Avira

Professional Security

Manual para usuarios

Marcas comerciales y copyright

Marcas comerciales

Windows es una marca registrada de Microsoft Corporation en EE. UU. y otros países.
Todas las marcas y productos mencionados son propiedad de sus respectivos propietarios.
Las marcas comerciales protegidas no están marcadas como tales en el presente manual. Esto no significa, de todas formas, que pueden usarse libremente.

Información de copyright

Para Avira Professional Security se utiliza el código de otros proveedores. Agradecemos a los titulares del copyright que hayan puesto su código a nuestra disposición.
Encontrará más información sobre el copyright en Licencias de terceros.

Acuerdo de licencia de usuario final: EULA

http://www.avira.com/es/license-agreement

Política de privacidad

http://www.avira.com/es/general-privacy

Índice

1. Introducción

Con su producto Avira protege su equipo frente a virus, gusanos, troyanos, adware y spyware, así como frente a otros riesgos. Para abreviar, en este manual se habla de virus o malware (software malintencionado) y programas no deseados.

El manual describe la instalación y el uso del programa.

Puede encontrar más opciones e información en nuestro sitio web:

http://www.avira.es

En el sitio web de Avira, podrá hacer lo siguiente:

- Acceder a información sobre otros programas de Avira Desktop
- Descargar los programas más recientes de Avira Desktop
- Descargar los manuales de producto más actuales en formato PDF
- Descargar herramientas gratuitas de soporte y reparación
- Utilizar la completa base de datos de conocimientos y los artículos de FAQ para solucionar problemas
- Acceder a las direcciones de soporte específicas de cada país.

Su equipo Avira

1.1 Iconos y resaltados

Se utilizan los siguientes iconos:

Icono/Denominación	Explicación
✓	Se coloca delante de una condición que debe cumplirse antes de ejecutar una acción.
▸	Se coloca delante de un paso de acción que se ejecuta.
↪	Se coloca delante de un resultado que se deduce de la acción precedente.
Advertencia	Se coloca delante de una advertencia en caso de riesgo de pérdida grave de datos.

Nota	Se coloca delante de una nota con información especialmente importante o delante de una sugerencia que facilita el entendimiento y uso de su producto Avira.

Se usan los siguientes resaltados:

Resaltado	Explicación
Cursiva	Nombre de fichero o indicación de ruta.
	Elementos que se muestran de la interfaz de software (p. ej., área de la ventana o mensaje de error).
Negrita	Elementos en los que se hace clic de la interfaz de software (p. ej., opción de menú, sección, botones de opción o botón).

2. Información de producto

En este capítulo se facilita la información que necesita para adquirir y usar su producto Avira:

- consulte el capítulo: Prestaciones
- consulte el capítulo: Requisitos del sistema
- consulte el capítulo: Licencias y actualizaciones

Los productos de Avira ofrecen herramientas completas y flexibles que permiten proteger eficazmente su equipo ante virus, malware, programas no deseados y otros riesgos.

▸ Tenga en cuenta lo siguiente:

Advertencia
La pérdida de datos valiosos con frecuencia conlleva consecuencias dramáticas. Y ni siquiera el mejor programa de protección antivirus puede protegerle al cien por cien ante pérdidas de datos. Haga copias de seguridad (backups) de sus datos con regularidad.

Nota
Un programa diseñado para la protección contra virus, malware, programas no deseados y otros riesgos tan solo puede ser fiable y eficaz si está actualizado. Asegúrese de que su producto Avira esté siempre al día activando la actualización automática. Para ello, configure el programa debidamente.

2.1 Prestaciones

Su producto Avira tiene las siguientes funciones:

- Centro de control para la supervisión, la administración y el control del programa
- Configuración central con ajustes estándar y avanzados fácilmente configurables y ayuda contextual
- Scanner (análisis por demanda) para la búsqueda configurable y guiada por perfiles de todo tipo de virus y malware
- Integración en el Control de cuentas de usuario (User Account Control) de Windows para poder llevar a cabo tareas que precisan de permisos de administrador.
- Real-Time Protection (análisis automático) para la supervisión continua de ficheros
- Componentes ProActiv para la supervisión continua de acciones de programa (solo para sistemas de 32 bits)

- Mail Protection (análisis POP3, análisis IMAP y análisis SMTP) para la detección continua de virus y malware en su correo electrónico, adjuntos incluidos
- Web Protection para la supervisión de los datos y ficheros transferidos desde Internet mediante el protocolo HTTP (supervisión de los puertos 80, 8080 y 3128)
- Administración integrada de la cuarentena para aislar y tratar ficheros sospechosos
- Rootkits Protection para detectar malware instalado de manera oculta en el sistema (rootkits)
  (no disponible en Windows XP 64 bits)
- Acceso directo a través de Internet a la detallada información relativa a los virus y malware detectados
- Actualización rápida y sencilla del programa, del archivo de firmas de virus y del motor de análisis mediante Single File Update; actualización incremental del archivo de firmas de virus a través de un servidor web en Internet o en una Intranet
- Concesión de licencias sencilla en la administración de licencias
- Programador integrado de tareas únicas o recurrentes, como actualizaciones o verificaciones
- Alta capacidad de detección de virus y malware mediante innovadoras tecnologías de análisis (motores de análisis), incluida la búsqueda heurística
- Detección de los tipos de archivo más corrientes, como archivos comprimidos y extensiones inteligentes
- Alto rendimiento gracias a la capacidad de multithreading (análisis concurrente de numerosos ficheros a alta velocidad)
- FireWall para proteger el equipo de accesos no autorizados desde Internet o desde una red, así como de accesos no autorizados a Internet o a una red por usuarios sin permiso.

2.2 Requisitos del sistema

2.2.1 Requisitos del sistema Avira Professional Security

Avira Professional Security presenta los siguientes requisitos para una una instalación con éxito del sistema:

Sistema operativo

- Windows 8, SP más reciente (32 o 64 bits) o
- Windows 7, SP más reciente (32 o 64 bits) o
- Windows XP, SP más reciente (32 bits o 64 bits)

Hardware

- Procesador Pentium, como mínimo 1 GHz

- Mínimo de 150 MB de espacio libre en disco duro (más espacio aún si se utiliza la cuarentena y para la memoria temporal)
- Mínimo de 1024 MB de memoria RAM en Windows 8, Windows 7
- Mínimo de 512 MB de memoria con Windows XP

Otros requisitos

- Para la instalación del programa: permisos de administrador
- Para todas las instalaciones: Windows Internet Explorer 6.0 o superior
- Conexión a Internet cuando sea necesario (consulte Preparación de la instalación)

2.2.2 Derechos de administrador (a partir de Windows Vista)

En Windows XP existen muchos usuarios que trabajan con derechos de administrador. Sin embargo, desde el punto de vista de la seguridad, esto no es en absoluto deseable, ya que los virus y programas no deseados también pueden penetrar más fácilmente en el equipo.

Por esa razón, Microsoft ha establecido el "Control de cuentas de usuario" (User Account Control, UAC). El Control de cuentas de usuario forma parte de los siguientes sistemas operativos:

- Windows Vista
- Windows 7
- Windows 8

El Control de cuentas de usuario ofrece más protección para los usuarios que han iniciado sesión como administradores. Así, un administrador disfruta en principio únicamente de los privilegios de un usuario normal. El sistema operativo marca claramente con un icono indicador las acciones que requieren derechos de administrador. Además, el usuario debe confirmar explícitamente la acción deseada. Una vez dado este consentimiento, aumentan los privilegios y el sistema operativo lleva a cabo la correspondiente tarea administrativa.

Avira Professional Security precisa de derechos de administrador para realizar diversas acciones. Estas se marcan con el siguiente signo:  . Si, además, este signo aparece en un botón, para llevar a cabo esta acción necesitará derechos de administrador. Si su actual cuenta de usuario no tiene derechos de administrador, la ventana de diálogo en Windows le pedirá que introduzca la contraseña del administrador para el Control de cuentas de usuario. Si no tiene contraseña de administrador, no podrá realizar esta acción.

2.2.3 Incompatibilidades con otros programas

Avira Professional Security

Avira Professional Security no puede usarse actualmente junto con los siguentes productos:

- PGP Desktop Home
- PGP Desktop Professional 9.0
- CyberPatrol

Un comportamiento erróneo de los productos mencionados puede provocar que Avira Mail Protection (escáner de POP3) de Avira Professional Security no funcione o que se desestabilice el sistema. Avira colabora con PGP y CyberPatrol para encontrar una solución al problema. Hasta que se encuentre la solución, recomendamos encarecidamente desinstalar los productos mencionados antes de instalar Avira Professional Security.

Avira Web Protection

Avira Web Protection no es compatible con los siguientes productos:

- Bigfoot Networks Killer Ethernet Controller
- Teleport Pro de Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording de SCM Microsystems
- MSN Messenger de Microsoft

Por ello, Avira Web Protection omite los datos que estos productos envían y solicitan.

> **Nota**
> Avira Mail Protection no funciona si en el mismo PC ya hay instalado un servidor de correo (p. ej., AVM KEN, Exchange...).

2.3 Licencias y actualizaciones

2.3.1 Concesión de licencia

Para poder utilizar su producto Avira, es necesario disponer de una licencia. Disponer de una licencia implica aceptar las condiciones de la misma.

La licencia se concede a través de una clave de licencia digital en forma de fichero *.KEY*. Esta clave de licencia digital constituye la central de activación de su licencia personal. Contiene la información específica sobre los programas para los que tiene licencia y los períodos de tiempo en que estas licencias son válidas. Una única clave de licencia digital puede incluir licencias de varios productos.

Si ha adquirido su producto Avira por Internet, se le enviará la clave de licencia digital a través de un correo electrónico; en caso contrario, puede encontrarla en el CD/DVD del

programa. Puede cargar la clave de licencia durante la instalación del programa o instalarla posteriormente desde la administración de licencias.

2.3.2 Prolongación de licencia

Si su licencia está a punto de vencer, Avira le recuerda mediante una ventana emergente que debe prolongarla. Para hacerlo solo debe hacer clic en un enlace y se le redirigirá a la tienda online de Avira.

Si se ha registrado en el portal de licencias de Avira, también puede prolongar su licencia adicionalmente a través del **Sinóptico de licencias** o seleccionar la prolongación automática.

> **Nota**
> Si su producto Avira está administrado por la consola AMC, su administrador llevará a cabo la actualización. Se le solicitará guardar sus datos y reiniciar el sistema. Si no realiza estas acciones, su equipo no estará suficientemente protegido.

2.3.3 Administración de licencias

La administración de licencias de Avira Professional Security permite instalar la licencia de Avira Professional Security de manera muy fácil.

Administración de licencias de Avira Professional Security

Para efectuar la instalación de la licencia, haga doble clic en el archivo de licencias en su administrador de archivos o en el correo electrónico de activación, y siga las instrucciones que aparecen en pantalla.

Nota
La administración de licencias de Avira Professional Security copia automáticamente la licencia correspondiente en la carpeta de producto. Si ya se dispone de una licencia, aparecerá un mensaje que pregunta si se desea remplazar el fichero de licencias existente. Si se acepta, este fichero será sustituido por el fichero de licencias actual.

3. Instalación y desinstalación

Este capítulo contiene información relativa a la instalación de Avira Professional Security.

3.1 Preparación de la instalación

✓ Antes de la instalación, compruebe si su equipo cumple los requisitos del sistema.
✓ Cierre todas las aplicaciones en ejecución.
✓ Asegúrese de que no existen otras soluciones de protección antivirus. Las funciones automáticas de protección de las distintas soluciones de seguridad podrían interferir entre ellas (para obtener información sobre las opciones automáticas, consulte Eliminar software incompatible).
✓ Si es necesario, desinstale las barras de herramientas de búsqueda instaladas anteriormente antes de instalar Avira SearchFree Toolbar. De lo contrario, no podrá instalar Avira SearchFree Toolbar.
✓ Establezca una conexión a Internet.

- La conexión es necesaria para llevar a cabo los siguientes pasos de la instalación:
  - Descarga de los archivos de programa actuales y del motor de análisis, así como de los archivos de firmas de virus actuales del día mediante el programa de instalación (en instalaciones basadas en Internet)
  - Activación del programa
  - Registro como usuario
  - Si fuera necesario, ejecución de una actualización tras finalizar la instalación

✓ Debe utilizar el código de activación o el archivo de licencia de Avira Professional Security cuando desee activar el programa.
✓ Para la activación o registro del producto, Avira Professional Security utiliza el protocolo HTTP y el puerto 80 (comunicaciones web), así como el protocolo de cifrado SSL y el puerto 443 para comunicarse con los servidores de Avira. Si usa un cortafuegos, asegúrese de que este no bloquee las conexiones necesarias y los datos entrantes o salientes.

3.2 Instalación desde CD en línea

- Introduzca el CD de Avira Professional Security.

  Si el inicio automático está habilitado, haga clic en **Abrir carpeta** para ver los archivos.
  O BIEN

  Vaya a la unidad de CD, haga clic con el botón derecho en AVIRA y seleccione **Abrir carpeta** para ver los archivos.

  Haga doble clic en el archivo *autorun.exe*.

  En el menú del CD, elija la versión en línea para la instalación.

  El programa comprueba si existe software incompatible (puede obtener más información aquí: Eliminar software incompatible).

  Haga clic en **Siguiente** en la pantalla de bienvenida.

  Seleccione el idioma y haga clic en **Siguiente**. Todos los archivos necesarios para la instalación se descargan de los servidores web de Avira.

  Continúe con Elección del tipo de instalación.

3.3 Instalación desde CD sin conexión

- Introduzca el CD de Avira Professional Security.

  Si el inicio automático está habilitado, haga clic en **Abrir carpeta** para ver los archivos.
  O BIEN

  Vaya a la unidad de CD, haga clic con el botón derecho en AVIRA y seleccione **Abrir carpeta** para ver los archivos.

  Haga doble clic en el archivo *autorun.exe*.

  En el menú del CD, elija la versión sin conexión para la instalación.

  El programa comprueba si existe software incompatible (puede obtener más información aquí: Eliminar software incompatible).

  Se extrae el archivo de instalación. Se inicia la rutina de instalación.

  Continúe con Elección del tipo de instalación.

3.4 Instalación de software descargado de la tienda Avira

- Vaya a www.avira.com/download.

  Seleccione el producto y haga clic en **Descargar**.

  Guarde el archivo descargado en el sistema.

  Haga clic en el archivo de instalación Avira Professional Security_es.exe.

Si aparece la ventana del Control de cuentas de usuario, haga clic en Sí.

El programa comprueba si existe software incompatible (puede obtener más información aquí: Eliminar software incompatible).

Se extrae el archivo de instalación. Se inicia la rutina de instalación.

Continúe con Selección del tipo de instalación.

3.5 Eliminar software incompatible

Avira Professional Security examinará su equipo para comprobar si existe software incompatible. Si se detecta software que puede ser incompatible, Avira Professional Security generará la correspondiente lista de estos programas. Se recomienda desinstalar el software que ponga en riesgo su equipo.

- Seleccione de la lista aquellos programas que desee desinstalar automáticamente de su equipo y haga clic en **Siguiente**.

