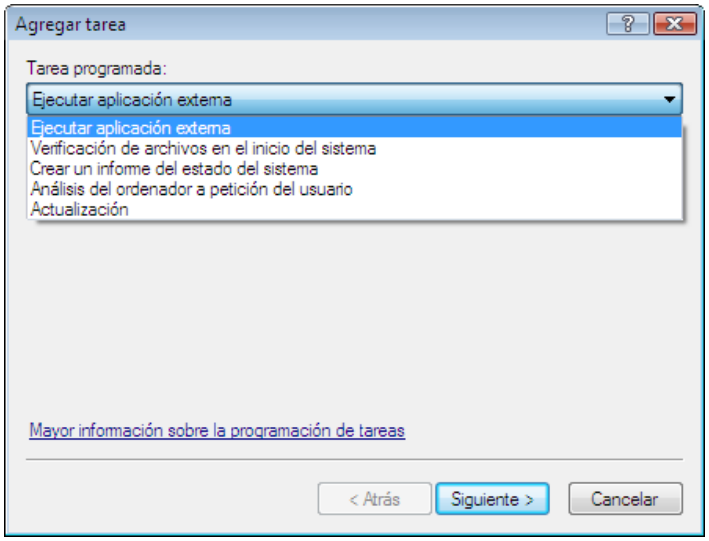
4.5.1 Finalidad de las tareas programadas

La característica Tareas programadas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas. La configuración y las propiedades contienen información como la fecha y la hora, así como los perfiles especificados que se van a utilizar durante la ejecución de la tarea.

4.5.2 Creación de tareas nuevas

Para crear una nueva tarea en Tareas programadas, haga clic en el botón **Agregar...** o haga clic con el botón secundario y seleccione **Agregar...** en el menú contextual. Existen cinco tipos de tareas programadas disponibles:

- **Ejecutar aplicación externa**
- **Mantenimiento de registros**
- **Verificación de la ejecución de archivos en el inicio del sistema**
- **Análisis del equipo a petición**
- **Actualización**



Ya que **Análisis del equipo a petición** y **Actualizar** son las tareas programadas utilizadas con más frecuencia, se explicará cómo se agrega una nueva tarea de actualización.

En el menú desplegable **Tarea programada:** seleccione **Actualizar**. Haga clic en **Siguiente** e introduzca el nombre de la tarea en el campo **Nombre de la tarea:** Seleccione la frecuencia de la misma. Las siguientes opciones están disponibles: **Una vez, Reiteradamente, Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Las siguientes tres opciones están disponibles:

- **Esperar hasta la próxima hora programada**
- **Ejecutar la tarea tan pronto como sea posible**
- **Ejecutar la tarea inmediatamente si la hora transcurrida desde su última ejecución supera el intervalo especificado** (el intervalo puede definirse inmediatamente utilizando el cuadro **Intervalo de la tarea**)

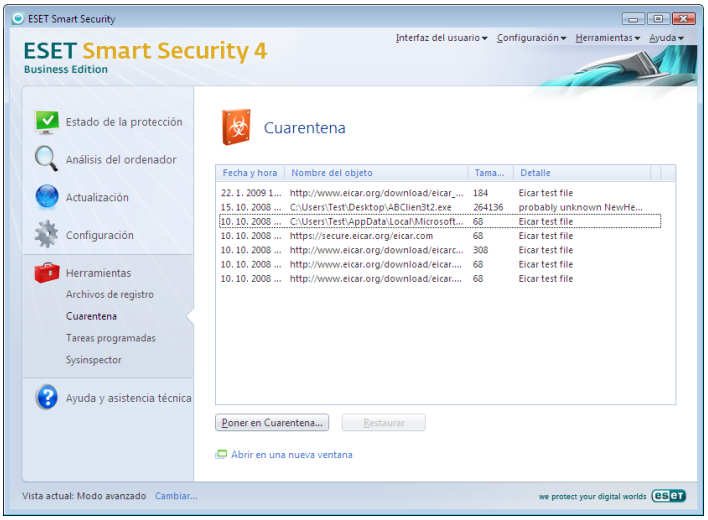
En el paso siguiente, se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente; la opción **Ejecutar tarea con parámetros específicos** debe activarse automáticamente. Haga clic en el botón **Finalizar**.

Aparecerá un cuadro de diálogo que le permite elegir los perfiles que se van a utilizar para la tarea programada. En este paso, puede especificar un perfil principal y uno alternativo, que se utiliza en caso de que no pueda completarse la tarea con el perfil principal. Para confirmar, haga clic en **Aceptar** en la ventana **Perfiles de actualización**. La nueva tarea se agregará a la lista de tareas programadas actualmente.

4.6 Cuarentena

La tarea fundamental de la cuarentena es almacenar de forma segura los archivos infectados. Los archivos deben colocarse en cuarentena si no se pueden desinfectar, si no es seguro ni aconsejable eliminarlos o si ESET Smart Security los está detectando falsamente.

El usuario puede poner en cuarentena cualquier archivo que desee. 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 a los laboratorios de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en las que se copiaron a cuarentena, la ruta a la ubicación original del archivo infectado, su tamaño en bytes, el motivo (**Agregado por el usuario...**) y el número de amenazas (por ejemplo, si se trata de un archivo que contiene varias amenazas).

4.6.1 Copia de archivos en cuarentena

El programa copia en cuarentena automáticamente los archivos eliminados (si no ha cancelado esta opción en la ventana de alerta). Si lo desea, puede copiar en cuarentena cualquier archivo sospechoso manualmente haciendo clic en el botón **Poner en Cuarentena...**. En este caso, el archivo original no se elimina de su ubicación original. El menú contextual también se puede utilizar con este fin, haga clic con el botón secundario en la ventana de cuarentena y seleccione **Agregar...**

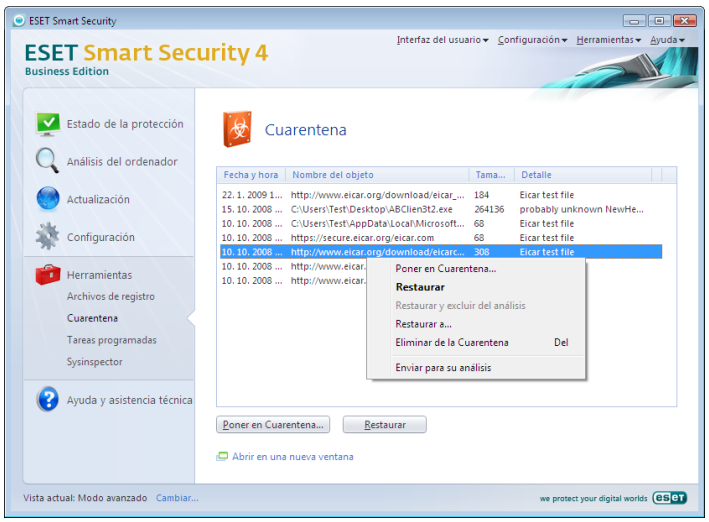
4.6.2 Restauración de archivos de cuarentena

Los archivos puestos en cuarentena pueden restaurarse a su ubicación original. Utilice la opción **Restaurar** para realizar esta tarea, disponible en el menú contextual al hacer clic con el botón secundario en el archivo específico que aparece en la ventana de cuarentena. El menú contextual también ofrece la opción **Restaurar a...**, que permite restaurar archivos en una ubicación distinta a la original de la que se hayan eliminado.

NOTA:
si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y envíelo a Atención al cliente de ESET.

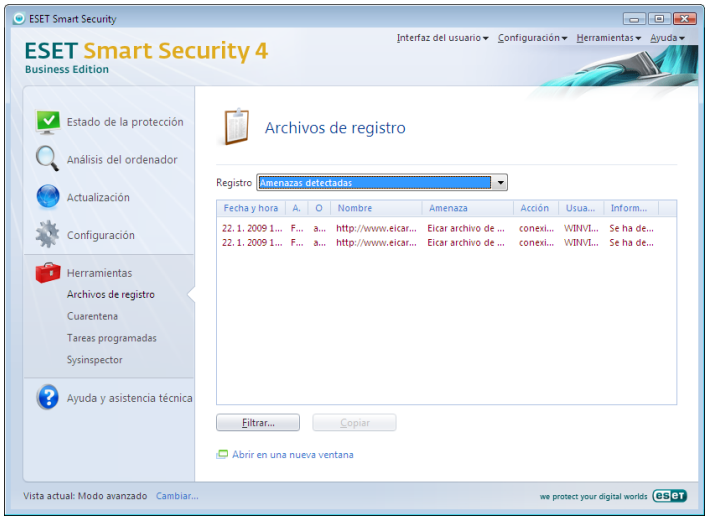
4.6.3 Envío de un archivo de cuarentena

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 virus de ESET. Para enviar un archivo de cuarentena, haga clic con el botón secundario en éste y seleccione **Enviar para su análisis** en el menú contextual.



4.7 Archivos de registro

Los archivos de registro contienen información acerca de todos los sucesos importantes del programa que se hayan producido 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 registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno ESET Smart Security, donde también se pueden archivar registros.



Se puede obtener acceso a los archivos de registro desde la ventana principal de ESET Smart Security al hacer clic en **Herramientas > Archivos de registro**. Seleccione el tipo de registro deseado utilizando el menú desplegable **Registro:** de la parte superior de la ventana. Están disponibles los siguientes registros:

1. **Amenazas detectadas:** utilice esta opción para ver toda la información relativa a la detección de amenazas.

2. **Sucesos:** esta opción está diseñada para administradores del sistema y usuarios con el fin de solucionar problemas. Todas las acciones importantes realizadas en ESET Smart Security se registran en los registros de sucesos.

3. **Análisis del equipo a petición:** en esta ventana se muestran los resultados de todos los análisis realizados. Haga doble clic en cualquier entrada para ver los detalles del análisis a petición correspondiente.

4. **Registros del cortafuegos personal de ESET:** contiene registros de todos los hechos que haya detectado el cortafuegos personal y relacionados con el mismo. El análisis del registro del cortafuegos puede ayudarle a detectar los intentos de entrar en el sistema a tiempo para evitar el acceso no autorizado al mismo.

En cada sección, la información mostrada se puede copiar directamente en el portapapeles si selecciona la entrada y hace clic en el botón **Copiar**. Para seleccionar varias entradas, se pueden utilizar las teclas CTRL. y MAYÚS.

4.7.1 Mantenimiento de registros

Se puede obtener acceso a la configuración de registro de ESET Smart Security desde la ventana principal del programa. Haga clic en **Configuración > Escriba el árbol completo de la configuración avanzada... > Herramientas > Archivos de registro**. Puede especificar las siguientes opciones para los archivos de registro:

- **Eliminar registros automáticamente:** las entradas de registros que superen el número de días especificado se eliminan automáticamente.

- **Optimizar los archivos de registro automáticamente:** activa la desfragmentación automática de los archivos de registros si se ha superado el porcentaje especificado de registros no utilizados.

- **Nivel mínimo de detalle al registrar:** especifica el nivel de contenido de los registros de sucesos. Opciones disponibles:

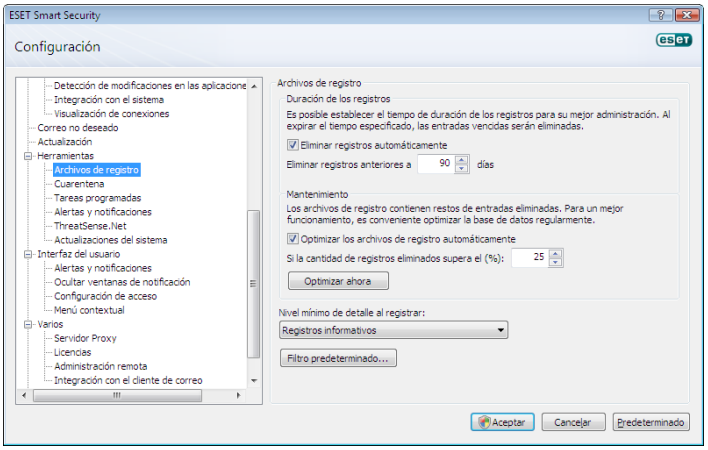
  - **Errores graves:** registra todos los errores graves (errores al comenzar la protección antivirus, cortafuegos personal, etc.)