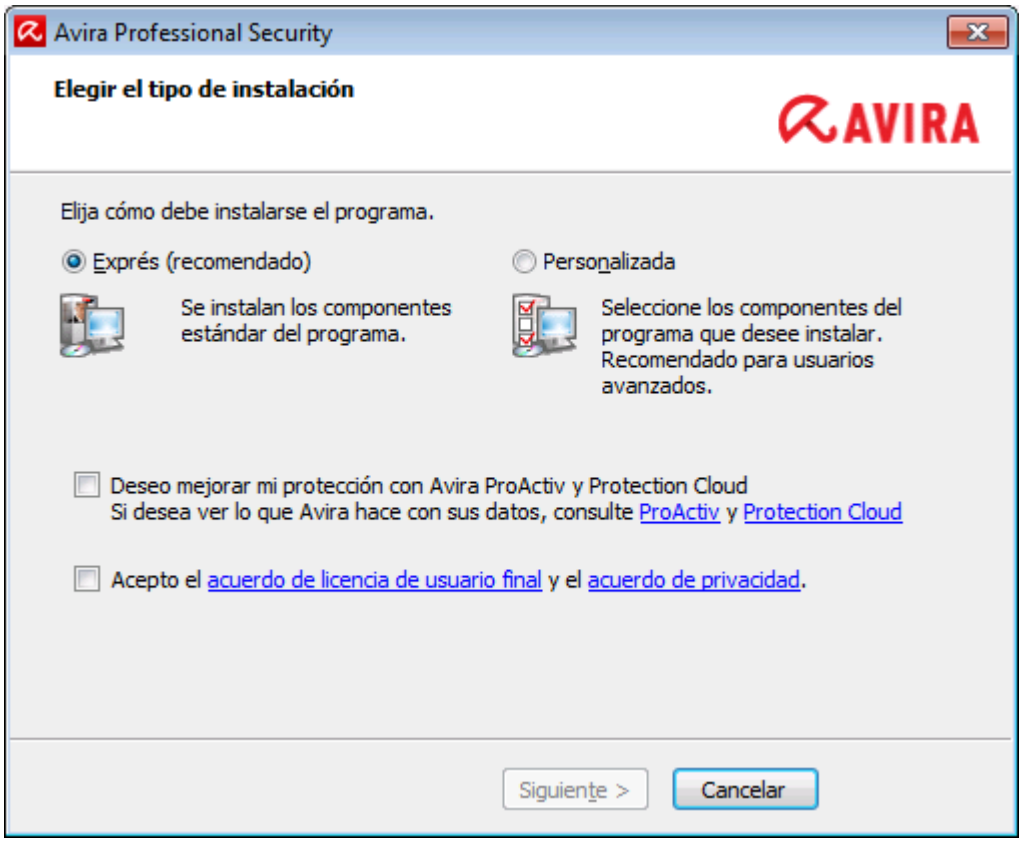
  En el caso de algunos productos, la desinstalación se ha de confirmar manualmente.

  Seleccione los programas y haga clic en **Siguiente**.

  La desinstalación de uno o varios programas puede precisar un reinicio del equipo. Tras el reinicio, comenzará el proceso de desinstalación.

3.6 Selección del tipo de instalación

Durante la instalación, puede seleccionar un tipo de instalación en el asistente de instalación. El asistente de instalación está diseñado para guiarle detalladamente por el proceso de instalación.



Temas relacionados:

- consulte Realizar una instalación exprés
- consulte Realizar una instalación personalizada

3.6.1 Realizar una instalación exprés

La *instalación exprés* es la rutina de instalación recomendada.

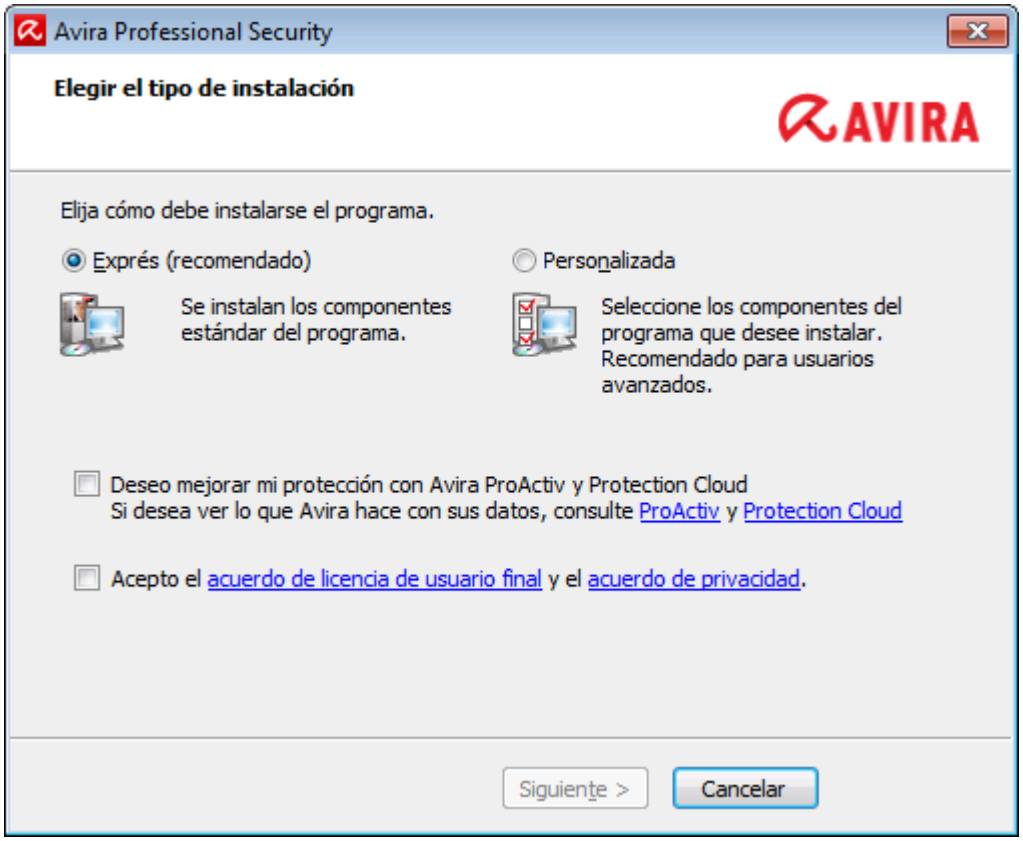
- Instala todos los componentes estándar de Avira Professional Security. Se utiliza la configuración de seguridad recomendada de Avira.
- De forma predeterminada, se elige una de las siguientes rutas de instalación:
  - *C:\Archivos de programa\Avira* (en las versiones de Windows de 32 bits) o
  - *C:\Archivos de programa (x86)\Avira* (en las versiones de Windows de 64 bits)
- En esta ruta puede encontrar todos los archivos relacionados con Avira Professional Security.
- Si elige este tipo de instalación, puede realizar la instalación con solo hacer clic en **Siguiente** hasta que finalice el proceso.
- Este tipo de instalación está diseñado especialmente para aquellos usuarios que no se sienten seguros a la hora de configurar herramientas de software.

3.6.2 Realizar una instalación personalizada

La *instalación personalizada* le permite configurar la instalación. Se recomienda únicamente a los usuarios avanzados con altos conocimientos en lo relativo al hardware, al software y a los problemas de seguridad.

- Puede optar por instalar componentes aislados del programa.
- Puede seleccionar una carpeta de destino para ubicar los archivos de programa que se instalarán.
- Puede establecer si debe crearse un acceso directo en el escritorio o un grupo de programas en el menú **Inicio**.
- Mediante el asistente de configuración, puede definir una configuración personalizada de Avira Professional Security. Además, puede elegir el nivel de seguridad con el que se sienta cómodo.
- Tras la instalación, puede iniciar un análisis rápido del sistema que se realiza de forma automática.

3.7 Instalación de Avira Professional Security



- Si no desea participar en la comunidad de Avira, anule la selección de la casilla de verificación **Deseo mejorar mi protección utilizando Avira ProActiv y Protection Cloud**, la cual aparece seleccionada de forma predeterminada.

Si confirma su participación en la comunidad de Avira, Avira Professional Security enviará datos acerca de los programas sospechosos a Avira Malware Research Center. Los datos solamente se utilizan para un análisis en línea avanzado y para ampliar y mejorar la tecnología de detección.

Puede hacer clic en los vínculos **ProActiv** y **Protection Cloud** para obtener más información sobre el análisis ampliado en línea y el análisis en la nube.

Confirme que acepta el **Acuerdo de licencia del usuario final**. Para leer el texto detallado del **Acuerdo de licencia del usuario final**, haga clic en el vínculo.

3.7.1 Elección de una carpeta de destino

La instalación personalizada le permite elegir la carpeta en la que instalar Avira Professional Security.

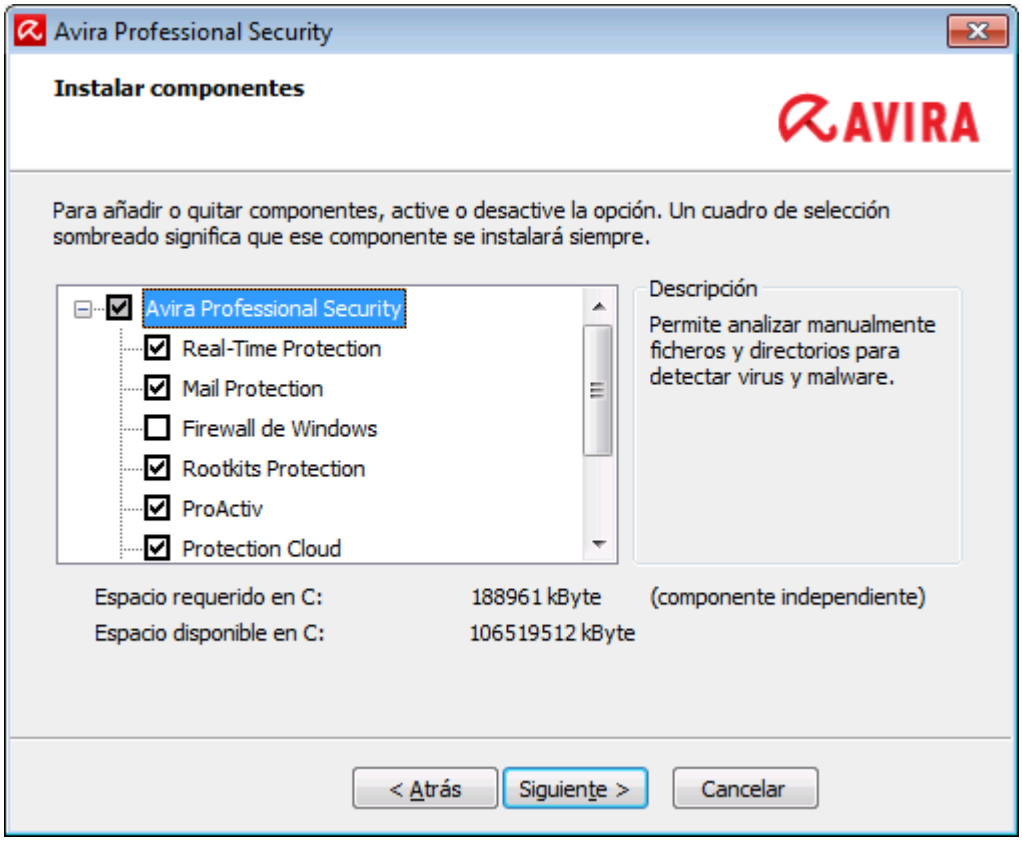
- Haga clic en **Examinar** y vaya hasta la ubicación en la que desee instalar Avira Professional Security.

  Seleccione la carpeta en la que desea instalar Avira Professional Security en la ventana **Seleccionar directorio de destino**.

  Haga clic en **Siguiente**.

3.7.2 Elección de los componentes de la instalación

En caso de realizar una instalación personalizada o cambios en la instalación, puede seleccionar los siguientes componentes para añadirlos a la instalación o bien para quitarlos de ella.



Seleccione o anule la selección de los componentes en la lista del cuadro de diálogo de instalación.

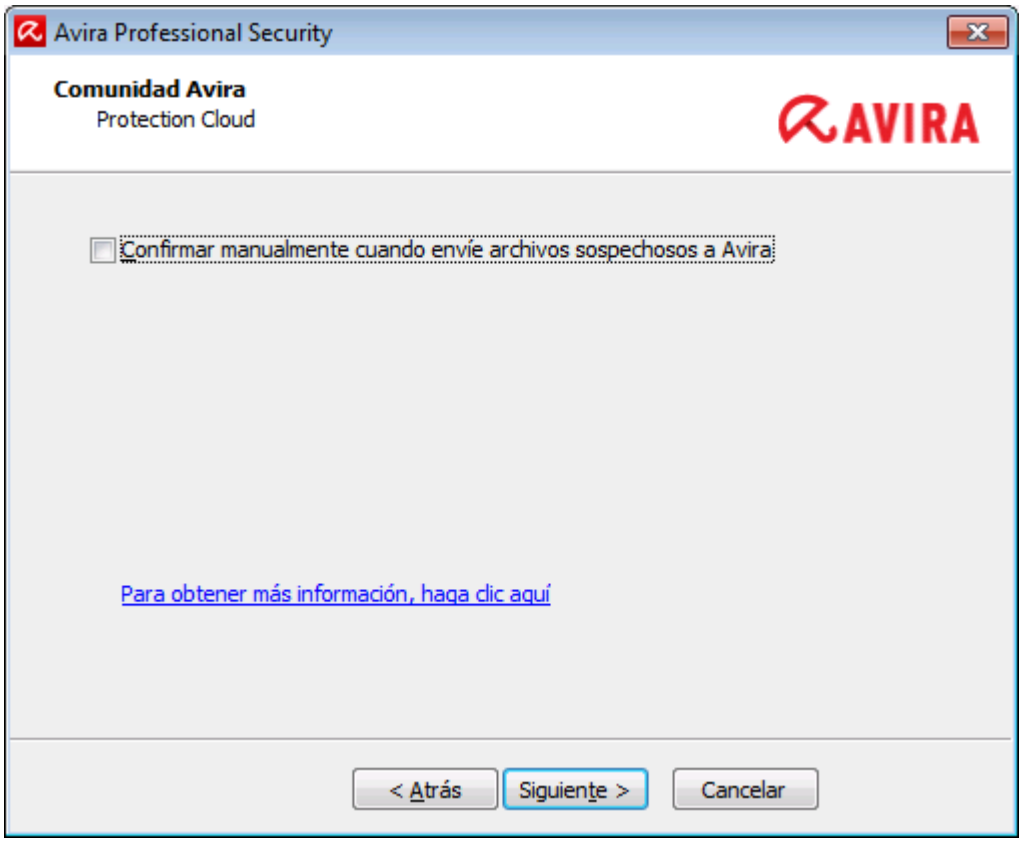
- **Avira Professional Security**
  Este contiene todos los componentes necesarios para la instalación correcta de Avira Professional Security.
  - **Real-Time Protection**
    Avira Real-Time Protection se ejecuta en segundo plano. Supervisa y repara, si fuera posible, los archivos en operaciones como abrir, escribir y copiar en tiempo real (en acceso). En tiempo real significa que, si un usuario realiza una operación con un archivo (p. ej., cargar, ejecutar, copiar el archivo), Avira Professional Security analiza automáticamente el archivo. Al cambiar el nombre de un archivo, no obstante, no se activa el análisis por parte de Avira Real-Time Protection.
  - **Mail Protection**
    Mail Protection es la interfaz entre su equipo y el servidor de correo electrónico del cual su programa de correo (cliente de correo) descarga los correos electrónicos. Mail Protection se conecta como proxy entre el programa de correo y el servidor de correo. Todos los correos electrónicos entrantes se dirigen a través de este proxy, que analiza la existencia de virus o programas no deseados en los correos

electrónicos y los entrega al programa de correo. Según la configuración, el programa trata los correos electrónicos infectados automáticamente o pregunta al usuario antes de realizar una determinada acción.

- **Avira FireWall** (hasta Windows XP)
  Avira FireWall controla las vías de comunicación de su ordenador. Permite o deniega la comunicación basándose en directrices de seguridad.
- **Firewall de Windows** (a partir de Windows 7)
  Este componente administra el Firewall de Windows desde Avira Professional Security.
- **Rookits Protection**
  Avira Rookits Protection comprueba si existe software instalado en su equipo que no se pueda detectar con los métodos convencionales de protección contra software malicioso una vez que ha entrado en el sistema del equipo.
- **ProActiv**
  El componente ProActiv supervisa las acciones de las aplicaciones y alerta a los usuarios del comportamiento sospechoso de las aplicaciones. Mediante este reconocimiento basado en el comportamiento podrá protegerse ante software malicioso desconocido. El componente ProActiv está integrado en Avira Real-Time Protection.
- **Protection Cloud**
  El componente Protection Cloud es un módulo para la detección dinámica en línea de software malicioso aún desconocido. Esto quiere decir que los archivos se cargan en una ubicación remota y se comparan con archivos conocidos y con otros archivos que se cargan y analizan en tiempo real (sin programación ni retardo). De este modo, la base de datos se actualiza constantemente y, por ende, se proporciona un nivel de seguridad incluso mayor.
  Si ha seleccionado el componente Protection Cloud en la instalación y, aun así, desea confirmar de manera manual qué datos deben cargarse al análisis de Cloud, active la opción **Confirmar de manera manual si se envían a Avira ficheros sospechosos**.
- **Web Protection**
  Mientras se navega por Internet, el explorador web solicita datos a un servidor web. Los datos transferidos por el servidor web (archivos HTML, archivos de secuencia de comandos y de imagen, archivos Flash, secuencias de audio y de vídeo, etc.) pasan por regla general a la memoria caché del navegador directamente para su ejecución en el navegador web, de modo que el análisis en tiempo real que ofrece Avira Real-Time Protection no es posible. Esta es una vía de acceso de virus y programas no deseados a su sistema informático. Web Protection es lo que se denomina un proxy HTTP, que supervisa los puertos utilizados para la transferencia de datos (80, 8080, 3128) y analiza los datos transferidos para detectar la existencia de virus y programas no deseados. Según la configuración, el programa trata los archivos infectados automáticamente o pregunta al usuario antes de realizar una determinada acción.
- **Extensión de shell**
  La Extensión de shell genera una entrada **Analizar ficheros seleccionados con Avira** en el menú contextual del Explorador de Windows (botón derecho del ratón). Esta entrada permite analizar directamente determinados archivos o directorios.

Temas relacionados:
Modificación de la instalación

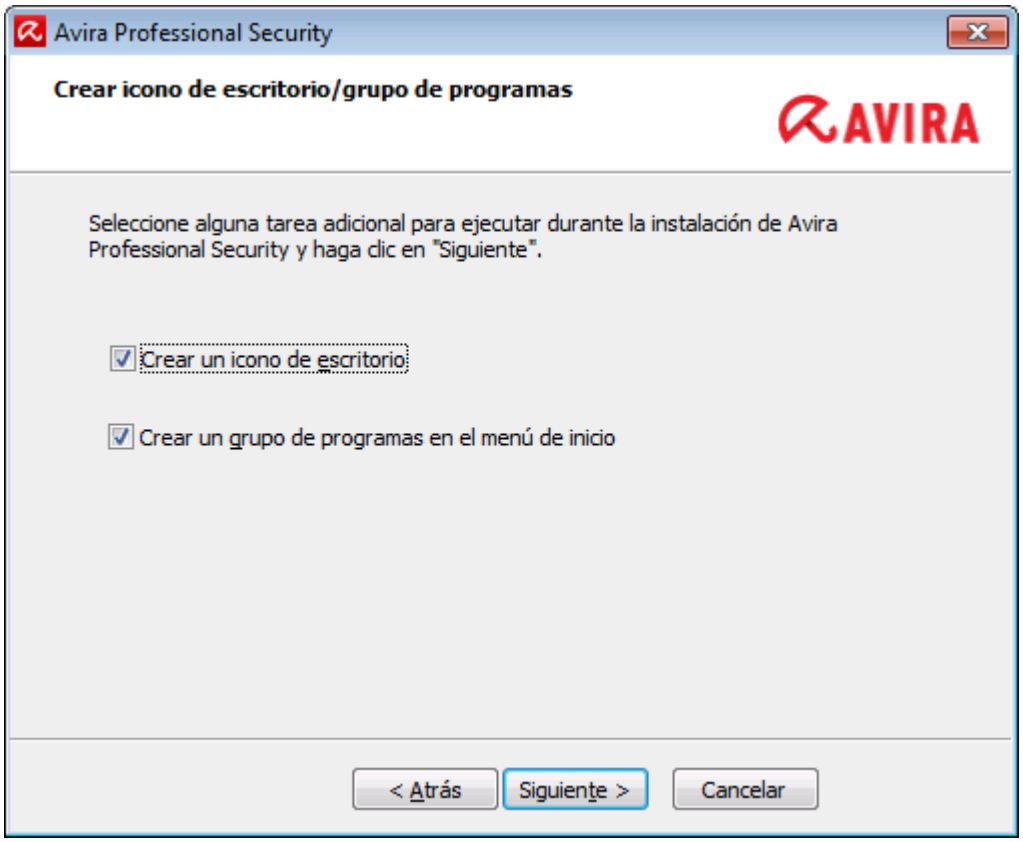
Si decide participar en la Comunidad Avira, puede elegir confirmar manualmente cada vez que un archivo es enviado a Avira Malware Research Center.



- Para que Avira Professional Security le pida su confirmación cada vez, active la opción **Confirmar manualmente cuando envíe archivos sospechosos a Avira**.

3.7.3 Creación de accesos directos para Avira Professional Security

Un acceso directo de escritorio y un grupo de programas en el menú Inicio hacen el acceso a Avira Professional Security más rápido y sencillo.



- Para crear un acceso directo a Avira Professional Security en el escritorio o un grupo de programas en el **menú Inicio**, deje la opción correspondiente activada.

3.7.4 Activación de Avira Professional Security

Existen varias formas de activar Avira Professional Security.

Si ya ha recibido un código de activación, introdúzcalo en los campos correspondientes.

- Si necesita adquirir un código de activación, haga clic en el enlace correspondiente.

  Se le dirigirá al sitio web de Avira, donde podrá adquirir un código de activación.

- Si solo desea probar el producto, seleccione **Producto de prueba** e introduzca sus datos en los campos de registro obligatorios.

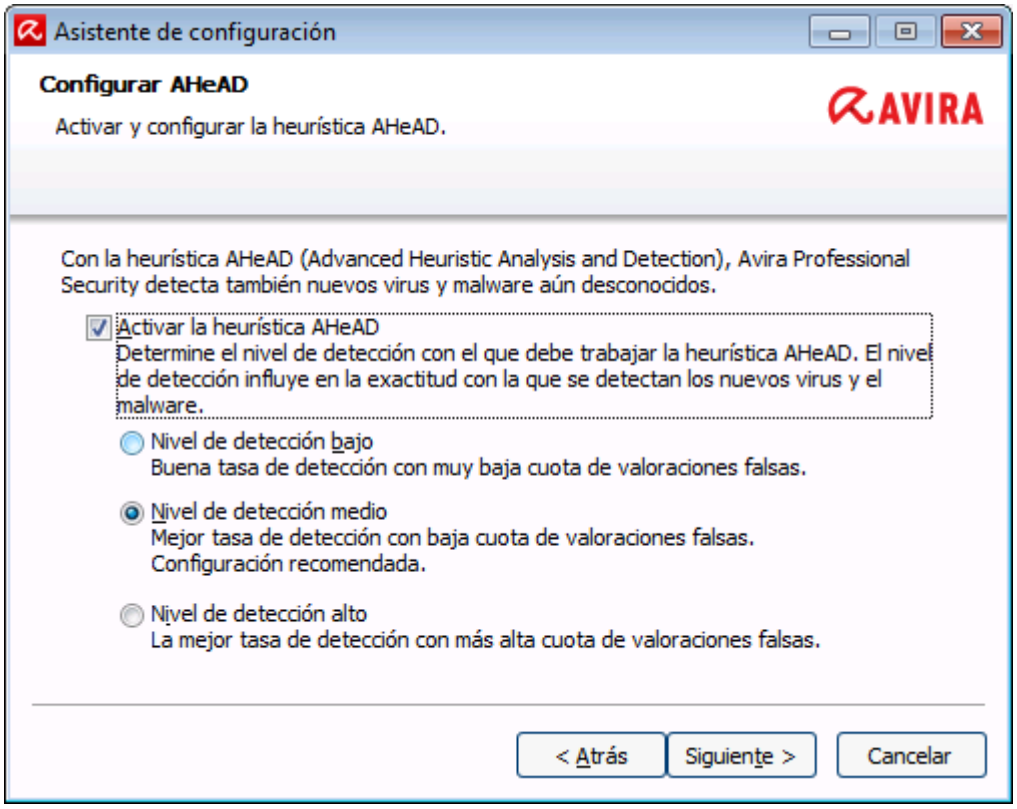
  La licencia de evaluación es válida durante 31 días.

- Si ya ha activado un producto y desea volver a instalar Avira, seleccione la opción **Ya tengo un fichero de licencia**.

  Se abre una ventana de navegación en la que puede buscar el archivo *hbedv.key* en el sistema.

3.7.5 Configuración del nivel de detección heurística (AHeAD)

Avira Professional Security contiene una eficaz herramienta con la tecnología de Avira AHeAD (*Detección y análisis heurísticos avanzados*). Esta tecnología utiliza técnicas de reconocimiento de patrones, por lo que es capaz de detectar software malicioso desconocido (nuevo) cuando ha analizado otro software malicioso anteriormente.

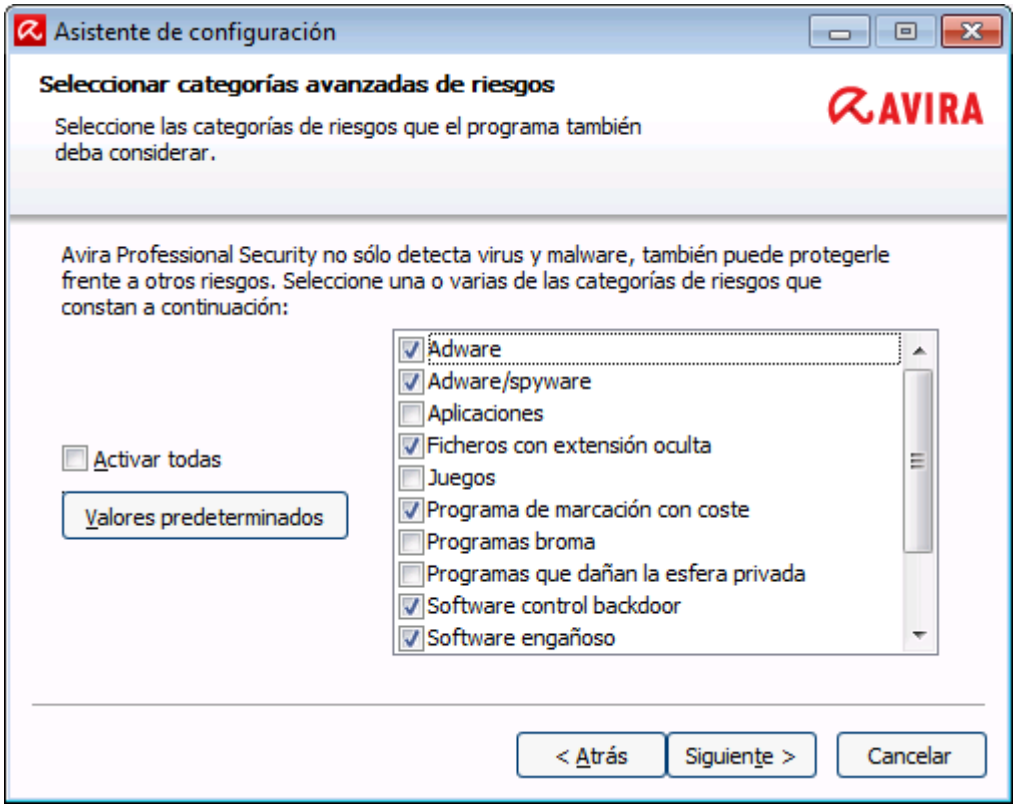


- Seleccione un nivel de detección en el cuadro de diálogo **Configurar AHeAD** y haga clic en **Siguiente**.

  El nivel de detección seleccionado se aplica a la configuración de la tecnología AHeAD de System Scanner (análisis directo) y Real-Time Protection (análisis en tiempo real).

3.7.6 Selección de categorías de riesgos avanzadas

Los virus y el software malicioso no son las únicas amenazas que suponen un peligro para el sistema del equipo. Hemos definido una lista completa de riesgos y los hemos organizado en categorías de riesgos avanzadas para nuestros usuarios.



- Varias categorías de riesgos están seleccionadas de manera predeterminada.

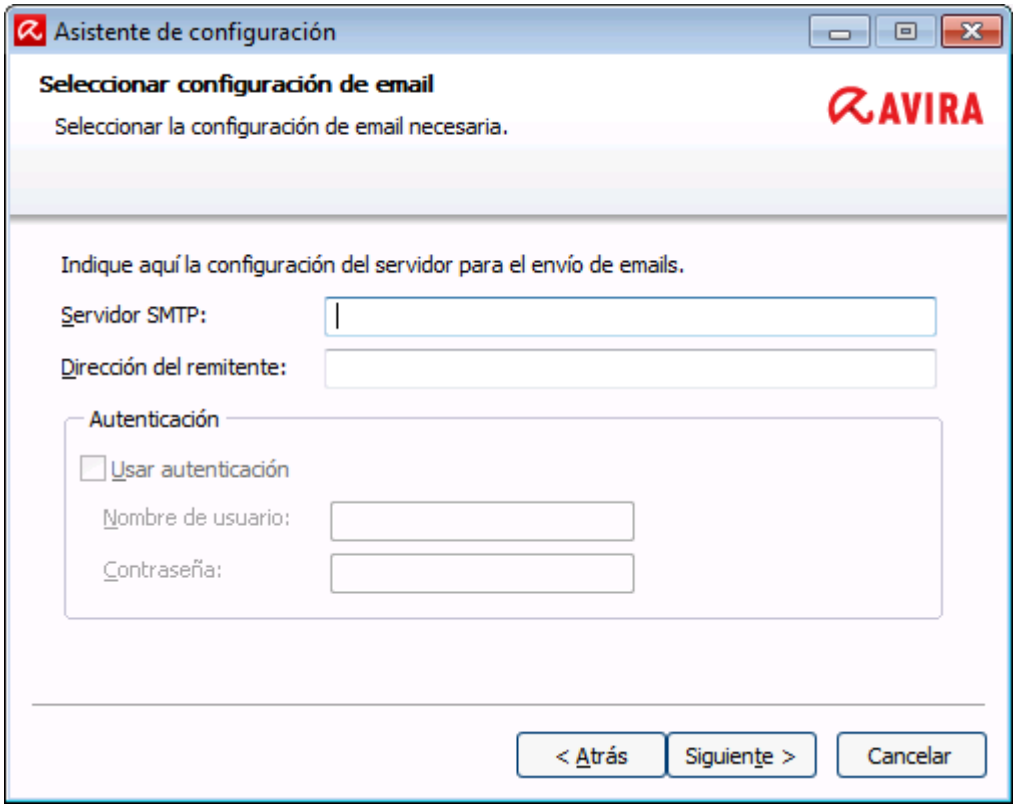
  Si es necesario, active más categorías de riesgos en el cuadro de diálogo **Seleccionar categorías de riesgos avanzadas**.