  - **Errores:** sólo se registrarán los errores graves y los de tipo “Error al descargar el archivo”.

  - **Alertas:** registra errores graves y mensajes de alerta.

  - **Registros informativos:** registra los mensajes informativos, incluidos los mensajes de actualización correcta y todos los registros anteriores.

  - **Registros de diagnóstico:** registra la información necesaria para ajustar el programa y todos los registros anteriores.



4.8 Interfaz del usuario

Las opciones de configuración de la interfaz de usuario de ESET Smart Security se pueden modificar de forma que pueda ajustar su entorno de trabajo conforme a sus necesidades. Se puede obtener acceso a estas opciones de configuración desde el apartado **Interfaz del usuario** del árbol Configuración avanzada de ESET Smart Security.

La sección **Elementos de la interfaz de usuario** proporciona a los usuarios la capacidad de cambiar al modo avanzado si se desea. La vista en modo avanzado muestra configuración más detallada y controles adicionales de ESET Smart Security.

La **interfaz gráfica de usuario** debe desactivarse si los elementos gráficos disminuyen el rendimiento del equipo o provocan otros problemas. También se puede desactivar la interfaz gráfica para usuarios con discapacidades visuales, ya que podría entrar en conflicto con aplicaciones especiales que se utilizan para leer el texto que aparece en pantalla.

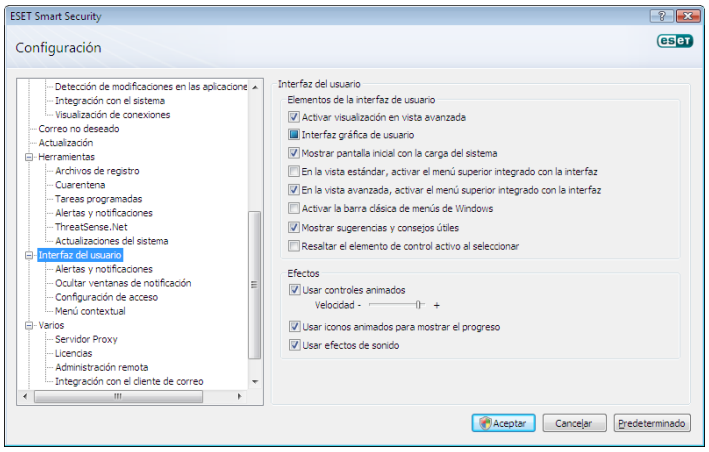
Si desea desactivar la pantalla de inicio de ESET Smart Security, desactive la opción **Mostrar pantalla de inicio al iniciar**.

En la parte superior de la ventana principal del programa ESET Smart Security, aparece un menú estándar que se puede activar o desactivar según la opción **Activar la barra clásica de menús de Windows**.

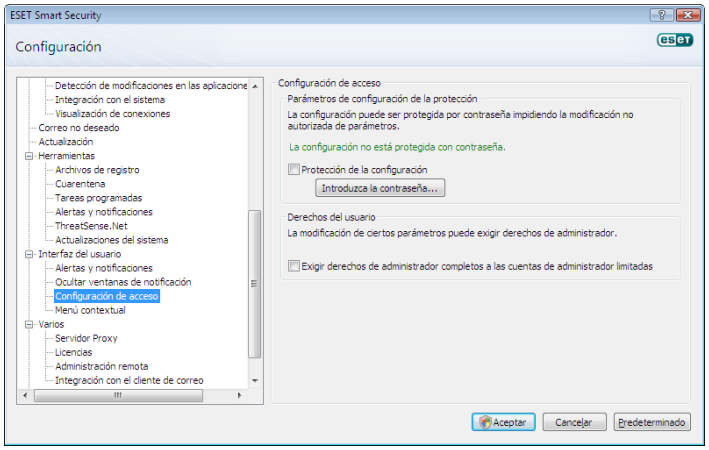
Si se activa la opción **Mostrar sugerencias y consejos útiles**, se mostrará una breve descripción de cualquier opción si se coloca el cursor sobre la misma. La opción **Resaltar el elemento de control activo al seleccionar**, provocará que el sistema resalte cualquier elemento que se encuentre actualmente debajo de la zona activa del cursor del "mouse" (ratón). El elemento resaltado se activará al hacer clic con el "mouse".

Para aumentar o disminuir la velocidad de los efectos animados, seleccione la opción **Usar controles animados** y mueva la barra deslizante **Velocidad** a la izquierda o a la derecha.

Para activar el uso de iconos animados y ver el progreso de varias operaciones, seleccione la casilla de verificación **Usar iconos animados...**. Si desea que el programa emita un sonido de alerta si tiene lugar un suceso importante, utilice la opción **Usar efectos de sonido**.



Las características de **Interfaz del usuario** también incluyen la opción de proteger mediante contraseña los parámetros de configuración de ESET Smart Security. Esta opción se encuentra en el submenú **Protección de parámetros** en **Interfaz del usuario**. 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 establecer una contraseña que proteja los parámetros de configuración, haga clic en **Introduzca la contraseña...**



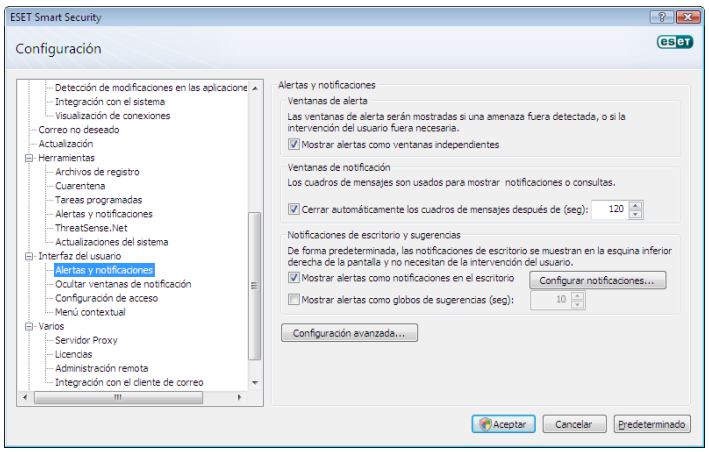
4.8.1 Alertas y notificaciones

La sección **Configuración de las alertas y notificaciones** que se encuentra en **Interfaz del usuario** le permite configurar el modo en el que se administran los mensajes de alertas de amenazas y las notificaciones del sistema en ESET Smart Security 4.

El primer elemento es **Mostrar alertas**. Si desactiva esta opción, se cancelarán todos los mensajes de alerta, lo que resulta útil únicamente en una serie de situaciones muy específicas. Para la mayoría de los usuarios, se recomienda que mantenga la opción predeterminada (activada).

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione la opción **Cerrar automáticamente los cuadros de mensajes después de (seg.)**. Si el usuario no las cierra manualmente, las ventanas de alerta se cerrarán automáticamente una vez transcurrido el período de tiempo especificado.

Las notificaciones del escritorio y los globos de sugerencias son medios de información que no requieren ni ofrecen la intervención del usuario. Se muestran en la zona de notificación situada en la esquina inferior derecha de la pantalla. Para activar la visualización de las notificaciones de escritorio, seleccione la opción **Mostrar alertas como notificaciones en el escritorio**. Se puede modificar el tiempo de visualización de las notificaciones y la transparencia mediante el botón **Configurar notificaciones...** Para obtener una vista previa del comportamiento de las notificaciones, haga clic en el botón **Vista previa**. Para configurar la duración del tiempo de visualización de los globos de sugerencias, consulte la opción **Mostrar alertas como globos de sugerencias (seg)**.



Haga clic en **Configuración avanzada...** para introducir opciones de configuración de **alertas y notificaciones** que incluyan la opción **Mostrar sólo las notificaciones en las que se necesite la interacción del usuario**. Con esta opción, puede activar

o desactivar la visualización de las alertas y las notificaciones que no requieran la interacción del usuario. Seleccione la opción Mostrar sólo las notificaciones en las que se necesite la interacción del usuario cuando se ejecuten aplicaciones a pantalla completa para ocultar todas las notificaciones en las que no se requiera la interacción. Desde el nivel mínimo de detalle de los sucesos para visualizar en el menú desplegable, puede seleccionar el nivel de gravedad inicial de las alertas y las notificaciones que se van a mostrar.

La última característica de esta sección consiste en especificar las direcciones de las notificaciones en un entorno con varios usuarios. El campo **En sistemas multiusuarios, mostrar las notificaciones en el escritorio del usuario:** este campo permite que el usuario defina quién va a recibir las notificaciones importantes de ESET Smart Security 4. Suele ser un administrador de red o del sistema. Esta opción resulta especialmente útil para servidores de terminal, siempre que todas las notificaciones del sistema se envíen al administrador.

4.9 ThreatSense.Net

El sistema de alerta temprana ThreatSense.Net es una herramienta que mantiene informado a ESET de forma constante e inmediata acerca de nuevas amenazas. El sistema de alerta temprana bidireccional ThreatSense.Net tiene una sola finalidad**:** mejorar la protección que le podemos ofrecer. La mejor forma de garantizar la detección de nuevas amenazas en cuanto aparecen es un "vínculo" al mayor número posible de clientes que funcionen como exploradores de amenazas. Existen dos opciones:

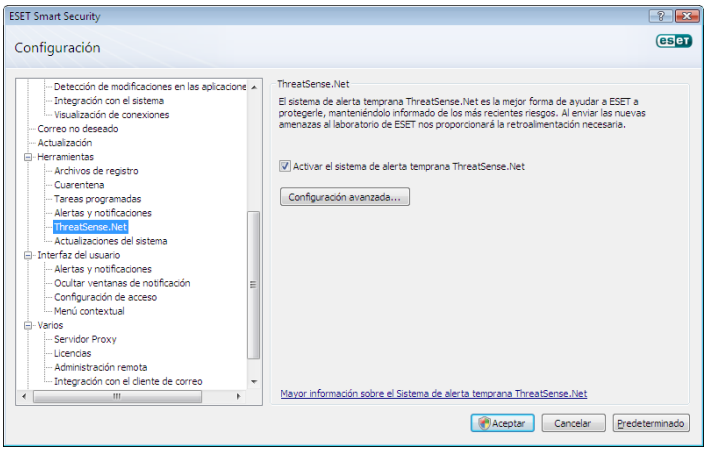
- Puede optar por no activar el sistema de alerta temprana ThreatSense.Net. No perderá ninguna funcionalidad del software y obtendrá igualmente la mejor protección disponible.

- Puede configurar el sistema de alerta temprana para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso en un único archivo. Este archivo se puede enviar a ESET para realizar un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar sus funciones de detección de amenazas. El sistema de alerta temprana ThreatSense.Net recopilará información anónima acerca de su equipo que esté relacionada con amenazas detectadas recientemente. Esta información puede incluir una muestra o copia del archivo en el que haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la información relativa a la fecha y la hora, el proceso por el que ha aparecido la amenaza en su equipo e información sobre el sistema operativo de su ordenador. Parte de esta información puede incluir información personal acerca del usuario del equipo, como podrían ser los nombres de usuario de una ruta al directorio, entre otros.

Aunque existe la posibilidad de que este proceso pueda revelar cierta información acerca del usuario o de su equipo al laboratorio de amenazas de ESET, dicha información no se utilizará con NINGÚN propósito que no esté relacionado con la ayuda necesaria para responder inmediatamente a nuevas amenazas.

De forma predeterminada, ESET Smart Security está configurado para confirmar el envío de archivos sospechosos para su análisis detallado en los laboratorios de ESET. Debe tener en cuenta que los archivos con ciertas extensiones, como .doc o .xls, siempre se excluyen en caso de que se detecte una amenaza en los mismos. También puede agregar otras extensiones si existen determinados archivos que usted o su empresa no deseen enviar.