  Si cambia de idea, puede volver a seleccionar los valores recomendados haciendo clic en el botón **Valores predeterminados**.

  Para continuar con la instalación, haga clic en **Siguiente**.

3.7.7 Selección de la configuración de correo electrónico

Avira Professional Security utiliza SMTP para enviar correos electrónicos, reenviar objetos sospechosos desde la Cuarentena a Avira Malware Research Center, así como enviar alertas por correo electrónico.



- Si desea poder enviar estos correos electrónicos automáticos a través de SMTP, establezca el envío de correos electrónicos en la configuración del servidor dentro del cuadro de diálogo **Seleccionar configuración de correo electrónico**.

Servidor SMTP

Introduzca el nombre del equipo o la dirección IP del servidor SMTP que desea usar.

Ejemplos:

Dirección: smtp.empresa.com

Dirección: 192.168.1.100

Dirección del remitente

Introduzca la dirección de correo electrónico del remitente.

Autenticación

Algunos servidores de correo electrónico esperan que un programa se autentique (inicie sesión) en el servidor antes de enviar un correo electrónico. Las advertencias por correo electrónico se pueden transmitir con la autenticación en un servidor SMTP.

Usar autenticación

Si esta opción está activada, es posible introducir un nombre de usuario y una contraseña en los campos correspondientes para el inicio de sesión (autenticación).

Nombre de inicio de sesión:

Introduzca su nombre de usuario aquí.

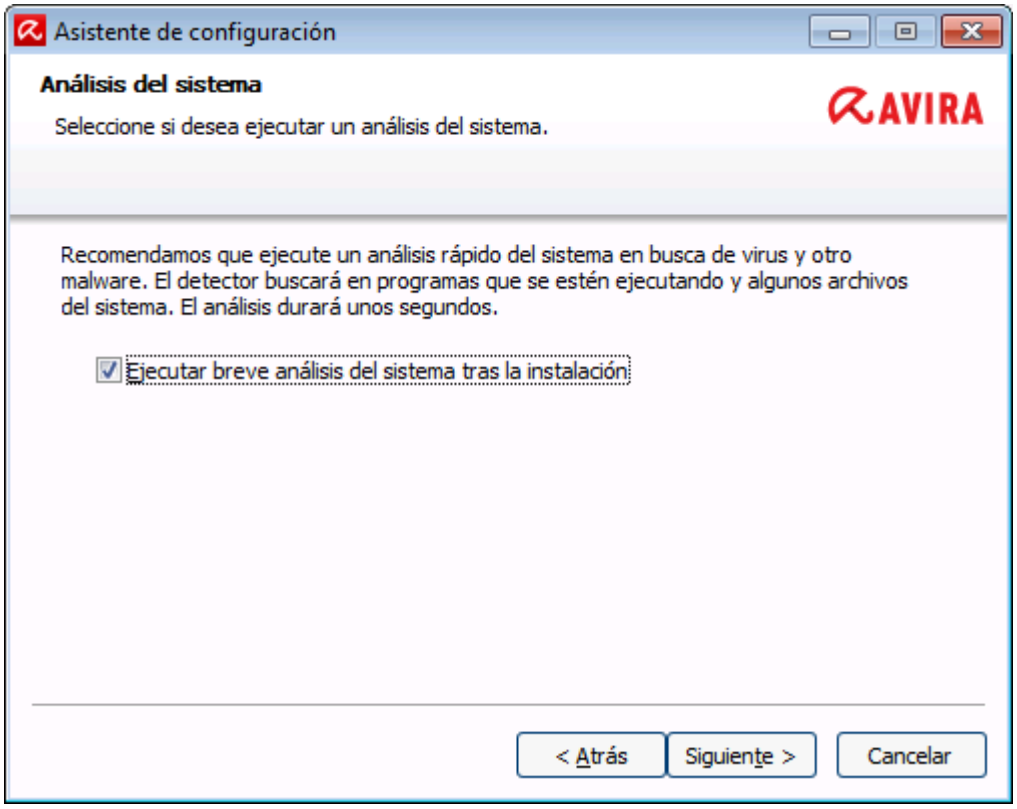
Contraseña:

Introduzca aquí la contraseña correspondiente. Esta contraseña se guarda cifrada. Como medida de seguridad, los caracteres que introduce en este campo se sustituyen por asteriscos (*).

Haga clic en **Siguiente**.

3.7.8 Iniciar un análisis tras la instalación

Para comprobar el estado de seguridad actual del equipo, se puede realizar un análisis rápido del sistema una vez finalizada la configuración y antes de reiniciar el equipo. System Scanner analiza los programas en ejecución y los archivos de sistema más importantes en busca de virus y software malicioso.



- Si desea realizar un análisis rápido del sistema, deje la opción **Análisis rápido del sistema** activada.

  Haga clic en **Siguiente**.

  Para terminar la configuración, haga clic en **Finalizar**.

  Si no ha desactivado la opción **Análisis rápido del sistema**, se abre la ventana *Luke Filewalker*.

  System Scanner realiza un análisis rápido del sistema.

3.7.9 Instalación en la red

Para facilitar al administrador del sistema la instalación de productos Avira en una red con varios equipos cliente, su producto Avira ofrece un procedimiento especial para la primera instalación y los cambios en la instalación.

Para la instalación automática, el programa de instalación utiliza el fichero de control *setup.inf*. El programa de instalación (*presetup.exe*) está incluido en el paquete de instalación del programa. La instalación se inicia con un script o un fichero por lotes y contiene toda la información necesaria del fichero de control. Los comandos del script sustituyen las habituales entradas manuales que se hacen durante la instalación.

Nota
Tenga en cuenta que para la primera instalación en la red es imprescindible un fichero de licencia.

Nota
Tenga en cuenta que para la instalación a través de la red necesitará un paquete de instalación para el producto Avira. No se puede usar un fichero de instalación para la instalación basada en Internet.

Con un script de inicio de sesión del servidor o mediante SMS se pueden distribuir cómodamente productos Avira en la red.

Aquí encontrará información sobre la instalación y desinstalación en la red:

- consulte el capítulo: Parámetros de línea de comandos para el programa de instalación
- consulte el capítulo: Parámetro del fichero *setup.inf*
- consulte el capítulo: Instalación en la red
- consulte el capítulo: Desinstalación en la red

Nota
Otra posibilidad cómoda de instalar y desinstalar productos Avira en la red la ofrece Avira Management Console (AMC). Esta consola sirve para la instalación y el mantenimiento remotos de productos Avira en la red. Encontrará más información en nuestro sitio web http://www.avira.es

Instalación en la red

La instalación puede ejecutarse controlada por el script en el modo por lotes.

Esta configuración es adecuada para las siguientes instalaciones:

- Primera instalación a través de la red (instalación desatendida)
- Instalación de equipos independientes
  - Cambios en la instalación o actualización

> **Nota**
> Recomendamos probar la instalación automática antes de ejecutar la rutina de instalación en la red.
>
> **Nota**
> Si la instalación se lleva a cabo en un sistema operativo servidor, Real-Time Protection y la protección de ficheros no están disponibles.

A continuación, le mostramos cómo instalar automáticamente los productos Avira en la red:

✓ Dispone de derechos de administrador (también es necesario en el modo por lotes)

- Configure los parámetros del fichero *setup.inf* y guarde el fichero.
- Inicie la instalación con el parámetro `/inf` o bien integre el parámetro en el script de inicio de sesión del servidor.

  Ejemplo: `presetup.exe /inf="c:\temp\setup.inf"`

  ↪ La instalación transcurre automáticamente.

Parámetros de línea de comandos para el programa de instalación

> **Nota**
> Los parámetros que contengan rutas o nombres de ficheros deben marcarse con comillas (Ejemplo: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

Para la instalación, puede usar el siguiente parámetro:

- `/inf`

  El programa de instalación se inicia con el script indicado y toma de él todos los parámetros necesarios.
  Ejemplo: `presetup.exe /inf="c:\temp\setup.inf"`

Para la desinstalación, puede usar los siguientes parámetros:

- `/remove`

  El programa de instalación desinstalará el producto Avira.
  Ejemplo: `presetup.exe /remove`

- `/remsilent`

  El programa de instalación desinstalará el producto Avira sin mostrar ningún cuadro de diálogo. El equipo se reinicia después de la desinstalación.
  Ejemplo: `presetup.exe /remsilent`

- `/remsilentaskreboot`

  El programa de instalación desinstalará el producto Avira sin mostrar ningún cuadro de diálogo y, después de la desinstalación, pregunta si debe reiniciarse el equipo.
  Ejemplo: `presetup.exe /remsilentaskreboot`

Para el registro de la desinstalación, dispone además del siguiente parámetro opcional:

- `/unsetuplog`

  Se registran todas las acciones durante la desinstalación.
  Ejemplo: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

Parámetros del fichero *setup.inf*

Para la instalación automática del producto Avira, en el fichero de control *setup.inf* puede establecer los siguientes parámetros en el área [DATA]. El orden de los parámetros no tiene importancia. Si un parámetro falta o se ha establecido erróneamente, la rutina de instalación se cancela con un mensaje de error.

> **Nota**
> Los parámetros que contengan rutas o nombres de ficheros deben marcarse con comillas (Ejemplo: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

- `DestinationPath`

  Ruta de destino en la que se instalará el programa. Debe indicarse en el script. Tenga en cuenta que el programa de instalación añade al final automáticamente nombres de empresa y de producto. Pueden utilizarse variables de entorno.
  Ejemplo: `DestinationPath=%PROGRAMFILES%`
  , que da como resultado la ruta de instalación *C:\Archivos de programa\Avira\AntiVir Server*

- `ProgramGroup`

  Crea un grupo de programas para todos los usuarios del equipo en el menú Inicio de Windows.
  `1`: Crear grupo de programas
  `0`: No crear grupo de programas
  Ejemplo: `ProgramGroup=1`

- `DesktopIcon`

  Crea un icono de acceso directo para todos los usuarios del equipo en el escritorio.
  `1`: Crear icono de escritorio

0: No crear icono de escritorio
Ejemplo: DesktopIcon=1

- ShellExtension

  Registra la extensión del shell en el registro. La extensión del shell permite analizar ficheros o directorios con el menú contextual del botón derecho del ratón para detectar la existencia de virus y malware.
  1: Registrar extensión del shell
  0: No registrar extensión del shell
  Ejemplo: ShellExtension=1

- Guard

  Instala Avira Real-Time Protection (escáner en acceso).
  1: Instalar Avira Real-Time Protection
  0: No instalar Avira Real-Time Protection
  Ejemplo: Guard=1

- MailScanner

  Instala Avira Mail Protection.
  1: Instalar Avira Mail Protection
  0: No instalar Avira Mail Protection
  Ejemplo: MailScanner=1

- KeyFile

  Indica la ruta del fichero de licencia que se copia durante la instalación. Se trata de un requisito imprescindible en la primera instalación. El nombre de fichero debe indicarse completo. (En instalación diferencial: opcional.)
  Ejemplo: KeyFile=D:\inst\license\hbedv.key

- ShowReadMe

  Muestra el fichero *readme.txt* tras la instalación.
  1: Mostrar fichero
  0: No mostrar fichero
  Ejemplo: ShowReadMe=1

- RestartWindows

  Reinicia el equipo tras la instalación. Esta entrada tiene una prioridad más alta que ShowRestartMessage.
  1: Reiniciar equipo
  0: No reiniciar el equipo
  Ejemplo: RestartWindows=1

- ShowRestartMessage

  Durante la instalación, muestra un mensaje antes de un reinicio automático.
  0: No mostrar información
  1: Mostrar información
  Ejemplo: ShowRestartMessage=1

- SetupMode

No es necesario en la primera instalación. El programa de instalación detecta si se ejecuta una primera instalación. Determina el tipo de instalación. No obstante, cuando ya existe una instalación, con SetupMode debe indicarse si para esa instalación solo se va a ejecutar una actualización o una modificación (nueva configuración) o bien se va a ejecutar una desinstalación.
`Actualización`: ejecuta una actualización de una instalación existente. Se omiten los parámetros de configuración, p. ej. `Guard`.
`Modificar`: ejecuta una modificación (nueva configuración) de una instalación existente. No se copia ningún fichero en la ruta de destino.
`Quitar`: desinstala su producto Avira del sistema.
Ejemplo: `SetupMode=Update`

- `AVWinIni` (opcional)

  Indica la ruta de destino del fichero de configuración que puede copiarse durante la instalación. El nombre de fichero debe indicarse completo.
  Ejemplo: `AVWinIni=d:\inst\config\avwin.ini`

- `Password`

  Esta opción pasa a la rutina de instalación la contraseña establecida para la instalación (así como para realizar cambios en la instalación) y la desinstalación. La rutina de instalación solo comprueba esta entrada si se estableció una contraseña. Si se estableció una contraseña y el parámetro de contraseña falta o se ha establecido erróneamente, la rutina de instalación se cancela.
  Ejemplo: `Password=Password123`

- `WebGuard`

  Instala Avira Web Protection.
  `1`: Instalar Avira Web Protection
  `0`: No instalar Avira Web Protection
  Ejemplo: `WebGuard=1`

- `RootKit`

  Instala el módulo Avira Rootkits Protection. Sin Avira Rootkits Protection, el escáner no puede analizar la existencia de rootkits en el sistema.
  `1`: Instalar Avira Rootkits Protection
  `0`: No instalar Avira Rootkits Protection
  Ejemplo: `RootKit=1`

- `ProActiv`

  Instala el componente Avira ProActiv. Avira ProActiv es una tecnología de reconocimiento basada en el comportamiento con la que se puede reconocer malware todavía desconocido.
  `1`: Instalar ProActiv
  `0`: No instalar ProActiv
  Ejemplo: `ProAvtiv=1`

- `FireWall`

Instala el componente Avira FireWall (hasta Windows 7). Avira FireWall monitoriza y regula el tráfico de datos entrante y saliente de su sistema informático y protege así su equipo contra las amenazas procedentes de Internet o de otros entornos de red.
`1`: Instalar FireWall
`0`: No instalar FireWall
Ejemplo: `FireWall=1`

- `MgtFirewall`

  Instala el componente de administración del FireWall de Windows. A partir de Windows 8, Avira FireWall deja de estar incluido en Avira Professional Security. No obstante, tiene la opción de gestionar Windows FireWall mediante el centro de configuración y control.
  `1`: instalar el componente de administración del FireWall de Windows
  `0`: no instalar el componente de administración del FireWall de Windows
  Ejemplo: `MgtFirewall=1`

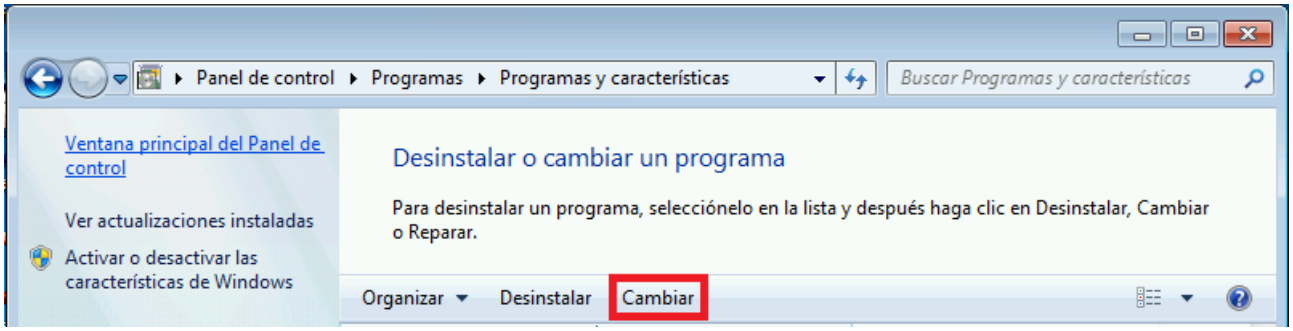
3.8 Modificación de la instalación

Si desea añadir o eliminar módulos de la instalación actual, puede hacerlo sin necesidad de desinstalar Avira Professional Security. Aquí se explica cómo:

- Modificar la instalación en Windows 8
- Modificar la instalación en Windows 7
- Modificar la instalación en Windows XP

3.8.1 Modificar la instalación en Windows 8

Tiene la posibilidad de añadir o eliminar componentes del programa de la instalación actual de Avira Professional Security (consulte Elección de los componentes de la instalación).



Si desea añadir o eliminar módulos de programa de la instalación actual, en el **Panel de control de Windows** puede usar la opción **Desinstalar programas** para **cambiar/desinstalar** programas.

- Haga clic con el botón derecho del ratón en la pantalla.

  Aparecerá el símbolo **Todas las aplicaciones**.

Haga clic en dicho símbolo y busque *Panel de control* en la sección **Aplicaciones - Sistema de Windows**.

Haga doble clic en el símbolo de **Panel de control**.

Haga clic en **Programas - Desinstalar un programa**.

Haga clic en **Programas y características - Desinstalar un programa**.

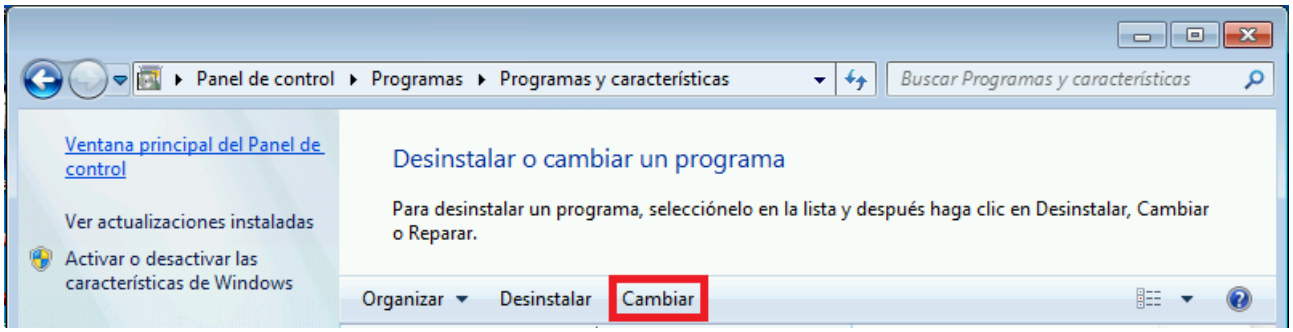
Seleccione Avira Professional Security y haga clic en **Cambiar**.

En el cuadro de diálogo **Bienvenido**, seleccione la opción **Modificar programa**. Se le guiará a través de la modificación de la instalación.

Temas relacionados:
Elección de los componentes de la instalación

3.8.2 Modificar la instalación en Windows 7

Tiene la posibilidad de añadir o eliminar componentes del programa de la instalación actual de Avira Professional Security (consulte Elección de los componentes de la instalación).



Si desea añadir o eliminar componentes de programa de la instalación actual, en el**Panel de control de Windows** puede usar la opción **Añadir o quitar programas** programas.

- En el menú **Iniciar**, abra el **Panel de control**.

  Haga doble clic en **Programas y características**.

  Seleccione Avira Professional Security y haga clic en **Cambiar**.

  En el cuadro de diálogo **Bienvenido**, seleccione la opción **Modificar programa**. Se le guiará a través de la modificación de la instalación.

Temas relacionados:
Elección de los componentes de la instalación

3.8.3 Modificar la instalación en Windows XP

Tiene la posibilidad de añadir o eliminar componentes del programa de la instalación actual de Avira Professional Security (consulte Elección de los módulos de la instalación).

Si desea añadir o eliminar componentes de programa de la instalación actual, en el**Panel de control de Windows** puede usar la opción **Añadir o quitar programas** programas.

- En el menú **Inicio > Configuración**, abra el **Panel de control**.

  Haga doble clic en **Agregar o quitar programas**.

  Seleccione Avira Professional Security y haga clic en **Cambiar**.

  En el cuadro de diálogo **Bienvenido**, seleccione la opción **Modificar programa**. Se le guiará a través de la modificación de la instalación.

Temas relacionados:
Elección de los componentes de la instalación

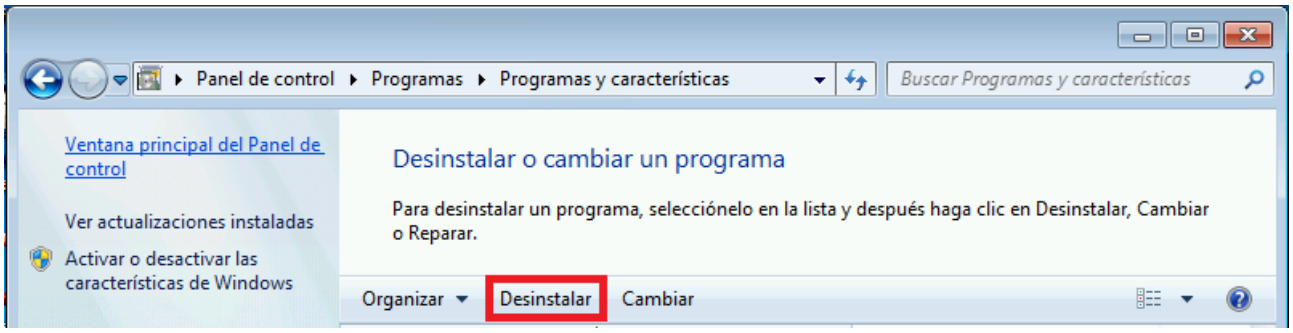
3.9 Desinstalación

Si en algún momento necesita desinstalar Avira Professional Security, siga estos pasos:

- Desinstalación de Avira Professional Security en Windows 8
- Desinstalación de Avira Professional Security en Windows 7
- Desinstalación de Avira Professional Security en Windows XP

3.9.1 Desinstalación de Avira Professional Security en Windows 8

Para desinstalar Avira Professional Security del equipo, utilice la opción **Programas y características** desde el Panel de control de Windows.



- Haga clic con el botón derecho del ratón en la pantalla.

  Aparecerá el símbolo **Todas las aplicaciones**.

  Haga clic en dicho símbolo y busque *Panel de control* en la sección **Aplicaciones - Sistema de Windows**.

  Haga doble clic en el símbolo de **Panel de control**.

  Haga clic en **Programas - Desinstalar un programa**.

  Haga clic en **Programas y características - Desinstalar un programa**.

  Seleccione Avira Professional Security en la lista y haga clic en **Desinstalar**.

Cuando se le pregunte si realmente desea quitar la aplicación y todos sus componentes, haga clic en **Sí** para confirmar.

Cuando se le pregunte si desea activar el Firewall de Windows (se desinstalará Avira FireWall), haga clic en **Sí** para confirmar y mantener al menos alguna protección para el sistema.

Se quitan todos los componentes del programa.

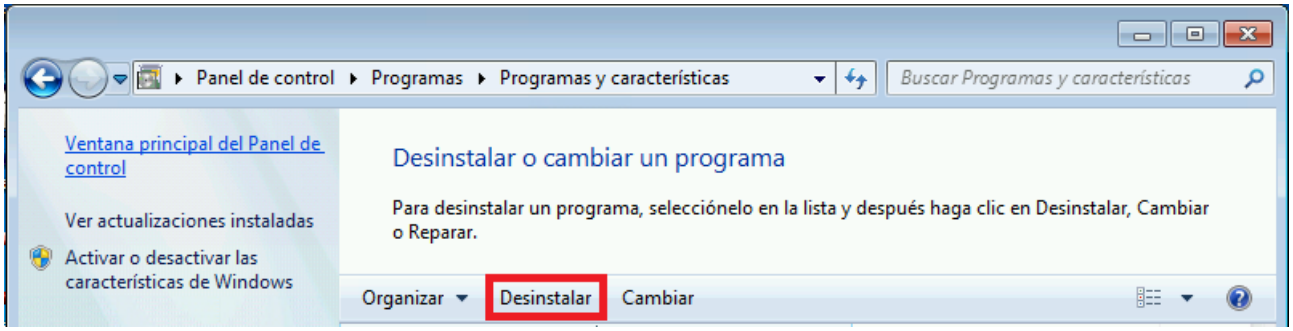
Haga clic en **Finalizar** para concluir con la desinstalación.

Si aparece un cuadro de diálogo recomendando el reinicio del equipo, haga clic en **Sí** para confirmar.

Avira Professional Security se habrá desinstalado y se eliminarán todos los directorios, archivos y entradas de registro del programa al reiniciar el equipo.

3.9.2 Desinstalación de Avira Professional Security en Windows 7

Para desinstalar Avira Professional Security del equipo, utilice la opción **Programas y características** desde el Panel de control de Windows.



- En el menú **Inicio**, abra el **Panel de control**.

  Haga clic en **Programas y características**.

  Seleccione Avira Professional Security en la lista y haga clic en **Desinstalar**.

  Cuando se le pregunte si realmente desea quitar la aplicación y todos sus componentes, haga clic en **Sí** para confirmar.

  Cuando se le pregunte si desea activar el Firewall de Windows (se desinstalará Avira FireWall), haga clic en **Sí** para confirmar y mantener al menos alguna protección para el sistema.

  Se quitan todos los componentes del programa.

  Haga clic en **Finalizar** para concluir con la desinstalación.

  Si aparece un cuadro de diálogo recomendando el reinicio del equipo, haga clic en **Sí** para confirmar.

  Avira Professional Security se habrá desinstalado y se eliminarán todos los directorios, archivos y entradas de registro del programa al reiniciar el equipo.

3.9.3 Desinstalación de Avira Professional Security en Windows XP

Para desinstalar Avira Professional Security del equipo, utilice la opción **Agregar o quitar programas** desde el Panel de control de Windows.

- En el menú **Inicio > Configuración**, abra el **Panel de control**.

  Haga doble clic en **Agregar o quitar programas**.

  Seleccione Avira Professional Security en la lista y haga clic en **Quitar**.

  Cuando se le pregunte si realmente desea quitar la aplicación y todos sus componentes, haga clic en **Sí** para confirmar.

  Se quitan todos los componentes del programa.

  Haga clic en **Finalizar** para concluir con la desinstalación.

  Si aparece un cuadro de diálogo recomendando el reinicio del equipo, haga clic en **Sí** para confirmar.

  Avira Professional Security se habrá desinstalado y se eliminarán todos los directorios, archivos y entradas de registro del programa al reiniciar el equipo.

3.9.4 Desinstalación en la red

A continuación, le mostramos cómo desinstalar los productos Avira en la red:

✓ Dispone de derechos de administrador (también es necesario en el modo por lotes)

- Inicie la desinstalación con el parámetro `/remsilent` o `/remsilentaskreboot`, o bien integre el parámetro en el script de inicio de sesión del servidor.

  Adicionalmente, puede indicar el parámetro para el registro de la desinstalación.

  Ejemplo: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

  ↪ La desinstalación transcurre automáticamente.

Nota
No inicie el programa de instalación para la desinstalación en una unidad de red compartida, sino de forma local en el equipo en el que deba desinstalarse el producto Avira.

4. Acerca de Avira Professional Security

En este capítulo se ofrece un resumen de las funciones y del modo de uso de su producto Avira.

- consulte el capítulo Interfaz de usuario y uso
- consulte el capítulo Procedimientos

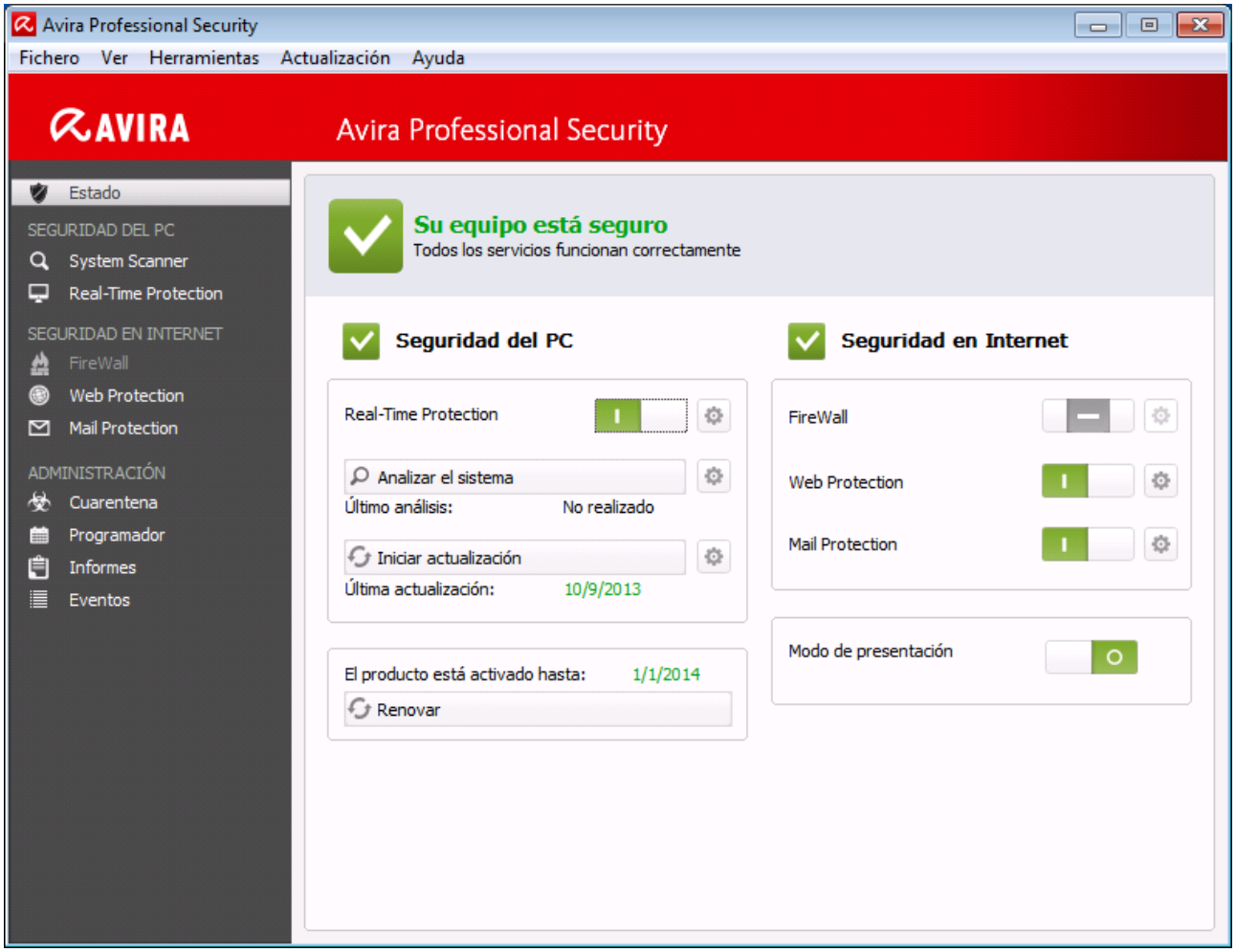
4.1 Interfaz de usuario y uso

Su producto Avira se utiliza por medio de tres elementos de la interfaz del programa:

- Centro de control: Supervisión y control del producto Avira
- Configuración: Configuración del producto Avira
- Icono de bandeja en la bandeja del sistema de la barra de tareas: apertura del Centro de control y otras funciones

4.1.1 Centro de control

El Centro de control sirve para supervisar el estado de protección de su sistema informático y para controlar y operar con los componentes de protección y las funciones de su producto Avira.