La configuración de ThreatSense.Net está disponible en el árbol de Configuración avanzada, en **Herramientas > ThreatSense.Net**. Seleccione la casilla de verificación **Activar el sistema de alerta temprana ThreatSense.Net**. Esta acción le permitirá activar y, a continuación, hacer clic en el botón **Configuración avanzada**.

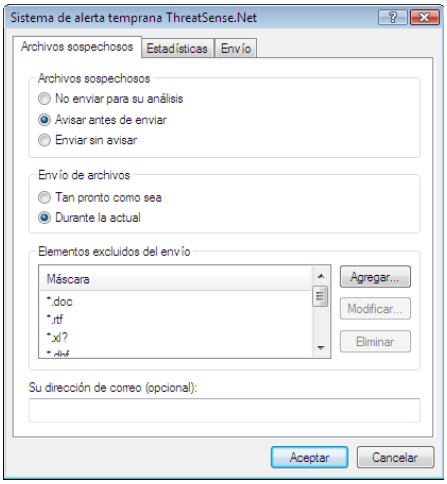


4.9.1 Archivos sospechosos

La pestaña **Archivos sospechosos** permite al usuario configurar la forma en la que se envían las amenazas al laboratorio de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo para su análisis a los laboratorios de virus. Si resulta ser una aplicación maliciosa, su detección se agregará a la siguiente actualización de firma de virus.

Se puede configurar el envío de los archivos para que se realice de forma automática sin avisar. Si se activa esta opción, los archivos sospechosos se envían en segundo plano. Si desea conocer los archivos que se han enviado para su análisis y confirmar el envío, seleccione la opción **Preguntar antes de enviar**.



Si no desea que se envíe ningún archivo, seleccione **No enviar para el análisis**. Tenga en cuenta que el hecho de no enviar archivos para su análisis no afecta al envío de información estadística a ESET. La información estadística se configura en su propia sección de configuración, como se describe en el capítulo siguiente.

Envío de archivos
Los archivos sospechosos se enviarán a los laboratorios de ESET para su análisis tan pronto como sea posible. Esta acción es aconsejable si dispone de una conexión a Internet permanente y es posible entregar los archivos sospechosos sin retrasos. La otra opción es enviar archivos sospechosos **Durante la actualización**. Si se selecciona esta opción, los archivos sospechosos se recopilarán y cargarán en los servidores del sistema de alerta temprana durante una actualización.

Elementos excluidos del envío
No es necesario enviar todos los archivos para su análisis. La opción Elementos excluidos del envío permite excluir determinados archivos o carpetas del envío. Por ejemplo, esta opción puede ser útil para excluir archivos que pueden contener posible información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen de forma predeterminada (Microsoft Office u OpenOffice). La lista de archivos excluidos se puede ampliar si se desea.

Correo electrónico de contacto
La dirección de correo electrónico se envía junto con los archivos sospechosos a ESET y puede utilizarse para ponerse en contacto con usted si es necesario enviar información adicional para poder realizar el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

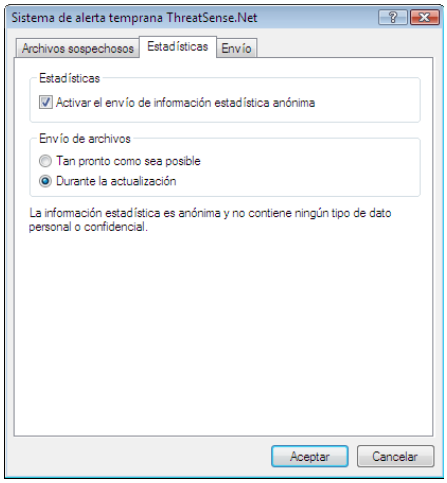
4.9.2 Estadísticas

El sistema de alerta temprana ThreatSense.Net recopila información anónima acerca de su equipo relacionada con amenazas detectadas recientemente. Esta información puede incluir el nombre de la amenaza, la fecha y la hora en las que se ha detectado, la versión de ESET Smart Security, la versión del sistema operativo de su equipo y la configuración regional. Normalmente, las estadísticas se envían a los servidores de ESET una o dos veces al día.

A continuación, se incluye un ejemplo de un paquete de información estadística enviado:

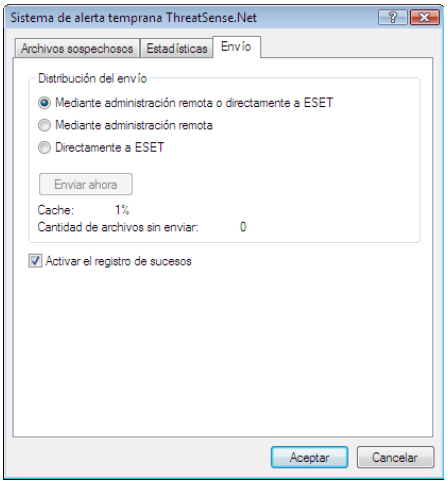
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Envío de archivos
En la sección **Envío de archivos**, puede definir cuándo desea enviar la información estadística. Si opta por enviarla **Tan pronto como sea posible**, la información estadística se enviará inmediatamente después de haberse creado. Esta configuración es aconsejable si dispone de una conexión a Internet permanente. Si selecciona **Durante la actualización**, la información estadística se conservará y enviará de forma conjunta durante la siguiente actualización.



4.9.3 Envío

En esta sección, puede determinar si desea que los archivos y la información estadística se envíen a través de un administrador remoto de ESET o directamente a ESET. Si desea asegurarse de que los archivos sospechosos y la información estadística se entregan a ESET, seleccione la opción **Mediante Administración remota o directamente a ESET**. Si se selecciona esta opción, los archivos y las estadísticas se envían a través de todos los medios disponibles. El envío de archivos sospechosos mediante administración remota permite entregar los archivos y las estadísticas al servidor de administración remota, que garantizará la entrega pertinente de los mismos a los laboratorios de virus de ESET. Si se selecciona la opción **Directamente a ESET**, todos los archivos sospechosos y la información estadística se envían a los laboratorios virtuales de ESET directamente desde el programa.



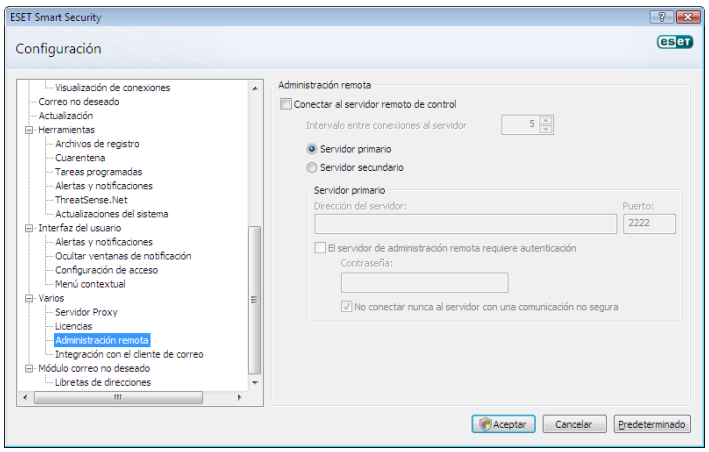
Cuando existen archivos sin enviar, el botón **Enviar ahora** se activa en esta ventana de configuración. Haga clic en este botón si desea enviar inmediatamente archivos e información estadística.

Seleccione la casilla de verificación **Activar registro de sucesos** para habilitar el registro del envío de archivos e información estadística. Después de cada envío de un archivo sospechoso o información estadística, se crea una entrada en el registro de sucesos.

4.10 Administración remota

La administración remota es una potente herramienta que permite mantener las directivas de seguridad y obtener información general acerca de la administración global de la seguridad en la red. Es especialmente útil cuando se aplica a redes de mayor tamaño. La administración remota no sólo proporciona un aumento del nivel de seguridad, sino que permite administrar de forma sencilla ESET Smart Security en estaciones de trabajo cliente.

Las opciones de configuración de la administración remota están disponibles en la ventana principal del programa ESET Smart Security. Haga clic en **Configuración > Escriba el árbol completo de la configuración avanzada... > Varios > Administración remota**.



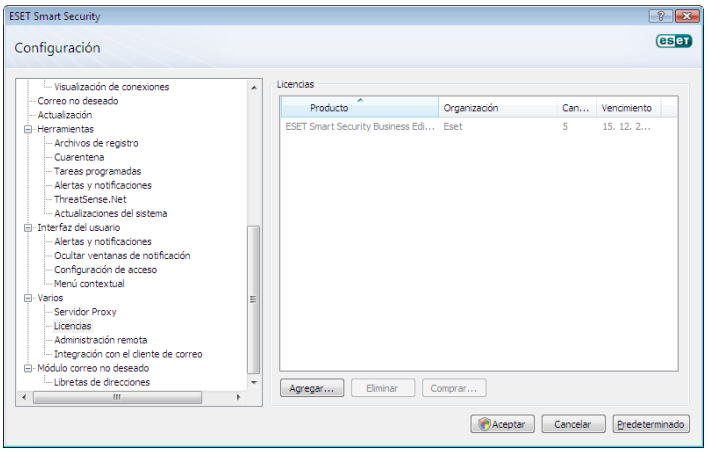
La ventana Configuración permite activar el modo de administración remota seleccionando primero **Conectar al servidor de administración remota**. Así, podrá obtener acceso a las opciones que se describen a continuación:

- **Dirección del servidor:** dirección de red del servidor donde se encuentra instalado el servidor de administración remota.
- **Puerto:** este campo contiene un puerto del servidor predefinido utilizado para la conexión. Se recomienda que deje la configuración predeterminada del puerto en 2222.
- **Intervalo entre conexiones al servidor (min.):** esta opción determina la frecuencia con la que ESET Smart Security se conectará al servidor ERA para enviar los datos. Es decir, la información se envía en los intervalos de tiempo que se definan en esta opción. Si se establece en 0, la información se enviará cada 5 segundos.
- **El servidor de administración remota requiere autentificación:** permite introducir una contraseña para conectarse al servidor de administración remota, si es necesario.

Haga clic en **Aceptar** para confirmar los cambios y aplicar los parámetros. ESET Smart Security los utilizará para conectarse al servidor remoto.

4.11 Licencia

El apartado **Licencias** administra claves de licencia para ESET Smart Security y otros productos de ESET, tales como el administrador remoto de ESET, ESET NOD32 para Microsoft Exchange, etc. Tras la compra, se entregan claves de licencia junto con su nombre de usuario y contraseña. Para **Agregar/ Eliminar** una clave de licencia, haga clic en el botón correspondiente de la ventana Administrador de licencia. Puede obtener acceso al administrador de licencias desde el árbol Configuración avanzada en **Varios > Licencias**.



La clave de licencia es un archivo de texto que contiene información acerca del producto adquirido: su propietario, número de licencias y fecha de caducidad.

La ventana del administrador de licencias permite al usuario cargar y ver el contenido de una clave de licencia mediante el botón **Agregar**, de modo que la información que contiene aparece en el administrador. Para eliminar los archivos de licencia de la lista, haga clic en **Eliminar**.

Si una clave de licencia ha caducado y está interesado en renovarla, haga clic en el **botón Comprar...** y será redirigido a la tienda en línea.