La ventana del Centro de control se divide en tres áreas: la **barra de menús**, el **área de exploración** y la ventana de detalles **Estado**:

- **Barra de menús:** en los menús del Centro de control puede activar funciones de programa generales y consultar información sobre el producto.
- **Área de exploración:** en el área de exploración puede cambiar fácilmente entre las diversas secciones del Centro de control. Las secciones contienen información y funciones de los componentes de programa y están dispuestas en la barra de exploración por áreas de actividades. Ejemplo: área de actividades *SEGURIDAD DEL PC*, sección **Real-Time Protection**.
- **Estado:** en la pantalla arranque **Estado** comprueba de un vistazo si su equipo está lo suficientemente protegido y dispone de la información general sobre qué módulos están activos, cuándo se han realizado la última actualización y el último análisis del sistema. En la ventana **Estado** se encuentran los botones para ejecutar funciones o acciones, como por ejemplo la conexión o desconexión de **Real-Time Protection**.

Inicio y finalización del Centro de control

Dispone de las siguientes opciones para iniciar el Centro de control:

- Con un doble clic en el icono del programa de su escritorio

- Por medio de la entrada de programa en el menú **Inicio > Programas**.
- Mediante el icono de bandeja de su producto Avira.

Para cerrar el Centro de control, utilice el comando **Finalizar** del menú **Fichero**, use el comando de teclado **Alt+F4** o haga clic en el aspa de cierre del Centro de control.

Usar el Centro de control

Así se navega por el Centro de control:

- Haga clic en un área de actividades de la barra de exploración, debajo de una sección.
  - ↪ El área de actividades se indica con modos de funcionamiento y opciones de configuración en la ventana de detalles.
- Si lo desea, pulse en otro área de actividades para mostrarla en la ventana de detalles.

> **Nota**
> La exploración usando el teclado de la barra de menús se activa con la tecla [**Alt**]. Con la tecla **Intro** se activa la opción de menú seleccionada en ese momento.
> Para abrir y cerrar los menús en el Centro de control o para explorarlos, también puede usar combinaciones de teclas: tecla [**Alt**] + letra subrayada del menú o comando de menú. Mantenga pulsada la tecla [**Alt**] si desea abrir un comando de menú de un menú o un submenú.

Para editar los datos u objetos que se muestran en la ventana de detalles:

- Seleccione los datos u objetos que va a editar.

  Para seleccionar varios elementos, mantenga pulsada la tecla **Ctrl** o la tecla **Mayús** (selección de elementos consecutivos) mientras selecciona los elementos.
- Pulse el botón que desee en la barra superior de la ventana de detalles para editar el objeto.

Descripción general del Centro de control

- **Estado**: en la pantalla de arranque **Estado** encontrará todas las secciones con las que puede supervisar la funcionalidad del producto Avira (consulte Estado).
  - La ventana **Estado** ofrece la posibilidad de ver de un solo vistazo qué módulos están activos y aporta información sobre la última actualización realizada.
- *SEGURIDAD DEL PC*: Aquí encontrará los componentes con los que se analizan los ficheros del sistema informático para detectar la existencia de virus o software malintencionado (malware).
  - La sección **Scanner** permite configurar o iniciar de forma sencilla el análisis directo (consulte Scanner). Los perfiles predefinidos permiten llevar a cabo un análisis con

opciones predeterminadas ya adaptadas. Del mismo modo, con ayuda de la selección manual (que se guarda) o con la creación de perfiles definidos por el usuario, es posible adaptar el análisis de detección de virus y programas no deseados a sus propias necesidades.

- La sección Real-Time Protection muestra información sobre los ficheros comprobados, así como datos estadísticos que pueden restablecerse en cualquier momento, y permite abrir el fichero de informe. Prácticamente con solo pulsar un botón, puede obtener información detallada sobre el último virus o programa no deseado que se haya detectado.

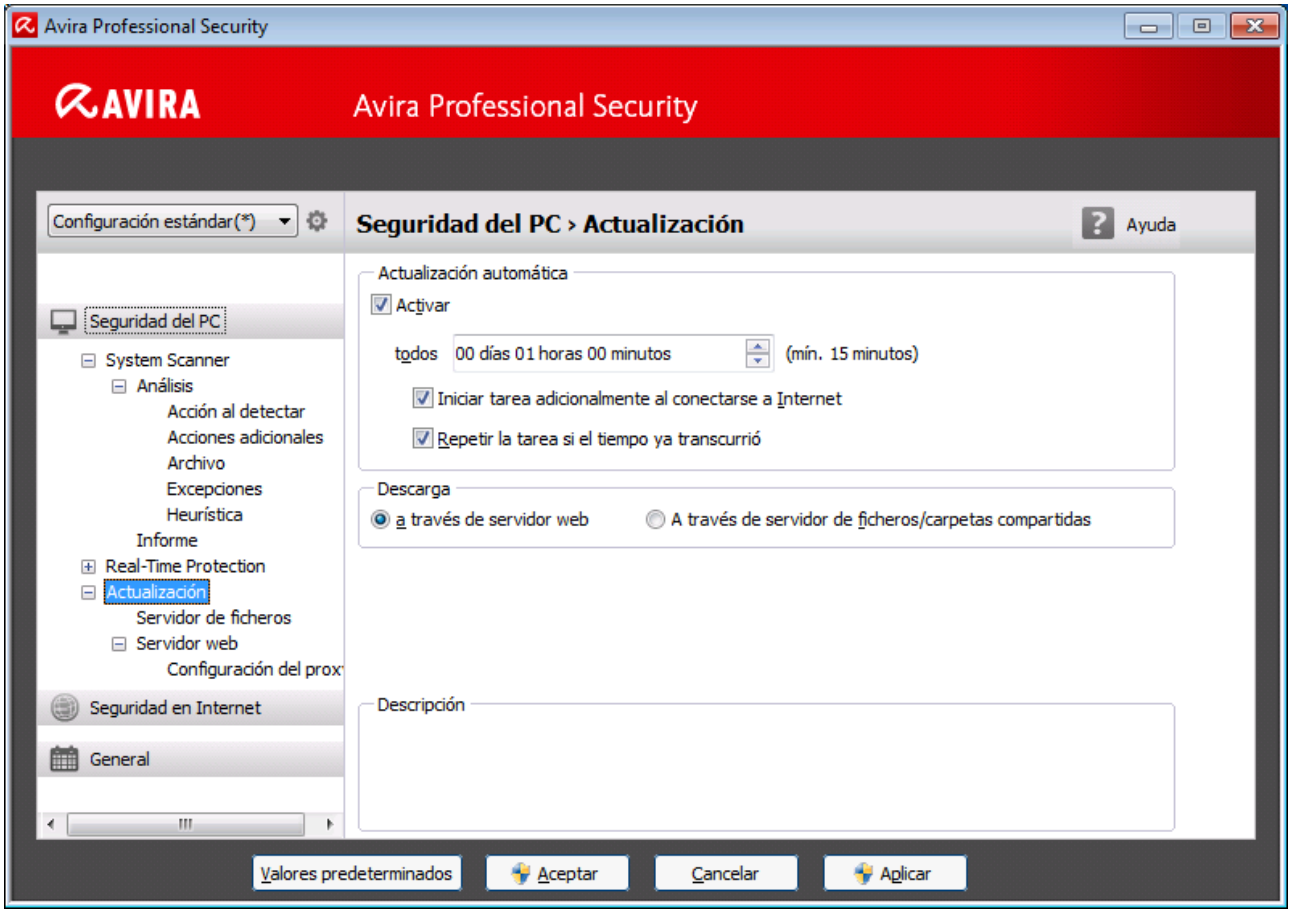
- *SEGURIDAD EN INTERNET*: Aquí encontrará encontrará los componentes con los que se protege el sistema informático frente a virus y malware de Internet, así como frente a los accesos no deseados a la red.
  - La sección **FireWall** le ofrece la posibilidad de establecer la configuración básica del Firewall. Además, se muestran la velocidad de transmisión de datos actual y todas las aplicaciones activas que utilizan una conexión de red (consulte FireWall).
  - La sección Web Protection muestra la información relativa a las direcciones URL comprobadas y a los virus detectados, así como datos estadísticos que pueden restablecerse en cualquier momento, y permite abrir el fichero de informe. Prácticamente con solo pulsar un botón, puede obtener información detallada sobre el último virus o programa no deseado que se haya detectado.
  - La sección **Mail Protection** muestra los correos electrónicos analizados, sus propiedades y otros datos estadísticos. Además, tiene la posibilidad de excluir direcciones de correo electrónico debe excluir en el futuro del análisis de spam y malware. También puede eliminar los emails de la memoria caché de Mail Protection. (consulte Mail Protection).

- *ADMINISTRACIÓN*: Aquí encontrará las herramientas con las que puede aislar y administrar ficheros sospechosos o infectados por virus, así como programar tareas periódicas.
  - En la sección **Cuarentena** se encuentra el denominado Gestor de cuarentena. Es el elemento central para ficheros ya puestos en cuarentena o para ficheros sospechosos que se quieren poner en cuarentena (consulte Cuarentena). Además, existe la posibilidad de enviar un determinado fichero por correo electrónico al Avira Malware Research Center.
  - La sección **Programador** permite crear tareas de análisis y actualización, así como tareas de backup programadas, y adaptar o eliminar tareas existentes (consulte Programador).
  - La sección **Informes** ofrece la posibilidad de consultar los resultados de las acciones realizadas (consulte Informes).
  - La sección **Eventos** ofrece la posibilidad de informarse sobre los eventos que generan los módulos del programa (consulte Eventos).

4.1.2 Configuración

En la configuración puede establecer los parámetros de su producto Avira. Tras la instalación, su producto Avira está configurado con parámetros predeterminados que

garantizan que el sistema informático esté óptimamente protegido. No obstante, su sistema informático o los requisitos que usted tiene respecto a su producto Avira pueden presentar particularidades, de modo que querrá adaptar los componentes de protección del programa.



La configuración tiene estructura de cuadro de diálogo: con los botones **Aceptar** o **Aplicar** se guardan los parámetros establecidos en la configuración, con **Cancelar** se descartan los parámetros, y con el botón **Valores predeterminados** puede restablecer los parámetros de la configuración en los valores predeterminados. En la barra de exploración de la izquierda, puede seleccionar las distintas secciones de configuración.

Abrir la configuración

Hay varias maneras de activar la configuración:

- A través del Panel de control de Windows.
- Desde el Centro de seguridad de Windows (con Windows XP Service Pack 2 o superior).
- Con el icono de bandeja de su programa Avira.
- En el Centro de control, con la opción de menú Extras > Configuración.
- En el Centro de control, con el botón Configuración.

Nota
Si activa la configuración pulsando el botón **Configuración** en el Centro de control, accederá a la ficha de configuración de la sección que esté activa en el Centro de control.

Usar la configuración

En la ventana de configuración, puede desplazarse como en el Explorador de Windows:

- Pulse en una entrada de la estructura de árbol para mostrar esa sección de configuración en la ventana de detalles.
- Pulse en el signo más (+) delante de una entrada para expandir la sección de configuración y mostrar otras secciones de configuración subordinadas en la estructura de árbol.
- Para ocultar secciones de configuración subordinadas, haga clic en el signo menos (-) situado delante de la sección de configuración expandida.

Nota
Para activar o desactivar opciones en la configuración y pulsar los botones, también puede usar combinaciones de teclas: tecla [**Alt**] + letra subrayada en el nombre de opción o en la denominación del botón.

Si quiere aceptar los parámetros establecidos en la configuración:

- Haga clic en el botón **Aceptar**.
  - ↪ La ventana de configuración se cierra y se aplican los parámetros establecidos.

  - O BIEN -

  Haga clic en el botón **Aplicar**.
  - ↪ Se aplican los parámetros establecidos. La ventana de configuración permanece abierta.

Si quiere finalizar la configuración sin aceptar los parámetros establecidos:

- Haga clic en el botón **Cancelar**.
  - ↪ La ventana de configuración se cierra y se descartan los parámetros establecidos.

Si desea restablecer todos los parámetros de la configuración en sus valores predeterminados:

- Haga clic en **Valores predeterminados**.

↳ Todos los parámetros de la configuración se restablecen con los valores predeterminados. Al restablecer los valores predeterminados, se pierde cualquier cambio efectuado y todas las entradas propias.

Perfiles de configuración

Tiene la posibilidad de guardar los parámetros en la configuración como perfiles de configuración. En el perfil de configuración, es decir, en una configuración, constan todas las opciones de configuración resumidas en un grupo. La configuración se representa en la barra de exploración como un nodo. Puede añadir más configuraciones a la configuración predeterminada. Existe la posibilidad de definir reglas para cambiar a una configuración en concreto:
El cambio de configuración basado en reglas permite acoplar configuraciones al uso de una conexión LAN o de Internet (identificación por medio de la puerta de enlace predeterminada): Puede crear así, por ejemplo, perfiles de configuración para los distintos escenarios de uso de un equipo portátil:

- Uso en la red de la empresa: actualización a través del servidor de la Intranet, Web Protection desactivado
- Uso doméstico: actualización a través de los servidores web predeterminados de Avira, Web Protection activado

Si no se han definido reglas para cambiar a otra configuración, puede cambiarla manualmente en el menú contextual del icono de la bandeja. Con los botones de la barra de exploración o los comandos del menú contextual de las secciones de configuración puede añadir configuraciones, cambiarles el nombre, eliminarlas, copiarlas, restablecerlas y definir reglas para el cambio a una configuración determinada.

Nota
El Control de cuentas de usuarios (UAC) precisa su aprobación para la activación o desactivación de los servicios Real-Time Protection, FireWall, Web Protection, así como Mail Protection en sistemas operativos a partir de Windows Vista.