5. Usuario avanzado

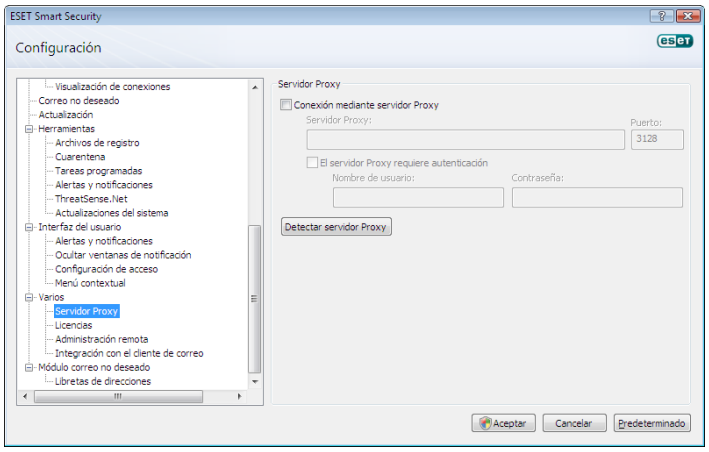
En este capítulo se describen características de ESET Smart Security que pueden resultar útiles para usuarios más avanzados. Sólo se puede obtener acceso a las opciones de configuración de estas características en el modo avanzado. Para cambiar al modo avanzado, haga clic en **Cambiar la visualización al modo avanzado** en la esquina inferior izquierda de la ventana principal del programa o pulse CTRL + M en su teclado.

5.1 Configuración del servidor Proxy

En ESET Smart Security, la configuración del servidor Proxy está disponible en dos secciones diferentes dentro de la estructura de árbol de Configuración avanzada.

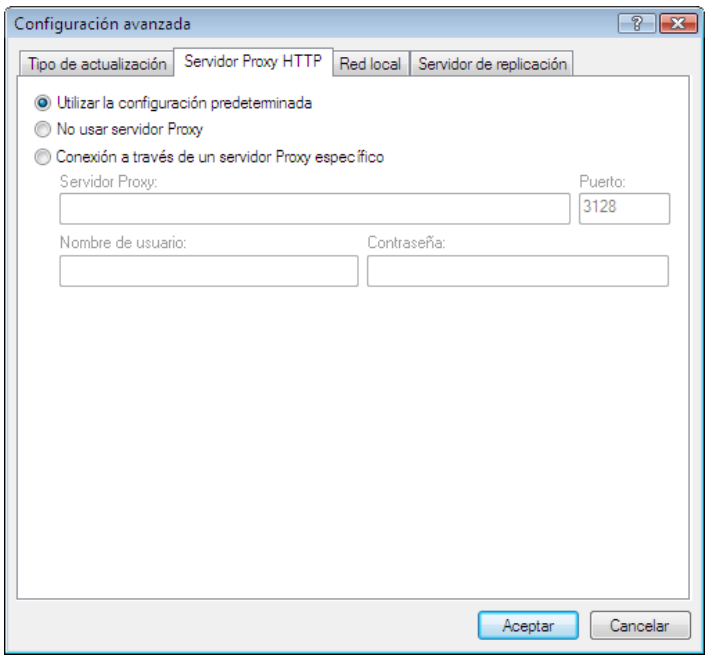
En primer lugar, los parámetros del servidor Proxy se pueden configurar en **Varios > Servidor Proxy**. Al especificar el servidor Proxy en este nivel, se definen los parámetros del servidor Proxy para todo ESET Smart Security. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar los parámetros del servidor Proxy para este nivel, seleccione la casilla de verificación **Conexión mediante servidor Proxy** y escriba la dirección del servidor Proxy en el campo **Servidor Proxy:** junto con el número de **Puerto** del servidor Proxy.



Si la comunicación con el servidor Proxy requiere autentificación, seleccione la casilla de verificación **El servidor Proxy requiere autentificación** y escriba un **Nombre de usuario** y **Contraseña** válidos en los campos correspondientes. Haga clic en el botón **Detectar servidor Proxy** para detectar automáticamente e insertar los parámetros del servidor Proxy. Se copiarán los parámetros especificados en Internet Explorer. Tenga en cuenta que esta función no recupera datos de autentificación (nombre de usuario y contraseña); el usuario debe proporcionar esta información.

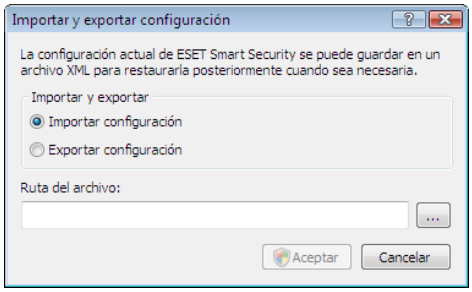
Los parámetros del servidor Proxy también se pueden establecer en **Configuración avanzada de actualizaciones** (apartado **Actualizar** del árbol Configuración avanzada). Esta configuración se aplica al perfil de actualización especificado y se recomienda para portátiles, ya que suelen recibir actualizaciones de firmas de virus de distintas ubicaciones. Para obtener más información sobre esta configuración, consulte la sección 4.4, "Actualización del sistema".



5.2 Importar y exportar configuración

La exportación e importación de la configuración actual de ESET Smart Security se encuentran disponibles en el modo avanzado en **Configuración**.

Tanto la exportación como la importación utilizan el tipo de archivo .xml. La importación y la exportación son útiles si necesita realizar una copia de seguridad de ESET Smart Security para poder utilizarla más tarde (por cualquier motivo). La opción de configuración de exportación también será útil para aquéllos que deseen utilizar su configuración favorita de ESET Smart Security en varios sistemas; sólo necesitan importar el archivo .xml.



5.2.1 Exportar configuración

Exportar la configuración es muy fácil. Si desea guardar la configuración actual de ESET Smart Security, haga clic en **Configuración > Importar y exportar configuración...**. Seleccione la opción **Exportar configuración** y escriba el nombre del archivo de configuración. Utilice el navegador para seleccionar una ubicación en su equipo en donde desee guardar el archivo de configuración.

5.2.2 Importar configuración

Los pasos para importar una configuración son muy similares. De nuevo, seleccione **Importar y exportar configuración** y la opción **Importar configuración**. Haga clic en el botón **...** y busque el archivo de configuración que desea importar.

5.3 Línea de comandos

El módulo antivirus de ESET Smart Security se puede iniciar a través de la línea de comandos de forma manual, con el comando "ecls", o con un archivo por lotes ("bat").

Los siguientes parámetros y modificadores se pueden utilizar al ejecutar el análisis a petición desde la línea de comandos:

Opciones generales:

– help	mostrar ayuda y salir
– version	mostrar información sobre la versión y salir
– base-dir = FOLDER	cargar módulos desde CARPETA
– quar-dir = FOLDER	CARPETA Cuarentena
– aind	mostrar indicador de actividad

Objetos:

– files	analizar archivos (predeterminado)
– no-files	no analizar archivos
– boots	analizar sectores de inicio (predeterminado)
– no-boots	no analizar sectores de inicio
– arch	analizar archivos comprimidos (predeterminado)
– no-arch	no analizar archivos comprimidos
– max-archive-level = LEVEL	máximo NIVEL de anidamiento de archivos comprimidos
– scan-timeout = LIMIT	analizar archivos comprimidos con un LÍMITE máximo de segundos. Si el tiempo del análisis alcanza este límite, el análisis del archivo comprimido se detiene y continuará con el siguiente archivo
– max-arch-size=SIZE	analizar sólo los bytes de primer TAMAÑO en los archivos (predeterminado 0 = ilimitado)
– mail	analizar archivos de correo
– no-mail	no analizar archivos de correo
– sfx	analizar archivos comprimidos de auto extracción
– no-sfx	no analizar archivos comprimidos de auto extracción
– rtp	analizar empaquetadores en tiempo real
– no-rtp	no analizar empaquetadores en tiempo real
– exclude = FOLDER	excluir CARPETA del análisis
– subdir	analizar subcarpetas (predeterminado)
– no- subdir	no analizar subcarpetas
– max-subdir-level = LEVEL	NIVEL de anidamiento de subcarpetas máximo (predeterminado 0 =ilimitado)
– symlink	seguir enlaces simbólicos (predeterminado)
– no-symlink	omitir enlaces simbólicos
– ext-remove = EXTENSIONS	
– ext-exclude = EXTENSIONS	excluir EXTENSIONES del análisis, separándolas por el signo ":" (dos puntos)

Métodos:

– adware	analizar en busca de Adware/ Spyware/Riskware
– no-adware	no analizar en busca de Adware/ Spyware/Riskware
– unsafe	analizar en busca de aplicaciones potencialmente peligrosas
– no-unsafe	no analizar en busca de aplicaciones potencialmente peligrosas
– unwanted	analizar en busca de aplicaciones potencialmente indeseables
– no-unwanted	no analizar en busca de aplicaciones potencialmente indeseables
– pattern	usar firmas
– no-pattern	no usar firmas
– heur	activar heurística
– no-heur	desactivar heurística
– adv-heur	activar la heurística avanzada
– no-adv-heur	desactivar la heurística avanzada

Desinfección:

– action = ACTION	ACCIÓN que se va a efectuar en los objetos infectados. Acciones disponibles: sin acciones, desinfectar, preguntar
– quarantine	copiar archivos infectados a cuarentena (ACCIÓN opcional)
– no-quarantine	no copiar archivos infectados a cuarentena

Registros:

– log-file=FILE	registrar en ARCHIVO
– log-rewrite	sobrescribir el archivo de salida (predeterminado – agregar)
– log-all	registrar también archivos sin infectar
– no-log-all	no registrar archivos sin infectar (predeterminado)

Los posibles códigos de salida del análisis son:

0 – sin amenazas detectadas.
1 – se ha encontrado una amenaza, pero no se ha desinfectado.
10 – no se han desinfectado algunos de los archivos infectados.
101 – error en el archivo.
102 – error de acceso.
103 – error interno.

NOTA:
los códigos de salida superiores a 100 significan que no se ha analizado el archivo y que, por tanto, puede estar infectado.

5.4 ESET SysInspector

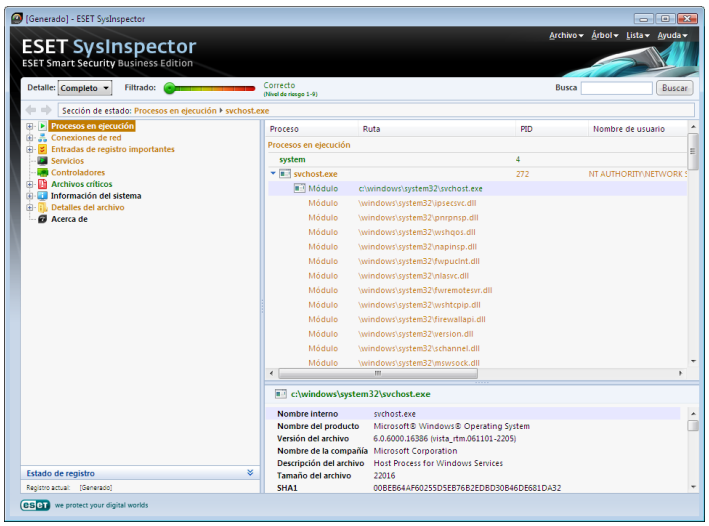
ESET SysInspector es una aplicación que inspecciona completamente su equipo y muestra datos recopilados de una manera detallada. Información como los controladores y aplicaciones instalados, las conexiones de red o entradas de registro importantes pueden ayudarle a investigar el comportamiento sospechoso del sistema debido a la incompatibilidad de software o hardware o infección de código malicioso.

Puede encontrar SysInspector en dos sitios diferentes de ESET. La aplicación portátil (SysInspector.exe) puede descargarla de forma gratuita del sitio web de ESET. La variante integrada se incluye en ESET Smart Security 4. Para abrir la sección SysInspector, active el modo de visualización avanzada en la esquina inferior izquierda y haga clic en **Herramientas > SysInspector**. Ambas opciones tienen el mismo funcionamiento y los mismos controles de programa. La única diferencia es la forma en la que se controlan los resultados. La aplicación portátil le permite exportar las instantáneas del sistema a un archivo XML y guardarlo en el disco. Esta acción también es posible en la aplicación SysInspector integrada. Además, puede almacenar dichas instantáneas de forma cómoda directamente en **ESET Smart Security 4 > Herramientas > SysInspector** (para obtener información adicional, consulte 5.4.1.4 SysInspector como parte de ESS).