Información general sobre las opciones de configuración

Dispone de las opciones de configuración siguientes:

- **Scanner**: configuración del análisis directo.
  - Opciones de análisis
  - Acción al detectar
  - Acciones adicionales
  - Opciones al analizar archivos
  - Excepciones del análisis directo
  - Heurística del análisis directo
  - Configuración de la función de informe

- **Real-Time Protection**: configuración del análisis en tiempo real.
  - Opciones de análisis
  - Acción al detectar
  - Acciones adicionales
  - Excepciones del análisis en tiempo real.
  - Heurística del análisis en tiempo real.
  - Configuración de la función de informe
- **Actualización**: Configuración de los ajustes de la actualización
  - Descarga mediante el servidor de ficheros
  - Descarga a través de servidor web
  - Configuración de proxy
- **FireWall**: configuración de FireWall.
  - Configuración de las reglas del adaptador
  - Configuración definida por el usuario de las reglas de aplicación
  - Lista de proveedores de confianza (excepciones durante el acceso a la red de las aplicaciones)
  - Configuración avanzada: tiempo de espera excesivo de las reglas, detener FireWall, notificaciones
  - Configuración de ventanas emergentes (mensajes de advertencia durante el acceso a la red de las aplicaciones)
- **Web Protection**: configuración de Web Protection.
  - Opciones de análisis, activación y desactivación de Web Protection.
  - Acción al detectar
  - Accesos bloqueados: tipos de fichero y tipos MIME no deseados, filtro web para direcciones URL conocidas no deseadas (malware, suplantación de identidad (phishing), etc.).
  - Excepciones del análisis de Web Protection: URL, tipos de fichero y tipos MIME.
  - Heurística de Web Protection
  - Configuración de la función de informe
- **Mail Protection**: configuración de Mail Protection.
  - Opciones de análisis: activación de la supervisión de cuentas POP3, cuentas IMAP, correos electrónicos salientes (SMTP).
  - Acción al detectar
  - Acciones adicionales
  - Heurística del análisis de Mail Protection
  - Función AntiBot: servidores SMTP permitidos, remitentes de correo electrónico permitidos.
  - Excepciones del análisis de Mail Protection
  - Configuración de la memoria caché, vaciar memoria caché
  - Configuración de un pie de página en correos electrónicos enviados

- Configuración de la función de informe

- **General**:
  - Configuración del envío de correos electrónicos mediante SMTP
  - Categorías de riesgos avanzadas para análisis directo y análisis en tiempo real
  - Protección avanzada: activar ProActiv y Protection Cloud
  - Filtro de aplicación: bloquear o permitir aplicaciones.
  - Protección con contraseña para el acceso al Centro de control y a la configuración
  - Seguridad: bloquear funciones de Autorun y el fichero host de Windows, protección del producto
  - WMI: activar compatibilidad con WMI.
  - Configuración del registro de eventos
  - Configuración de las funciones de informe
  - Configuración de los directorios empleados
  - Advertencias:

    Configuración de advertencias de red de los componentes:

    - Scanner
    - Real-Time Protection

    Configuración de advertencias por email de los componentes:

    - Scanner
    - Real-Time Protection
    - Updater
  - Configuración de las advertencias acústicas tras la detección de malware

4.1.3 El icono de bandeja

Tras la instalación, verá el icono de bandeja de su producto Avira en la bandeja del sistema de la barra de tareas:

Icono	Descripción
	Se han activado Real-Time Protection y FireWall
	Se ha desactivado Real-Time Protection o FireWall

El icono de la bandeja muestra el estado de Real-Time Protection y del FireWall.

Por medio del menú contextual del icono de bandeja puede acceder rápidamente a las funciones principales de su producto Avira.

- Para activar el menú contextual, pulse con el botón derecho del ratón en el icono de bandeja.

Entradas en el menú contextual

- **Activar Real-Time Protection**: Activa o desactiva Avira Real-Time Protection.
- **Activar Mail Protection**: Activa o desactiva Avira Mail Protection.
- **Activar Web Protection**: Activa o desactiva Avira Web Protection.
- **FireWall**:
  - **Activar FireWall**: Activa o desactiva Avira FireWall.
  - **Activar Windows Firewall**: Activa o desactiva Windows Firewall (esta función está disponible a partir de Windows 8).
  - **Bloquear todo el tráfico**: Si está activa, bloquea cualquier transferencia de datos excepto aquellas que vayan dirigidas al propio ordenador (Local Host / IP 127.0.0.1).
- **Iniciar Avira Professional Security**: Abre el Centro de control.
- **Configurar Avira Professional Security**: Abre la configuración.
- **Iniciar actualización**: Inicia una actualización.
- **Seleccionar configuración**: Abre un submenú que contiene los perfiles de configuración disponibles. Haga clic en una configuración para activarla. El comando de menú estará desactivado si ya se han definido las reglas para la selección automática de una configuración.
- **Ayuda**: Abre la ayuda en línea.
- **Acerca de Avira Professional Security:** Abre una ventana de diálogo con información relativa a su producto Avira: información de producto, versión y licencias.
- **Avira en Internet**: Abre el portal web de Avira en Internet. Para ello, es imprescindible disponer de un acceso activo a Internet.

4.2 Procedimientos

En el capítulo denominado "Procedimientos" puede obtener información básica sobre la activación de licencias y productos, así como sobre las principales funciones de su producto Avira. Las breves aportaciones seleccionadas sirven para proporcionarle una rápida información general sobre las funcionalidades de su producto Avira. Sin embargo, no sustituyen las explicaciones detalladas de cada uno de los capítulos de la presente ayuda.

4.2.1 Activar licencia

Así se activa la licencia de su producto Avira:

Con el fichero de licencia *.KEY* puede activar la licencia para su producto Avira. Avira le enviará el fichero de licencia por email. Este fichero contiene la licencia para todos los productos que haya pedido.

Si todavía no ha instalado su producto Avira:

- Guarde el fichero de licencia en un directorio local de su equipo.
- Instale su producto Avira.
- Durante la instalación, indique dónde guardó el fichero de licencia.

Si ya ha instalado su producto Avira:

- En el administrador de ficheros o en el email de activación, haga doble clic en el fichero de licencia y siga las instrucciones en pantalla de la administración de licencias que aparece.

  - O BIEN -

  En el Centro de control de su producto Avira seleccione la opción de menú **Ayuda > Cargar fichero de licencia**

> **Nota**
> A partir de Windows Vista aparece el cuadro de diálogo Control de cuentas de usuario. En caso necesario, inicie sesión como administrador. Haga clic en **Continuar**.

- Seleccione el fichero de licencia y haga clic en **Abrir**.
  - ↳ Aparecerá un mensaje.
- Confirme la operación pulsando **Aceptar**.
  - ↳ La licencia ya está activada.
- Si fuera necesario, reinicie el sistema.

4.2.2 Ejecutar actualizaciones automáticas

A continuación, le mostramos cómo crear con el Programador de Avira una tarea para llevar a cabo actualizaciones automáticas de su producto Avira:

- Seleccione en el Centro de control la sección *ADMINISTRACIÓN* **> Programador**.
- Haga clic en el icono  **Crear tarea nueva con el asistente**.
  - ↳ Aparece el cuadro de diálogo **Nombre y descripción de la tarea**.
- Asigne nombre a la tarea y descríbala si fuera el caso.

- Haga clic en **Siguiente**.
  - ↪ Aparece el cuadro de diálogo **Tipo de tarea**.
- Seleccione una **tarea de actualización** de la lista de selección.
- Haga clic en **Siguiente**.
  - ↪ Aparece el cuadro de diálogo **Momento de inicio de la tarea**.
- Escoja el momento en que se ejecutará el análisis:

- **Inmediatamente**
- **Diariamente**
- **Semanalmente**
- **Intervalo**
- **Una vez**
- **Inicio de sesión**

> **Nota**
> Recomendamos llevar a cabo actualizaciones frecuentes y periódicas. El intervalo de actualización recomendado es de: 60 minutos.

- Según lo que seleccione, indique la fecha si fuera necesario.
- Si se diera el caso, seleccione opciones adicionales (disponible según el tipo de tarea):

- **Repetir la tarea si el tiempo ya transcurrió**
  Las tareas del pasado se relanzan si no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.
- **Iniciar tarea adicionalm. al conectarse a Internet (acceso telef. a redes)**
  Además de la frecuencia definida, la tarea se lanza al iniciarse la conexión a Internet.

- Haga clic en **Siguiente**.
  - ↪ Aparece el cuadro de diálogo **Selección del modo de visualización**.
- Seleccione el modo de visualización de la ventana de tareas:

- **Invisible**: ninguna ventana de tarea
- **Minimizado**: solo barra de progreso
- **Maximizado**: toda la ventana de tarea

- Haga clic en **Finalizar**.
  - ↪ La tarea recién creada aparece en la página de inicio de la sección *ADMINISTRACIÓN* **> Programador** como activada (marca de verificación).
- Si es el caso, desactive las tareas que no deban ejecutarse.

Los siguientes iconos permiten continuar con la edición de las tareas:

 Ver las propiedades de una tarea

 Modificar tarea

 Eliminar tarea

 Iniciar tarea

Detener tarea

4.2.3 Iniciar una actualización manualmente

Dispone de varias posibilidades de iniciar manualmente una actualización: En las actualizaciones iniciadas manualmente también se ejecuta siempre una actualización del fichero de firmas de virus y el motor de análisis.

Así se inicia manualmente una actualización de su producto Avira:

- Haga clic con el botón derecho del ratón en el icono de bandeja de Avira en la barra de tareas y seleccione **Iniciar actualización**.

  - O BIEN -

- Seleccione en el Centro de control la sección **Estado** y, a continuación, haga clic en el área **Última actualización** en el enlace **Iniciar actualización**.

  - O BIEN -

  Seleccione en el Centro de control, en el menú **Actualización**, la opción **Iniciar actualización**.

  ↪ Aparece el cuadro de diálogo **Updater**.

Nota
Recomendamos llevar a cabo actualizaciones automáticas periódicamente. El intervalo de actualización recomendado es de: 60 minutos.

Nota
También puede ejecutar la actualización automática directamente en el Centro de seguridad de Windows.

4.2.4 Analizar la existencia de virus y malware con un perfil de análisis

El perfil de análisis es una agrupación de unidades y directorios que deben analizarse.

Dispone de las siguientes maneras de analizar mediante un perfil de análisis:

Usar perfil de análisis predefinido

Cuando los perfiles de análisis predefinidos satisfacen sus necesidades.

Adaptar y usar perfil de análisis (selección manual)

Cuando desea analizar con un perfil de análisis personalizado.

Crear y usar nuevo perfil de análisis

Cuando desea crear su propio perfil de análisis.

Según el sistema operativo que use, dispondrá de distintos iconos para iniciar un perfil de análisis:

- En Windows XP:

   Este icono permite iniciar el análisis por medio de un perfil de análisis.

- A partir de Windows Vista:

  A partir de Microsoft Windows Vista, de momento el Centro de control solo tiene derechos limitados, p. ej., de acceso a directorios y ficheros. El Centro de control solo puede ejecutar determinadas acciones y accesos a ficheros con derechos de administrador ampliados. Estos derechos de administrador ampliados deben concederse al iniciar cualquier análisis mediante un perfil de análisis.

  -  Este icono permite iniciar un análisis limitado por medio de un perfil de análisis. Solo se analizan los directorios y ficheros para los que el sistema operativo ha concedido derechos de acceso.
  -  Este icono permite iniciar el análisis con derechos de administrador ampliados. Tras una confirmación, se analizan todos los directorios y ficheros del perfil de análisis seleccionado.

Así se analiza la existencia de virus y malware con un perfil de análisis:

- Seleccione en el Centro de control la sección *SEGURIDAD DEL PC* **> Scanner**.
  - ↪ Aparecen perfiles de análisis predefinidos.
- Seleccione uno de los perfiles de análisis predefinidos.

  -O BIEN-

  Adapte el perfil de análisis **Selección manual**.

  -O BIEN-

  Cree un perfil de análisis nuevo
- Haga clic en el icono (Windows XP:  o a partir de Windows Vista: ).
- Aparece la ventana **Luke Filewalker** y se inicia el análisis directo.

↳ Una vez transcurrido el proceso de análisis, se muestran los resultados.

Si desea adaptar un perfil de análisis:

- Despliegue el árbol de ficheros del perfil de análisis **Selección manual** de manera que estén abiertos todos los directorios y las unidades que va a analizar.
- Haga clic en el signo **+**: aparece el siguiente nivel de directorios.
- Haga clic en el signo **-**: se oculta el siguiente nivel de directorios.
- Seleccione los nodos y directorios que deban analizarse haciendo clic en la casilla del nivel de directorios correspondiente:

  Dispone de las siguientes posibilidades de seleccionar directorios:

- Directorio con subdirectorios incluidos (marca de verificación negra)
- Solo los subdirectorios de un directorio (marca de verificación gris, los subdirectorios tienen marcas de verificación negras)
- Ningún directorio (ninguna marca de verificación)

Si desea crear un perfil de análisis nuevo:

- Haga clic en el icono  **Crear nuevo perfil.**

  ↳ Aparece el perfil **Nuevo perfil** debajo de los perfiles existentes.
- Si es necesario, cambie el nombre del perfil de análisis haciendo clic en el icono  .
- Seleccione los nodos y directorios que desee analizar mediante un clic en la casilla del nivel de directorios correspondiente.

  Dispone de las siguientes posibilidades de seleccionar directorios:

- Directorio con subdirectorios incluidos (marca de verificación negra)
- Solo los subdirectorios de un directorio (marca de verificación gris, los subdirectorios tienen marcas de verificación negras)
- Ningún directorio (ninguna marca de verificación)

4.2.5 Análisis directo: Analizar la existencia de virus y malware mediante arrastrar y soltar

A continuación, le mostramos cómo analizar de manera selectiva la existencia de virus y malware mediante arrastrar y soltar:

✓ El Centro de control de su programa Avira está abierto.

- Seleccione el fichero o el directorio que se va a analizar.
- Arrastre con el botón izquierdo del ratón el fichero o el directorio seleccionado al Centro de control.

  ↳ Aparece la ventana **Luke Filewalker** y se inicia el análisis directo.

↪ Una vez transcurrido el proceso de análisis, se muestran los resultados.

4.2.6 Análisis directo: Analizar la existencia de virus y malware mediante el menú contextual

Así se analiza la existencia de virus y malware a través del menú contextual de forma precisa:

- Haga clic (p. ej., en el Explorador de Windows, en el escritorio o en un directorio de Windows abierto) con el botón derecho del ratón en el fichero o directorio que desee analizar.
  ↪ Aparece el menú contextual del Explorador de Windows.
- En el menú contextual seleccione **Analizar ficheros seleccionados con Avira**.
  ↪ Aparece la ventana**Luke Filewalker** y se inicia el análisis directo.
  ↪ Una vez transcurrido el proceso de análisis, se muestran los resultados.

4.2.7 Análisis directo: Analizar la existencia de virus y malware de forma automática

> **Nota**
> Después de la instalación, la tarea de análisis *Análisis completo del sistema* queda creada en el planificador: Se ejecuta un análisis completo del sistema en un intervalo recomendado.

Así se crea una tarea con la que analizar automáticamente la existencia de virus y malware:

- Seleccione en el Centro de control la sección *ADMINISTRACIÓN* **> Programador**.
- Haga clic en el icono  **Crear tarea nueva con el asistente**.
  ↪ Aparece el cuadro de diálogo **Nombre y descripción de la tarea**.
- Asigne nombre a la tarea y descríbala si fuera el caso.
- Haga clic en **Siguiente**.
  ↪ Aparece el cuadro de diálogo **Tipo de tarea**.
- Seleccione la **tarea de análisis**.
- Haga clic en **Siguiente**.
  ↪ Aparece el cuadro de diálogo **Selección del perfil**.
- Seleccione el perfil que debe analizarse.
- Haga clic en **Siguiente**.
  ↪ Aparece el cuadro de diálogo **Momento de inicio de la tarea**.

- Seleccione cuándo se ejecutará el análisis:
  - **Inmediatamente**
  - **Diariamente**
  - **Semanalmente**
  - **Intervalo**
  - **Una vez**
  - **Inicio de sesión**
- Según lo que seleccione, indique la fecha si fuera necesario.
- En caso necesario, seleccione la siguiente opción adicional (disponible en algunos tipos de tarea): **Repetir la tarea si el tiempo ya transcurrió**
  - ↪ Las tareas del pasado se relanzan si no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.
- Haga clic en **Siguiente**.
  - ↪ Aparece el cuadro de diálogo **Selección del modo de visualización**.
- Seleccione el modo de visualización de la ventana de tareas:
  - **Invisible**: ninguna ventana de tarea
  - **Minimizado**: solo barra de progreso
  - **Maximizado**: toda la ventana de tarea
- Seleccione la opción **Apagar equipo cuando haya finalizado la tarea** si desea que el equipo se apague en cuanto la tarea haya sido ejecutada y finalizada.