Espere mientras ESET SysInspector analiza el equipo. El análisis puede durar entre 10 segundos y algunos minutos en función de la configuración del hardware, del sistema operativo y de la cantidad de aplicaciones que tenga instaladas en el equipo.

5.4.1 Interfaz del usuario y uso de la aplicación

Para una administración sencilla, la ventana principal se divide en cuatro secciones: controles de programa ubicados en la parte superior de la ventana principal, la ventana de navegación a la izquierda, la ventana de descripción en la parte central derecha y la ventana de detalles en la parte inferior derecha de la ventana principal.



5.4.1.1 Controles de programa

En esta sección se encuentra la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo
Al hacer clic aquí, puede guardar el estado del informe actual para examinarlo más tarde o abrir un informe guardado anteriormente. En caso de que desee publicar su informe, le recomendamos que lo genere según sea necesario para enviarlo. De esta forma, el informe omite la información personal.

Nota: *puede abrir informes de ESET SysInspector previamente guardados simplemente arrastrando y soltándolos en la ventana principal.*

Árbol
Le permite expandir o cerrar todos los nodos.

Lista
Contiene funciones para una navegación más sencilla por el programa y otras funciones como buscar información en línea.

Importante: *los elementos resaltados en rojo son desconocidos; el motivo de esto es que el programa los marca como potencialmente peligrosos. Si un elemento está en rojo, no significa automáticamente que puede eliminar el archivo. Antes de eliminarlos, asegúrese de que los archivos son verdaderamente peligrosos o innecesarios.*

Ayuda
Contiene información sobre la aplicación y sus funciones.

Detalle
Aparece información en otras secciones de la ventana principal y, por tanto, hace que la utilización del programa resulte sencilla. En el modo *básico* tiene acceso a información utilizada para buscar soluciones a problemas comunes de su sistema. En el modo *medio*, el programa muestra información menos utilizada mientras que en el modo *completo* ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado de elementos
Es la mejor opción para buscar archivos o entradas de registro sospechosos en el sistema. Mediante el ajuste del control deslizante, puede filtrar elementos por su nivel de riesgo. Si el control deslizante se establece lo más a la izquierda posible (nivel de riesgo 1), se mostrarán todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos menos peligrosos que el nivel de riesgo actual y muestra sólo los elementos que son más sospechosos que el nivel mostrado. Con el control deslizante establecido lo más a la derecha posible, el programa mostrará sólo elementos dañinos conocidos.

Todos los elementos pertenecientes al intervalo de riesgo comprendido entre 6 y 9 pueden suponer un riesgo de seguridad. Si no está utilizando algunas de las soluciones de seguridad de ESET, recomendamos que analice su sistema con el Escáner en línea ESET después de que el programa haya encontrado dicho elemento. El Escáner en línea ESET es un servicio gratuito y se puede encontrar en http://www.eset.eu/online-scanner.

Nota: *el nivel de riesgo de un elemento se puede determinar rápidamente comparando el color del elemento con el color del control deslizante del nivel de riesgo.*

Buscar
Se puede utilizar esta opción para buscar rápidamente un elemento específico por nombre o parte de su nombre. Los resultados de la solicitud de búsqueda aparecerán en la ventana de descripción.

Retorno
Al hacer clic en la flecha hacia atrás y hacia delante, puede volver a la información mostrada anteriormente en la ventana de descripción.

Sección de estado
Muestra el nodo actual en la ventana de navegación.

5.4.1.2 Navegación por ESET SysInspector

ESET SysInspector divide varios tipos de información en varias secciones denominadas nodos. Si está disponible, puede encontrar información adicional expandiendo cada nodo en sus subnodos. Para abrir o contraer un nodo, sólo tiene que hacer doble clic en el nombre del nodo o bien, hacer clic en ⊞ o ⊟, que se encuentra junto al nombre del nodo. a medida que explora la estructura de árbol de nodos y subnodos en la ventana de navegación, puede encontrar información variada de cada nodo que aparece en la ventana de descripción. Si echa un vistazo a los elementos de la ventana de descripción, es posible que se muestre información adicional de cada elemento en la ventana de detalles.

A continuación se encuentran las descripciones de los nodos principales en la ventana de navegación e información relacionada en las ventanas de descripción y detalles.

Procesos en ejecución
Este nodo contiene información sobre aplicaciones y procesos que se ejecutan en el momento de generar el informe. En la ventana de descripción, puede encontrar información adicional de cada proceso como, por ejemplo, bibliotecas dinámicas utilizadas por el proceso y su ubicación en el sistema, el nombre del proveedor de la aplicación, el nivel de riesgo del archivo, etc.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

Nota: *un sistema operativo incluye varios componentes del núcleo (kernel) importantes que se ejecutan de forma ininterrumpida y proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, dichos procesos aparecen en la herramienta ESET SysInspector con la ruta de archivo comenzando por \??\. Estos símbolos optimizan el inicio previo de esos procesos; son seguros para el sistema y como tal son correctos.*

Conexiones de red
La ventana de descripción contiene una lista de procesos y aplicaciones que se comunican a través de la red utilizando el protocolo seleccionado en la ventana de navegación (TCP o UDP) junto con la dirección remota a la que se conecta la aplicación. También puede comprobar el DNS que asigna las direcciones IP asignadas.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

Entradas de registro importantes
Contiene una lista de entradas de registro seleccionadas que suelen estar relacionadas con varios problemas con el sistema como las que

especifican programas de arranque, objeto de ayuda al navegador (BHO), etc.

En la ventana de descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana de detalles.

Servicios
La ventana de descripción contiene una lista de archivos registrados como Windows Services (Servicios de Windows). Puede comprobar la manera en la que se ha establecido el inicio del servicio junto con información específica del archivo en la ventana de detalles.

Controladores
Una lista de los controladores instalados en el sistema.

Archivos críticos
La ventana de descripción muestra el contenido de los archivos críticos relacionados con el sistema operativo Microsoft Windows.

Información del sistema
Contiene información detallada sobre el hardware y el software, junto con información sobre variables de entorno y derechos de usuario establecidos.

Detalles del archivo
Una lista de archivos importantes del sistema y archivos de la carpeta Archivos de programa. Se puede encontrar información adicional específica de los archivos en las ventanas de descripción y detalles.

Acerca de
Información sobre ESET SysInspector

5.4.1.3 Comparar

La característica Comparar permite al usuario comparar dos registros existentes. El resultado de esta función es un conjunto de elementos no comunes a ambos registros. Puede usar esta opción si desea realizar un seguimiento de los cambios realizados en el sistema; puede, por ejemplo, detectar la actividad de un código malicioso.

Una vez iniciada, la aplicación crea un nuevo registro, que aparecerá en una ventana nueva. Vaya a **Archivo** -> **Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, utilice el menú **Archivo** -> **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro a la vez.

Si compara dos registros, el principio fundamental reside en el hecho de que compara un registro activo actualmente con un registro guardado en un archivo. Para comparar registros, utilice la opción **Archivo** -> **Comparar registros** y seleccione **Seleccionar archivo**. El registro seleccionado se comparará con el activo en la ventana principal del programa. El resultante, denominado registro comparativo, mostrará sólo las diferencias entre esos dos registros.

Nota: *en caso de que compare dos archivos de registro, seleccione Archivo -> Guardar registro, y guárdelo como un archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, los registros incluidos en el mismo se compararán automáticamente.*

Junto a los elementos mostrados, SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.
Los elementos marcados con un ▬ sólo se encuentran en el registro activo y no están presentes en el registro comparativo abierto. Por otra parte, los elementos marcados con un ✚ están presentes sólo en el registro abierto y no en el registro activo.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

✚ Nuevo valor, que no se encuentra en el registro anterior.

La sección de estructura de árbol contiene nuevos valores.

▬ Valor eliminado, que sólo se encuentra en el registro anterior.

La sección de estructura de árbol contiene valores eliminados.

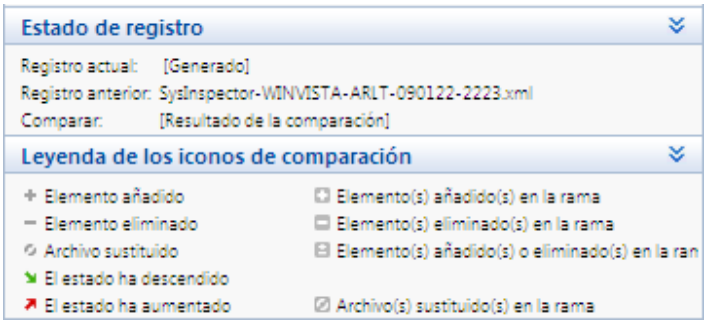
Se ha cambiado un valor o archivo.

La sección de estructura de árbol contiene valores o archivos modificados.

Ha disminuido el nivel de riesgo o era superior en el registro anterior.

Ha aumentado el nivel de riesgo o era inferior en el registro anterior.

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos, además de mostrar los nombres de los registros que se están comparando.



Se puede guardar cualquier registro comparativo en un archivo y abrirse posteriormente.

Ejemplo:
Genere y guarde un registro, registrando información original sobre el sistema, en un archivo con el nombre previo.xml. Tras realizar los cambios en el sistema, abra SysInspector y deje que genere un nuevo registro. Guárdelo en un archivo con el nombre actual.xml.

Para realizar un seguimiento de los cambios entre estos dos registros, vaya a **Archivo** -> **Comparar registros**. El programa creará un registro comparativo que muestra las diferencias entre los registros.

Se puede lograr el mismo resultado si utiliza la siguiente opción de la línea de comandos:

SysIsnpector.exe actual.xml previo.xml

5.4.1.4 SysInspector como parte de ESET Smart Security 4

Para abrir la sección SysInspector en ESET Smart Security 4, haga clic en **Herramientas > SysInspector**. El sistema de administración de la ventana de SysInspector es parecido al de los registros de análisis del equipo o las tareas programadas. Se puede obtener acceso a todas las operaciones con instantáneas del sistema (como crear, ver, comparar, eliminar y exportar), simplemente haciendo clic con el "mouse" una o dos veces.

La ventana de SysInspector contiene información básica acerca de las instantáneas creadas como, por ejemplo, la hora de creación, un breve comentario, el nombre del usuario que ha creado la captura y su estado.

Para **Comparar, Agregar...** o **Quitar** instantáneas, utilice los botones correspondientes ubicados debajo de la lista de instantáneas de la ventana de SysInspector. Estas opciones también están disponibles en el menú contextual. Para ver la instantánea del sistema seleccionada, utilice la opción del menú contextual **Ver**. Para exportar la instantánea seleccionada a un archivo, haga clic con el botón secundario del "mouse" en ella y seleccione **Exportar...**.
A continuación, se muestra una descripción detallada de las opciones disponibles:

Comparar: permite comparar dos registros existentes. Esta opción es ideal para realizar un seguimiento de los cambios entre el registro actual y el antiguo. Para poder aplicar este opción, debe seleccionar dos instantáneas con el fin de compararlas.

Agregar permite crear un nuevo registro. Debe introducir antes un breve comentario acerca del registro. Para obtener información sobre el porcentaje de progreso del proceso de creación de la instantánea que se está generando, consulte la columna Estado. Todas las instantáneas completadas aparecen marcadas con el estado Creada.

Quitar: elimina puertos de la lista.

Mostrar: muestra la instantánea seleccionada. También puede hacer doble clic en la entrada seleccionada.

Exportar...: guarda la entrada seleccionada en un archivo XML (y también en una versión comprimida).

5.5 ESET SysRescue

ESET Recovery CD (ERCD) es una utilidad que permite crear un disco de arranque que incluya ESET Smart Security 4 (ESS). La principal ventaja de ESET Recovery CD es que ESS se ejecuta de forma independiente del sistema operativo host, además de tener acceso directo al disco y a todo el sistema de archivos. Gracias a esto, se pueden eliminar amenazas que normalmente son imposibles de quitar como, por ejemplo, cuando el sistema operativo se está ejecutando, etc.

5.5.1 Requisitos mínimos

ESET SysRescue (ESR) se utiliza en el entorno de preinstalación de Microsoft Windows (Windows PE) versión 2.x basado en Windows Vista. Windows PE forma parte del paquete gratuito Kit de instalación automatizada de Windows (AIK de Windows), que debe instalarse previamente para poder crear ESR. Debido a la compatibilidad con la versión de 32 bits de Windows PE, ESR sólo se puede crear en la versión de 32 bits de ESS/ENA. ESR admite AIK de Windows 1.1 y posterior. ESR está disponible en ESS/ENA 4.0 y posterior.

5.5.2 Cómo crear un CD de recuperación

Si se cumplen los requisitos mínimos para la creación de un CD de ESET SysRescue (ESR), esta tarea es bastante sencilla. Para iniciar el asistente de ESR, haga clic en **Inicio > Programas > ESET > ESET Smart Security 4 > ESET SysRescue**.

En primer lugar, el asistente comprobará si están presentes AIK de Windows y un dispositivo adecuado para la creación de medios de arranque.

A continuación, seleccione el medio de destino en el que se encuentra ESR. Además de en CD/DVD/USB, puede optar también por guardar ESR en un archivo ISO. Puede grabar posteriormente esta imagen ISO en CD/DVD o utilizarla de algún otro modo (por ejemplo, en un entorno virtual como VmWare o Virtualbox).

Una vez especificados los parámetros, obtendrá una vista previa de la compilación en el último paso del asistente de ESET SysRescue. Revise los parámetros e inicie la compilación. Entre las opciones disponibles, se incluyen:

Carpetas
ESET Antivirus
Avanzadas
Dispositivo de arranque USB
Grabación

5.5.2.1 Carpetas

Carpeta temporal es un directorio de trabajo de archivos necesarios durante la compilación de ESET SysRescue.

Carpeta ISO es una carpeta donde el archivo ISO resultante se guarda una vez completada la compilación.

La lista de esta pestaña muestra todas las unidades de red locales y asignadas junto con el espacio libre disponible. Si alguna de las carpetas se ubican en una unidad con espacio libre insuficiente, recomendamos que seleccione otra unidad con más espacio libre disponible. De lo contrario, la compilación puede finalizar antes de tiempo debido a que el espacio libre en el disco es insuficiente.

Aplicaciones externas
Le permite seleccionar programas adicionales que se ejecutarán o instalarán después de efectuar el arranque desde el medio SysRescue.

Incluir aplicaciones externas: le permite agregar un programa externo a la compilación de SysRescue.

Carpeta seleccionada: carpeta en la que se encuentran los programas que se van a agregar al disco de SysRescue.

5.5.2.2 Antivirus ESET

Para crear un CD de ESET SysRescue, puede seleccionar dos fuentes de archivos ESET para que se utilicen en la compilación.

Carpeta de ESS: archivos que ya se encuentran en la carpeta en la que se ha instalado el producto ESET en el equipo.

Archivo MSI: se utilizan los archivos que se encuentran en el instalador de MSI.

Perfil: puede utilizar una de las siguientes fuentes de nombre de usuario y contraseña:

ESS instalado: el nombre de usuario y contraseña se copian desde la versión instalada actualmente de ESET Smart Security 4 o ESET NOD32.

Del usuario: se utilizan el nombre de usuario y la contraseña introducidas en los cuadros de textos correspondientes que aparecen a continuación.

Nota: *las aplicaciones ESET Smart Security 4 o ESET NOD32 que se encuentra en el CD de ESET SysRescue se actualizan a través de Internet o mediante la solución ESET Security instalada en el equipo donde se ejecuta el CD de ESET SysRescue.*

5.5.2.3 Avanzadas

La pestaña **Avanzadas** le permite optimizar el CD de ESET SysRescue respecto al tamaño de la memoria del equipo. Seleccione **512 MB o más** para escribir el contenido del CD en la memoria operativa (RAM). Si selecciona **menos de 512 MB**, se obtendrá acceso temporalmente al CD de recuperación cuando WinPE esté ejecutándose.

Controladores externos: en esta sección puede insertar controladores para su hardware específico (normalmente un adaptador de red). Aunque WinPE se basa en Windows Vista SP1 que admite hardware a gran escala, a veces éste no se reconoce y debe agregar manualmente el controlador. Hay dos maneras de agregar el controlador a la compilación de ESET SysRescue: manualmente (mediante el botón **Agregar**) y de forma automática (mediante el botón **Búsq. auto.**). En caso de agregarlo manualmente, tiene que seleccionar la ruta del archivo .inf correspondiente (el archivo *.sys aplicable también debe estar presente en esta carpeta). En caso de agregarlo automáticamente, se busca el controlador automáticamente en el sistema operativo del equipo en cuestión. Recomendamos utilizar el modo automático sólo si se utiliza SysRescue en un equipo con el mismo adaptador de red que el utilizado en el equipo en el que se creó SysRescue. Durante la creación de ESET SysRescue, el controlador se agrega a la

compilación para que el usuario no tenga que buscarlo por separado posteriormente.

5.5.2.4 Dispositivo de arranque USB

Si ha seleccionado un dispositivo USB como medio de destino, puede seleccionar uno de los medios USB disponibles en la pestaña Dispositivo de arranque USB (en caso de que haya más dispositivos USB).

Advertencia: *se le dará formato al dispositivo USB seleccionado durante el proceso de creación de ESET SysRescue, lo que significa que se eliminarán todos los datos del dispositivo.*

5.5.2.5 Grabar

Si ha seleccionado CD/DVD como medio de destino, puede especificar los parámetros de grabación adicionales en la pestaña Grabar.

Eliminar archivo ISO: marque esta opción para eliminar los archivos ISO una vez creado el CD de recuperación de ESET

Eliminación activada: permite seleccionar entre borrado rápido y completo.

Dispositivo de grabación: seleccione la unidad que se utilizará para grabar.

Advertencia: *ésta es la opción predeterminada. Si se utiliza un CD/DVD regrabable, se borrarán todos los datos que incluya dicho CD/DVD.*

La sección Medio incluye información sobre el medio actual introducido en su dispositivo de CD/DVD.

Velocidad de grabación: seleccione la velocidad deseada en el menú desplegable. Las capacidades de su dispositivo de grabación y el tipo de CD/DVD utilizado deben tenerse en cuenta a la hora de seleccionar la velocidad de grabación.

5.5.3 Trabajo con ESET SysRescue

Para poder utilizar eficazmente el CD/DVD/USB de recuperación, debe indicar que el equipo se inicie desde el medio de arranque de ESET SysRescue. La prioridad de arranque puede modificarse en el BIOS. También puede ejecutar el menú de arranque durante el inicio del equipo, normalmente mediante la tecla F9 o F12, en función de la versión de la placa base/BIOS que utilice.

Una vez efectuado el arranque, se iniciará ESS/ENA. Como ESET SysRescue sólo se utiliza en situaciones específicas, algunos módulos de protección y características del programa presentes en la aplicación ESS/ENA común no son necesarios. La lista se limitará a Análisis del equipo, Actualización y algunas secciones de la configuración. La capacidad de actualizar la base de firmas de virus es la característica más importante de ESET SysRescue. Le recomendamos que actualice el programa antes de iniciar un análisis del equipo.

5.5.3.1 Uso de ESET SysRescue

Imagine que un virus ha infectado los equipos de la red y modificado los archivos ejecutables (EXE). ESS/ENA es capaz de desinfectar todos los archivos infectados, a excepción de explorer.exe, que no se puede desinfectar, ni siquiera en el modo seguro.

Esto se debe a que explorer.exe, al ser un proceso fundamental de Windows, se inicia también en el modo seguro. ESS/ENA no puede realizar ninguna acción con el archivo, por lo que permanece infectado.

En ese caso, puede utilizar ESET SysRescue para solucionar el problema. Esta herramienta no necesita ningún componente del sistema operativo host, por lo que puede procesar (desinfectar y eliminar) cualquier archivo del disco.

6. Glosario

6.1 Tipos de amenazas

Una amenaza es un software malicioso que intenta entrar en el equipo de un usuario y dañarlo.

6.1.1 Virus

Un virus informático es una amenaza que daña los archivos existentes de su equipo. Su nombre se debe a los virus biológicos, ya que usan técnicas similares para extenderse desde un equipo a otro.

Los virus informáticos atacan principalmente a los archivos y documentos ejecutables. Para reproducirse, un virus adjunta su "cuerpo" al final de un archivo objetivo. En resumen, así es como funciona un virus informático: después de la ejecución del archivo infectado, el virus se activa (antes de la aplicación original) y realiza su tarea predefinida. Sólo después de hacerlo, se ejecuta la aplicación original. Un virus no puede infectar un equipo, a menos que un usuario (bien accidental o deliberadamente) ejecute o abra el programa malintencionado.

Los virus informáticos pueden variar en actividad y gravedad. Algunos son muy peligrosos, debido a su capacidad para eliminar archivos deliberadamente del disco duro. Por otro lado, algunos virus no pueden causar un daño real, sólo sirven para molestar al usuario y demostrar las capacidades técnicas de sus autores.

Es importante mencionar que los virus son (si se comparan con los troyanos o los spyware) cada vez más inusuales, ya que no son comercialmente atractivos para los autores de software malintencionado. Además, el término "virus" se utiliza incorrectamente con mucha frecuencia para abarcar todo tipo de amenazas. En la actualidad, esto se está superando gradualmente y se usa el nuevo y más preciso término "malware" (software malintencionado).

Si su equipo se infecta con un virus, será necesario restaurar los archivos infectados a su estado original, es decir, desinfectarlos usando un programa antivirus.

Ejemplos de virus son: OneHalf, Tenga y Yankee Doodle.

6.1.2 Gusanos

Un gusano informático es un programa que contiene códigos maliciosos que atacan a los equipos host y se extienden a través de una red. La diferencia básica entre un virus y un gusano es que los gusanos tienen la capacidad de reproducirse y viajar por sí mismos. No dependen de archivos host (ni sectores de arranque).

Los gusanos proliferan mediante el correo electrónico o paquetes de red. Así, los gusanos se pueden clasificar de dos formas:

- **Correo electrónico:** se distribuyen en direcciones de correo electrónico que se encuentran en la lista de contactos del usuario.
- **Red:** explotan las vulnerabilidades de seguridad en varias aplicaciones.

Por tanto, los gusanos son mucho más viables que los virus informáticos. Debido a la disponibilidad de Internet, se pueden extender por el globo en cuestión de horas desde su lanzamiento y, en algunos casos, incluso en cuestión de minutos. Esta capacidad para reproducirse de forma independiente y rápida los hace más peligrosos que otros tipos de malware, como los virus.

Un gusano activado en un sistema puede causar una serie de molestias: puede eliminar archivos, degradar el rendimiento del sistema o incluso desactivar algunos programas. Su naturaleza le permite servir de "medio de transporte" para otros tipos de amenazas.

Si el equipo está infectado con un gusano informático, es recomendable que elimine los archivos infectados, ya que son susceptibles de contener códigos maliciosos.

Ejemplos de gusanos conocidos son: Lovsan/Blaster, Stration/Warezov, Bagle y Netsky.

6.1.3 Troyanos

Históricamente, los troyanos informáticos se han definido como una clase de amenaza que intenta presentarse como programas útiles, engañando así a los usuarios para que les permitan ejecutarse. Sin embargo, es importante señalar que esto era verdad en el caso de los troyanos en el pasado; hoy en día, ya no necesitan camuflarse. Su único fin es infiltrarse lo más fácilmente posible y cumplir sus malintencionados objetivos. "Troyano" se ha convertido en un término muy general para describir cualquier amenaza que no se incluya bajo ninguna clase específica de amenaza.

Dado que se trata de una categoría muy amplia, con frecuencia se divide en muchas subcategorías. Las más conocidas son:

- descargador: programa malintencionado con capacidad para descargar otras amenazas de Internet.
- lanzador: tipo de troyano diseñado para lanzar otros tipos de malware en equipos cuya seguridad se ha visto comprometida.
- puerta trasera: aplicación que se comunica con atacantes remotos, lo que les permite tener acceso a los sistemas y controlarlos.
- registrador de pulsaciones: programa que registra cada pulsación que el usuario escribe y envía la información a atacantes remotos.
- marcador: los marcadores son programas diseñados para conectar con números de tarifa con recargo. Es casi imposible que un usuario note que se ha creado una conexión. Los marcadores sólo pueden causar daño a los usuarios con módems de marcación, que ya casi no se utilizan.

Normalmente, los troyanos adoptan la forma de archivos ejecutables con la extensión .exe. Si se detecta un archivo como troyano en su equipo, es recomendable que lo elimine, ya que lo más probable es que contenga códigos maliciosos.

Ejemplos de troyanos conocidos son: NetBus, Trojandownloader. Small.ZL, Slapper

6.1.4 Rootkits

Los rootkits son programas malintencionados que conceden a los atacantes de Internet un acceso ilimitado a un sistema, al tiempo que ocultan su presencia. Una vez que han obtenido acceso al sistema (normalmente explotando alguna vulnerabilidad del mismo), usan funciones del propio sistema operativo para evitar su detección por parte del antivirus: ocultan procesos, archivos y datos de registro de Windows. Por ello, es casi imposible detectarlos con las técnicas de detección normales.

A la hora de adoptar precauciones contra los rootkits, recuerde que existen dos niveles de detección:

1. Cuando intentan obtener acceso a un sistema. Aún no están presentes y, por tanto, están inactivos. La mayoría de los sistemas antivirus pueden eliminar rootkits en este nivel (suponiendo que realmente detecten dichos archivos como infectados).
2. Cuando se ocultan en la realización normal de análisis. Los usuarios del sistema antivirus ESET disfrutan de la ventaja de la tecnología Anti Stealth, que también puede detectar y eliminar rootkits activos.

6.1.5 Adware

Adware es la abreviatura de software relacionado con publicidad. Los programas que muestran material publicitario se incluyen en esta categoría. Las aplicaciones de adware suelen abrir automáticamente una nueva ventana emergente en un navegador de Internet que contiene anuncios o cambian la página de inicio del navegador. La aplicación de adware suele instalarse con programas gratuitos, lo que permite a los desarrolladores de esos programas cubrir los costes de desarrollo de sus aplicaciones (normalmente útiles).

La aplicación de adware no es peligrosa en sí, pues sólo molesta a los usuarios con publicidad. El peligro reside en el hecho de que la aplicación de adware también puede realizar funciones de seguimiento (tal y como lo hace una aplicación de spyware).

Si decide utilizar un producto gratuito, preste especial atención al programa de instalación. La mayoría de los programas de instalación le informarán sobre la instalación de un programa de adware adicional. Normalmente podrá cancelarlo e instalar el programa sin esta aplicación de adware. Por otra parte, en algunos casos, los programas no se instalarán sin la aplicación de adware, o su funcionalidad estará limitada. Esto significa que la aplicación de adware puede obtener acceso a menudo al sistema de manera "legal", porque los usuarios lo han aceptado. En este caso, es mejor ser prudente.

Si detecta un archivo como adware en su equipo, es recomendable que lo elimine, ya que lo más probable es que contenga códigos maliciosos.

6.1.6 Spyware

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento/conocimiento del usuario. Usan funciones de seguimiento para enviar varios datos estadísticos, como una lista de sitios web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista de palabras escritas.

Los autores de spyware afirman que el objetivo de estas técnicas es averiguar más sobre las necesidades y los intereses de los usuarios y permitir una publicidad mejor gestionada. El problema es que no existe una distinción clara entre las aplicaciones útiles y las malintencionadas, y no existe la completa seguridad de que no se haga un uso inadecuado de la información recuperada. Los datos obtenidos por aplicaciones spyware pueden contener códigos de seguridad, números PIN, números de cuentas bancarias, etc. Con frecuencia, el spyware se envía junto con versiones gratuitas de programas para generar ingresos o para ofrecer un incentivo para comprar el software. A menudo, se informa a los usuarios sobre la presencia de spyware durante la instalación de un programa para ofrecerles un incentivo para actualizar a una versión de pago sin necesidad de abonar la actualización.

Entre los ejemplos de productos freeware conocidos que se envían junto con spyware se encuentran las aplicaciones de cliente de redes P2P (peer to peer). Spyfalcon o Spy Sheriff (y muchos más) pertenecen a una subcategoría específica de spyware: parecen ser programas antiespía, pero son en realidad programas spyware.

Si detecta un archivo como spyware en su equipo, es recomendable que lo elimine, ya que lo más probable es que contenga códigos maliciosos.

6.1.7 Aplicaciones potencialmente peligrosas

Existen muchos programas legítimos que sirven para simplificar la administración de equipos en red. Sin embargo, en las manos equivocadas, se pueden utilizar con fines malintencionados. Por ello, ESET ha creado esta categoría especial. Nuestros clientes tienen ahora la opción de elegir si el sistema antivirus debería o no detectar estas amenazas.

"Aplicaciones potencialmente peligrosas" es la clasificación utilizada para el software comercial legítimo. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban cada tecla pulsada por un usuario).

Si averigua que existe una aplicación potencialmente peligrosa presente y en ejecución en su equipo (y no la ha instalado usted), consulte con el administrador de red o elimine la aplicación.

6.1.8 Aplicaciones potencialmente indeseables

Las aplicaciones potencialmente indeseables no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del equipo de forma negativa. Dichas aplicaciones suelen necesitar consentimiento para su instalación. Si se encuentran en su equipo, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontraba antes de la instalación). Los cambios más importantes son:

- Se abren nuevas ventanas que no se habían visto anteriormente.
- Activación y ejecución de procesos ocultos.
- Mayor aumento de los recursos del sistema.
- Cambios en los resultados de búsqueda.
- La aplicación se comunica con servidores remotos.

6.2 Tipos de ataques remotos

Existen muchas técnicas especiales que permiten a los atacantes poner en peligro sistemas remotos. Se dividen en varias categorías.

6.2.1 Ataques por denegación de servicio (DoS)

DoS, o denegación de servicio, es un tipo de ataque que intenta que el equipo o la red no esté disponible para sus usuarios. La comunicación entre los usuarios afectados se bloquea y no puede continuar de una manera funcional. Normalmente, los equipos expuestos a ataques DoS deben reiniciarse; de lo contrario, no funcionarán correctamente.

En la mayoría de casos, los objetivos son servidores web y la intención es que no estén disponibles para los usuarios durante un determinado período de tiempo.

6.2.2 Envenenamiento DNS

Mediante el método de envenenamiento DNS (Servidor de nombre de dominio), los atacantes pueden engañar al servidor DNS de cualquier equipo para que crea que los datos falsos que envían son legítimos y auténticos. La información falsa se guarda en la caché durante un determinado período de tiempo, lo que permite a los atacantes volver a escribir respuestas DNS de direcciones IP. Como resultado, los usuarios que intentan obtener acceso a sitios web en Internet descargarán virus o gusanos en sus equipos en lugar de su contenido original.

6.2.3 Ataques de gusanos

Un gusano informático es un programa que contiene códigos maliciosos que atacan a los equipos host y se extienden a través de una red. Los gusanos de la red explotan las vulnerabilidades de seguridad en varias aplicaciones. Debido a la disponibilidad de Internet, se pueden extender por todo el mundo en cuestión de horas desde su lanzamiento. En algunos casos, incluso en cuestión de minutos.

La mayoría de los ataques de gusanos (Sasser, SqlSlammer) se pueden evitar usando la configuración de seguridad predeterminada del cortafuegos o bloqueando los puertos no protegidos o no usados. Además, también es esencial proteger el sistema con los parches de seguridad más recientes.

6.2.4 Análisis de puertos

El análisis de puertos controla si existen puertos del equipo abiertos en un host de red. Un analizador de puertos es un software diseñado para encontrar estos puertos.

Un puerto de un equipo es un punto virtual que administra los datos entrantes y salientes; esto es crucial desde el punto de vista de la seguridad. En una red de gran tamaño, la información recopilada por los analizadores de puertos puede ayudar a identificar posibles vulnerabilidades. Dicho uso es legítimo.

Sin embargo, con frecuencia, los delincuentes informáticos usan los análisis de puertos para poner en peligro la seguridad. Su primer paso es enviar paquetes a cada puerto. En función del tipo de respuesta, es posible determinar qué puertos están en uso. El análisis en sí no causa daños, pero tenga en cuenta que esta actividad puede revelar vulnerabilidades potenciales y permitir a los atacantes tomar el control de equipos remotos.

Se aconseja a los administradores de red que bloqueen todos los puertos no usados y que protejan aquéllos que están en uso contra el acceso no autorizado.

6.2.5 Desincronización TCP

La desincronización TCP es una técnica que se usa en ataques de secuestro de TCP. Se desencadena mediante un proceso en el que el número secuencial en paquetes entrantes difiere del número secuencial previsto. Se rechazan los paquetes con un número secuencial no previsto (o se guardan en el almacén del búfer, si están presentes en la ventana de comunicación actual).

En el estado de desincronización, ambos puntos finales de comunicación rechazan los paquetes recibidos. Éste es el punto en el que los atacantes remotos pueden infiltrar y suministrar paquetes con un número secuencial correcto. Los atacantes incluso pueden manipular la comunicación con sus comandos o modificarla de alguna otra forma.

El objetivo de los ataques de secuestro de TCP es interrumpir las comunicaciones servidor-cliente o de igual a igual. Muchos ataques se pueden evitar mediante la autentificación de cada segmento de TCP. También se aconseja usar las configuraciones recomendadas para sus dispositivos de red.

6.2.6 SMB Relay

SMBRelay y SMBRelay2 son programas especiales para llevar a cabo un ataque contra equipos remotos. Los programas aprovechan el protocolo para compartir archivos Bloque de mensajes del servidor, que tiene capas en NetBIOS. Si un usuario comparte una carpeta o directorio en la red LAN, lo más probable es que use este protocolo para compartir archivos.

Dentro de la comunicación de red local, se intercambian hashes de contraseña.

SMBRelay recibe una conexión en los puertos UDP 139 y 445, transmite los paquetes intercambiados por el cliente y el servidor y los modifica. Una vez realizada la conexión y la autentificación, se desconecta al cliente. SMBRelay crea una nueva dirección IP virtual. Se puede tener acceso a la nueva dirección con el comando "net use \\192.168.1.1". Después, cualquiera de las funciones de red de Windows puede usar la dirección. SMBRelay transmite la comunicación del protocolo SMB, excepto la negociación y la autentificación. Los atacantes remotos pueden usar la dirección IP, siempre que el equipo del cliente esté conectado.

SMBRelay2 funciona según el mismo principio que SMBRelay, excepto que usa nombres de NetBIOS en lugar de direcciones IP. Ambos pueden realizar ataques "hombre en medio". Estos ataques permiten a los atacantes remotos leer, insertar y modificar mensajes intercambiados entre dos puntos finales de comunicación sin ser detectados. Normalmente, los equipos expuestos a dichos ataques dejan de responder o se reinician inesperadamente.

Para evitar ataques, es recomendable que use contraseñas o claves de autentificación.

6.2.7 Ataques ICMP

El ICMP (Protocolo de mensajes de control de Internet) es un protocolo de Internet muy conocido y utilizado. Lo usan fundamentalmente equipos en red para enviar distintos mensajes de error.

Los ataques remotos intentan aprovecharse de los puntos débiles del protocolo ICMP. El protocolo ICMP está diseñado para una comunicación unidireccional que no requiera autentificación. De esta forma, los ataques remotos pueden activar los ataques denominados DoS (por denegación de servicio), o los ataques que proporcionan a individuos no autorizados acceso a paquetes entrantes y salientes.

Entre los ejemplos más habituales de ataques ICMP se encuentran los ataques "flood" mediante Ping, "flood" de ICMP_ECHO y los ataques Smurf (denegación de servicios). Los equipos expuestos al ataque de ICMP son significativamente más lentos (afecta a todas las aplicaciones que usen Internet) y tienen problemas para conectarse a Internet.

6.3 Correo electrónico

El correo electrónico es una forma de comunicación moderna que cuenta con muchas ventajas. Es flexible, rápido y directo. El correo electrónico tuvo un papel fundamental en la expansión de Internet a comienzos de los años 90.

Desafortunadamente, con su alto nivel de anonimato, el correo electrónico e Internet dan cabida a actividades ilegales como la distribución de correo no deseado. El correo no deseado cuenta con diversas categorías, entre las que se incluyen anuncios no solicitados, información falsa y la difusión de software malicioso (malware). El inconveniente y el peligro para el usuario se ve incrementado por el hecho de que los costes de envío son nulos y los autores de los mensajes de correo no deseado disponen de muchos recursos y herramientas para adquirir nuevas direcciones de correo electrónico. Además, la cantidad y la variedad de correo no deseado dificulta en gran medida su regulación. Cuanto más utilice su dirección de correo electrónico, mayores serán las posibilidades de que acabe en la base de datos de un motor de correo no deseado. a continuación, le ofrecemos algunos consejos para su prevención:

- Si es posible, no publique su dirección de correo electrónico en Internet.
- Proporcione su dirección de correo electrónico únicamente a personas de confianza.
- Si es posible, no utilice alias muy comunes; cuanto más complicados sean, menor será la posibilidad de que puedan obtenerlos.
- No conteste a mensajes de correo no deseado que hayan llegado a su buzón de correo.
- Tenga cuidado a la hora de rellenar formularios de Internet; preste especial atención a casillas como "Sí, deseo recibir información sobre (...) en mi bandeja de entrada".
- Utilice direcciones de correo electrónico "especializadas", por ejemplo, una para el trabajo, otra para comunicarse con sus amigos, etc.
- Cambie su dirección de correo electrónico periódicamente.
- Utilice una solución contra el correo no deseado.

6.3.1 Publicidad

La publicidad en Internet es una de las formas de publicidad con un mayor y más rápido crecimiento. La publicidad por correo electrónico utiliza éste como medio de contacto. Sus principales ventajas de marketing son los costes inexistentes, un alto nivel de eficacia y confianza y, lo más importante, el hecho de que los mensajes se entregan casi de inmediato. Muchas compañías utilizan herramientas de marketing por correo electrónico para comunicarse eficazmente con sus clientes actuales y potenciales.

Este medio de publicidad es legítimo, ya que es posible que el usuario esté interesado en recibir información comercial sobre algunos productos. Sin embargo, la realidad es que muchas compañías envían mensajes comerciales no solicitados en serie. En dichos casos, la publicidad por correo electrónico cruza la línea y se convierte en correo no deseado.

La cantidad de correo electrónico comercial no solicitado se ha convertido en un verdadero problema, ya que no muestra signos de moderación. Los autores de correo electrónico no solicitado intentan disfrazar el correo no deseado como mensajes legítimos. Por otra parte, la publicidad legítima en grandes cantidades puede producir reacciones negativas.

6.3.2 Información falsa

La información falsa se extiende a través de Internet en forma de mensaje. Normalmente, se envía por correo electrónico y, en ocasiones, a través de herramientas de comunicación como ICQ y Skype. El mensaje en sí suele tratarse de una broma o de una leyenda urbana.

La información falsa sobre virus informáticos pretende generar miedo, incertidumbre y duda en los destinatarios, haciéndoles creer que existe un "virus indetectable" que elimina archivos y recupera contraseñas, o que realiza ciertas acciones que pueden provocar daños en el sistema.

Algunos mensajes de información falsa pretenden causar situaciones embarazosas para otras personas. Normalmente, se solicita a los destinatarios que reenvíen estos mensajes a todos sus contactos, de forma que se prolongue el ciclo de vida del mensaje con información falsa. La información falsa también se transmite a través de teléfonos móviles, peticiones de ayuda, personas que se ofrecen a enviarle dinero desde países extranjeros, etc. En la mayoría de los casos, es imposible averiguar la intención del creador.

En principio, si ve un mensaje que le solicita que lo reenvíe a todas las personas que conozca, es muy probable que se trate de información falsa. Existen muchos sitios web especializados en Internet que pueden verificar si un mensaje de correo electrónico es legítimo o no. Antes de reenviarlos, realice una búsqueda en Internet sobre cualquier mensaje del que sospeche que contiene información falsa.

6.3.3 Phishing

El término phishing define una actividad delictiva que usa técnicas de ingeniería social (manipulando a los usuarios para obtener información confidencial). Su objetivo es obtener acceso a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc.

Normalmente, el acceso se consigue enviando mensajes de correo electrónico que fingen proceder de personas o empresas de confianza (instituciones financieras, compañías de seguros). La apariencia del mensaje de correo electrónico podría ser muy genuina y contener gráficos y texto originales de la fuente por la que desean hacerse pasar. Se le pedirá que escriba, con varios pretextos (verificación de datos, operaciones financieras, etc.), algunos de sus datos personales: números de cuentas bancarias o nombres de usuario y contraseñas. Dichos datos, si se envían, se pueden sustraer fácilmente o utilizar fraudulentamente.

Tenga en cuenta que los bancos, las compañías de seguros y otras empresas legítimas nunca le pedirían sus nombres de usuario y contraseñas en un mensaje de correo electrónico no solicitado.

6.3.4 Reconocimiento de correo no deseado

Generalmente, existen varios indicadores que pueden ayudarle a identificar el correo no deseado (SPAM) en su buzón de correo. Si un mensaje cumple, como mínimo, una de las siguientes condiciones, es muy probable que se trate de un mensaje de correo no deseado.

- La dirección del remitente no pertenece a ninguna persona de su lista de contactos
- El mensaje le ofrece una gran cantidad de dinero, pero tiene que proporcionar una pequeña cantidad previamente.
- El mensaje le solicita que introduzca, con varios pretextos (verificación de datos, operaciones financieras, etc.), algunos de sus datos personales (números de cuentas bancarias, nombres de usuario y contraseñas, etc.).
- Está escrito en un idioma extranjero.
- Le solicita que adquiera un producto en el que no está interesado. Si decide comprarlo de todos modos, compruebe que el remitente del mensajes es un proveedor fiable (consulte el fabricante del producto original).
- Algunas palabras están mal escritas para intentar engañar a su filtro de correo no deseado. Por ejemplo, "vaigra" en lugar de "viagra", entre otras.

6.3.4.1 Reglas

En el contexto de las soluciones contra correo no deseado y los clientes de correo electrónico, las reglas son herramientas para manipular funciones de correo electrónico. Consisten en dos partes lógicas:

1. Condición (por ejemplo, un mensaje entrante de una dirección concreta)
2. Acción (por ejemplo, eliminación del mensaje, llevándolo a una carpeta específica).

El número y la combinación de reglas varía en función de la solución contra correo no deseado. Estas reglas sirven como medidas contra el correo no deseado. Ejemplos típicos:

- 1. Condición: un mensaje de correo electrónico entrante contiene algunas palabras que normalmente aparecen en los mensajes de correo no deseado.
  2. Acción: Elimine el mensaje.
- 1. Condición: un mensaje de correo electrónico entrante contiene un archivo adjunto con una extensión .exe.
  2. Acción: Elimine el archivo adjunto y envíe el mensaje a la bandeja de entrada.
- 1. Condición: Recibe un mensaje entrante de su jefe.
  2. Acción: Envíe el mensaje a la carpeta "Trabajo".

Es recomendable que use una combinación de reglas en programas contra correo no deseado para facilitar la administración y filtrar el correo no deseado de forma más eficaz.

6.3.4.1 Filtro Bayesiano

El filtro Bayesiano de correo no deseado es una forma muy efectiva de filtrar correo electrónico utilizada por casi todos los productos contra correo no deseado. Puede identificar correo electrónico no solicitado con un alto grado de precisión, así como funcionar según las necesidades del usuario.

La funcionalidad se basa en el proceso de aprendizaje que tiene lugar en la primera fase. El usuario marca manualmente un número suficiente de mensajes como mensajes legítimos o como correo no deseado (normalmente 200/200). El filtro analiza ambas categorías y aprende, por ejemplo, que el correo no deseado suele contener palabras como "rolex" o "viagra", mientras que los familiares envían mensajes legítimos o éstos proceden de direcciones de la lista de contactos del usuario. Si se procesa un número mayor de mensajes, el filtro Bayesiano puede asignar un determinado "índice de correo no deseado" a cada mensaje y determinar si se trata de correo no deseado o no.

La principal ventaja es su flexibilidad. Por ejemplo, si un usuario es biólogo, todos los mensajes de correo electrónico entrantes sobre biología o campos de estudio relativos recibirán normalmente un índice de probabilidad inferior. Si un mensaje incluye palabras que, de lo contrario, lo califican de no solicitado, pero lo envía alguien de una lista de contactos, se marcará como legítimo, ya que los remitentes de una lista de contactos reducen la probabilidad general de correo no deseado.

6.3.4.2 Lista blanca

En general, una lista blanca es una lista de elementos o personas aceptados o a los que se ha concedido permiso de acceso. El término "lista blanca de correo electrónico" es una lista de contactos de quienes el usuario desea recibir mensajes. Estas listas blancas se basan en palabras clave que se buscan en direcciones de correo electrónico, nombres de dominios o direcciones IP.

Si una lista blanca funciona en "modo de exclusividad", los mensajes de una dirección, un dominio o una dirección IP distintos no se recibirán. Por otra parte, si no es exclusiva, estos mensajes no se eliminarán, sino que se filtrarán de alguna otra forma.

Una lista blanca se basa en el principio opuesto al de una lista negra. Las listas blancas son relativamente fáciles de mantener, más que las listas negras. Es recomendable que use las listas blanca y negra para filtrar el correo no deseado de forma más eficaz.

6.3.4.3 Lista negra

Normalmente una lista negra es una lista de personas o elementos prohibidos o no aceptados. En el mundo virtual, es una técnica que permite aceptar mensajes de todos los usuarios no presentes en dicha lista.

Existen dos tipos de lista negra. Los usuarios pueden crear listas negras personalizadas usando el programa contra correo no deseado. Por otra parte, se pueden encontrar en Internet muchas listas negras profesionales, actualizadas con regularidad, creadas por instituciones especializadas.

Una lista negra se basa en el principio opuesto al de una lista blanca. El uso de listas negras es un componente esencial para filtrar correo no deseado correctamente; sin embargo, son muy difíciles de mantener, ya que todos los días aparecen nuevos elementos que deben bloquearse. Es recomendable que use las listas blanca y negra para filtrar el correo no deseado de forma más eficaz.

6.3.4.5 El control del servidor

El control del servidor es una técnica que sirve para identificar correo electrónico no deseado en masa basándose en el número de mensajes recibidos y las reacciones de los usuarios. Cada mensaje deja una "huella" digital única en el servidor basada en el contenido del mismo. De hecho, es un número de identificación exclusivo que no dice nada sobre el contenido del mensaje de correo electrónico. Dos mensajes idénticos tendrán huellas idénticas, mientras que los mensajes diferentes tendrán huellas diferentes.

Si se marca un mensaje como no deseado, su huella se envía al servidor. Si el servidor recibe más huellas idénticas (correspondientes a un determinado mensaje no deseado), la huella se guarda en la base de datos de huellas de correo no deseado. Al analizar mensajes entrantes, el programa envía las huellas de los mensajes al servidor, que devuelve información sobre las huellas que corresponden a los mensajes ya marcados por los usuarios como no deseados.