  La opción solamente está disponible en el modo de representación minimizado o maximizado.
- Haga clic en **Finalizar**.
  - ↪ La tarea recién creada aparece en la página de inicio de la sección *ADMINISTRACIÓN* **> Programador** como activada (marca de verificación).
- Si es el caso, desactive las tareas que no deban ejecutarse.

Los siguientes iconos permiten continuar con la edición de las tareas:

Ver las propiedades de una tarea

Modificar tarea

Eliminar tarea

Iniciar tarea

Detener tarea

4.2.8 Analizar directamente la existencia de rootkits activos

Para analizar la existencia de rootkits activos, use el perfil de análisis predefinido **Búsqueda de rootkits y malware activo**.

Así se analiza directamente la existencia de rootkits activos:

- Seleccione en el Centro de control la sección *SEGURIDAD DEL PC* **> Scanner**.
  - ↳ Aparecen perfiles de análisis predefinidos.
- Seleccione el perfil de análisis predefinido **Búsqueda de rootkits y malware activo**.
- Seleccione si fuera el caso más nodos y directorios para analizar mediante un clic en la casilla del nivel de directorios.
- Haga clic en el icono (Windows XP:  o a partir de Windows Vista: ).
  - ↳ Aparece la ventana **Luke Filewalker** y se inicia el análisis directo.
  - ↳ Una vez transcurrido el proceso de análisis, se muestran los resultados.

4.2.9 Reaccionar a virus y malware detectados

Para cada uno de los componentes de protección de su producto Avira puede establecer, en la sección de la configuración **Acción al detectar**, la manera en que su producto Avira reaccionará al detectar un virus o programa no deseado.

En el componente ProActiv de Real-Time Protection no existen opciones de acción configurables: La detección se notificará en la ventana **Real-Time Protection: comportamiento sospechoso de una aplicación**.

Opciones de acción de Scanner:

- **Interactivo**

  En el modo de acción interactivo, las detecciones de Scanner se notifican en un cuadro de diálogo. Este ajuste está activado de forma estándar.
  Al finalizar el **análisis de Scanner**, recibirá un mensaje de advertencia con una lista de los ficheros afectados encontrados. Tiene la posibilidad de seleccionar la acción que desea ejecutar para cada archivo afectado mediante un menú contextual. Puede ejecutar las acciones seleccionadas para los ficheros afectados o finalizar Scanner.

- **Automático**

  Al detectar un virus o programa no deseado en el modo de acción automático, se ejecuta automáticamente la acción seleccionada en esta área. Si activa la opción **Mostrar mensaje de advertencia**, al detectar un virus recibirá un mensaje de advertencia en el que se muestra la acción ejecutada.

Opciones de acción de Real-Time Protection:

- **Interactivo**

En el modo de acción interactivo se impide el acceso a los datos y se muestra una notificación en el escritorio. En esta podrá eliminar el malware detectado o pasar el malware a Scanner a través del botón **Detalles** para el consiguiente tratamiento de virus. Scanner informa de la detección en una ventana en la que dispondrá de distintas opciones para el tratamiento del fichero afectado a través de un menú (consulte Detección > Scanner).

- **Automático**

  Al detectar un virus o programa no deseado en el modo de acción automático, se ejecuta automáticamente la acción seleccionada en esta área. Si activa la opción **Mostrar mensaje de advertencia**, al detectar un virus recibirá una notificación de escritorio.

Opciones de acción de Mail Protection, Web Protection:

- **Interactivo**

  Al detectar un virus o programa no deseado en el modo de acción interactivo, aparece un cuadro de diálogo en el que puede seleccionar lo que debe hacerse con el objeto afectado. Este ajuste está activado de forma estándar.

- **Automático**

  Al detectar un virus o programa no deseado en el modo de acción automático, se ejecuta automáticamente la acción seleccionada en esta área. Si activa la opción **Mostrar barra de progreso**, al detectar un virus recibirá un mensaje de advertencia en el que debe confirmar la acción que se va a ejecutar.

Modo de acción interactivo

- Tras detectar virus y programas no deseados en el modo de acción interactivo, en el mensaje de advertencia que recibe debe seleccionar una **acción para los objetos afectados** y ejecutarla mediante **confirmación**.

Dispone de las siguientes acciones de tratamiento de los objetos afectados entre las que elegir:

> **Nota**
> Las acciones que se pueden seleccionar dependen del sistema operativo, del componente de protección (Avira Scanner, Avira Real-Time Protection, Avira Mail Protection, Avira Web Protection) que notifica la detección y del malware detectado.

Acciones de Scanner y Real-Time Protection (sin detecciones de ProActiv):

- **Reparar**

  Se repara el fichero.
  Solo puede activar esta opción si el fichero detectado se puede reparar.

- **Cambiar el nombre**

Se cambia el nombre del fichero añadiéndole la extensión **.vir*. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Posteriormente, los ficheros se pueden reparar y su nombre se puede cambiar de nuevo.

- **Cuarentena**

  El fichero se comprime con un formato especial (**.qua*) y se mueve al directorio de cuarentena *INFECTED* del disco duro, de manera que ya no se puede tener acceso a él. Los ficheros de este directorio pueden repararse posteriormente en la cuarentena o, si fuera necesario, enviarse a Avira.

- **Eliminar**

  Se borra el archivo. Este proceso es considerablemente más rápido que **Sobrescribir y eliminar**.
  Si la detección corresponde a un virus del sector de arranque, su eliminación elimina también el sector de arranque. Se escribe un sector de arranque nuevo.

- **Omitir**

  No se ejecuta ninguna acción más. El fichero afectado permanece activo en el equipo.

- **Sobrescribir y eliminar**

  El fichero se sobrescribe con un patrón predeterminado y, a continuación, se elimina. El archivo no se puede recuperar.

Advertencia
Existe el riesgo de pérdida de datos y de daños del sistema operativo.
Use la opción **Omitir** solo en casos excepcionales justificados.

- **Ignorar siempre**

  Opción de acción en caso de detecciones de Real-Time Protection: Real-Time Protection no ejecuta ninguna acción más. Se permite el acceso al fichero. Todos los demás accesos a ese fichero se admiten y no se notifican hasta que se reinicie el equipo o tenga lugar una actualización del fichero de firmas de virus.

- **Copiar a cuarentena**

  Opción de acción al detectar un rootkit: la detección se copia a la cuarentena.

- **Reparar sector de arranque | Descargar herramienta de reparación (Repair Tool)**

  Opciones de acción en caso de detección de sectores de arranque infectados: Para disqueteras infectadas se dispone de opciones para la reparación. Si una reparación con su producto Avira no fuera posible, podrá descargar una herramienta especial para la detección y eliminación de virus del sector de arranque.

Nota
Si aplica acciones a procesos activos, los procesos afectados se terminarán antes de ejecutar la acción.

Acciones de Real-Time Protection en caso de detecciones del componente ProActiv (aviso de acciones sospechosas de una aplicación):

- **Programa de confianza**

  Se continúa la ejecución de la aplicación. El programa se añade a la lista de las aplicaciones autorizadas y se excluye de la monitorización por el componente ProActiv. Al añadir la aplicación autorizada a la lista, se establece el tipo de monitorización *Contenido*. Esto significa que la aplicación solamente se excluye de una monitorización por el componente ProActiv si su contenido permanece invariado (consulte Filtro de aplicación: Aplicaciones a excluir).

- **Bloquear programa una vez**

  La aplicación se bloquea, es decir, la ejecución de la aplicación finaliza. Las acciones de la aplicación se seguirán monitorizando por el componente ProActiv.

- **Bloquear siempre este programa**

  La aplicación se bloquea, es decir, la ejecución de la aplicación finaliza. El programa se añade a la lista de las aplicaciones que se deben bloquear y ya no podrá ejecutarse (consulte Filtro de aplicación: Aplicaciones a bloquear).

- **Omitir**

  Se continúa la ejecución de la aplicación. Las acciones de la aplicación se seguirán monitorizando por el componente ProActiv.

Acciones de Mail Protection: emails entrantes

- **Mover a cuarentena**

  El email con todos sus datos adjuntos se mueve a la cuarentena. El email afectado se elimina. El texto principal y los datos adjuntos, si los hay, se sustituyen por un texto predeterminado.

- **Eliminar email**

  El email afectado se elimina. Un texto predeterminado sustituye el cuerpo de texto y, si fuera el caso, los datos adjuntos.

- **Eliminar datos adjuntos**

  Un texto predeterminado sustituye los datos adjuntos afectados. Si está afectado el texto principal del correo electrónico, este se borra y se sustituye también por un texto predeterminado. El email en sí se entrega.

- **Mover datos adjuntos a cuarentena**

  Los datos adjuntos afectados se ponen en cuarentena y posteriormente se eliminan (se sustituyen por un texto predeterminado). El cuerpo del texto en sí se entrega. Los datos adjuntos se pueden enviar posteriormente mediante el Gestor de cuarentena.

- **Omitir**

  El email afectado se entrega.

> **Advertencia**
> Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. Seleccione la opción **Omitir** solo en casos excepcionales justificados. Desactive la vista previa en su cliente de correo y ¡nunca abra un fichero adjunto con un doble clic!

Acciones de Mail Protection: emails salientes

- **Mover correo a cuarentena (no enviar)**

  El email con todos sus datos adjuntos se copia en la cuarentena y no se envía. El email permanece en la bandeja de salida del cliente de correo. El programa de correo emite un mensaje de error. En cada proceso de envío posterior de la cuenta de correo se analiza este email para detectar si contiene malware.

- **Bloquear envío de correo (no enviar)**

  El email no se envía y permanece en la bandeja de salida del cliente de correo. El programa de correo emite un mensaje de error. En cada proceso de envío posterior de la cuenta de correo se analiza este email para detectar si contiene malware.

- **Omitir**

  El email afectado se envía.

> **Advertencia**
> Hay posibilidad de que un virus o programa no deseado pueda acceder al equipo del destinatario del email.

Acciones de Web Protection:

- **Denegar acceso**

  El sitio web requerido por el servidor web y los datos solicitados no son transferidos a su navegador. Un error de acceso denegado ha sido mostrado en su navegador web.

- **Cuarentena**

  La página web solicitada por el servidor web o los datos y ficheros transmitidos se mueven a la cuarentena. El gestor de cuarentena puede recuperar el fichero afectado si tiene valor informativo o, en caso necesario, enviarlo al Avira Malware Research Center.

- **Omitir**

  La página web solicitada por el servidor web o los datos y ficheros transmitidos se pasan por Web Protection a su navegador.

Advertencia
Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. Seleccione la opción **Omitir** solo en casos excepcionales justificados.

Nota
Se recomienda mover a la cuarentena cualquier fichero sospechoso que no se pueda reparar.

Nota
Envíenos los ficheros notificados por la heurística para analizarlos.
Estos ficheros se pueden cargar a través de nuestra página web, por ejemplo: http://www.avira.es/sample-upload
Los ficheros notificados por la heurística pueden reconocerse por la denominación *HEUR/* o *HEURISTIC/* antepuesta al nombre de fichero, p. ej.: *HEUR/prueba.**.

4.2.10 Cuarentena: Tratamiento de ficheros (*.qua) en la cuarentena

A continuación, le mostramos cómo tratar los ficheros en la cuarentena:

- Seleccione en el Centro de control la sección *ADMINISTRACIÓN* **> Cuarentena**.
- Compruebe de qué ficheros se trata, de modo que pueda cargar los originales desde otro lugar a su equipo si fuera necesario.

Si desea ver información más detallada de un fichero:

- Seleccione el fichero y haga clic en  .
  - ↳ Aparece el cuadro de diálogo **Propiedades** con más información sobre el fichero.

Si desea analizar de nuevo un fichero:

Se recomienda analizar un fichero cuando se ha actualizado el fichero de firmas de virus de su producto Avira y se sospecha que existe una falsa alarma. De esta forma, podrá confirmar tras un nuevo análisis que se trata de una falsa alarma y restablecer el fichero.

- Seleccione el fichero y haga clic en  .
  - ↳ El fichero se analiza con la configuración del análisis directo para detectar virus y malware.

↳ Tras el análisis, aparece el cuadro de diálogo **Estadística del análisis**, que muestra una estadística sobre el estado del fichero antes y después del nuevo análisis.

Si desea eliminar un fichero:

- Seleccione el fichero y haga clic en  .
- Debe confirmar su selección con **Sí**.

Si desea cargar el fichero en un servidor web del Avira Malware Research Center para analizarlo:

- Seleccione el fichero que desea cargar.
- Haga clic en  .
  ↳ Se abre el cuadro de diálogo *Carga de ficheros* con un formulario para indicar sus datos de contacto.
- Indique los datos completos.
- Seleccione un tipo: **Fichero sospechoso** o **Sospecha de falsa alarma**.
- Seleccione un formato de respuesta: **HTML**, **texto**, **HTML y texto**.
- Haga clic en **Aceptar.**
  ↳ El fichero se carga comprimido en un servidor web del Avira Malware Research Center.

Nota
En los siguientes casos se recomienda un análisis por el Avira Malware Research Center:
Detección mediante heurística (fichero sospechoso): Durante un análisis, su producto Avira ha clasificado un fichero como sospechoso y lo ha movido a la cuarentena: en el cuadro de diálogo de detección de virus o en el fichero de informe del análisis se recomienda el análisis del fichero por parte del Avira Malware Research Center.
Fichero sospechoso: Considera que un fichero es sospechoso por lo que lo ha añadido a la cuarentena; sin embargo, el análisis del fichero en cuanto a virus y malware da un resultado negativo.
Sospecha de falsa alarma: Supone que la detección de un virus es una falsa alarma: Su producto Avira notifica la detección en un fichero que con toda probabilidad no está afectado por malware.

Nota
El tamaño de los ficheros que se cargan está limitado a 20 MB sin comprimir o 8 MB comprimido.

Nota
Para cargar varios ficheros simultáneamente, debe seleccionar todos los ficheros que desea cargar y pulsar el botón **Enviar objeto**.

Si desea copiar un objeto de la cuarentena a otro directorio:

- Seleccione el objeto en cuarentena y haga clic en  .
  - ↪ Se abre el cuadro de diálogo *Analizar carpeta* en el que puede seleccionar un directorio.
- Seleccione un directorio donde desee guardar una copia del objeto en cuarentena y confirme su selección con **Aceptar**.
  - ↪ El objeto de cuarentena seleccionado se guardará en el directorio elegido.

Nota
El objeto de cuarentena no es idéntico al fichero restaurado. El objeto de cuarentena está cifrado y no puede ejecutarse ni leerse en su formato original.

Si desea exportar las propiedades de un objeto en cuarentena a un fichero de texto:

- Seleccione el objeto en cuarentena y haga clic en  .
  - ↪ Se abre un fichero de texto con los datos sobre el objeto en cuarentena seleccionado.
- Guarde el fichero de texto.

Los ficheros que están en la cuarentena se pueden restaurar (consulte capítulo: Cuarentena: Restaurar los ficheros de cuarentena).

4.2.11 Restaurar los ficheros de cuarentena

Según el sistema operativo que use, dispondrá de distintos iconos para la restauración:

- En Windows XP:
  -  Este icono permite restaurar los ficheros en su directorio original.
  -  Este icono permite restaurar los ficheros en el directorio que elija.
- A partir de Windows Vista:

  A partir de Microsoft Windows Vista, de momento el Centro de control solo tiene derechos limitados, p. ej., de acceso a directorios y ficheros. El Centro de control solo puede ejecutar determinadas acciones y accesos a ficheros con derechos de

administrador ampliados. Estos derechos de administrador ampliados deben concederse al iniciar cualquier análisis mediante un perfil de análisis.

-  Este icono permite restaurar los ficheros en el directorio que elija.
-  Este icono permite restaurar los ficheros en su directorio original. Si para acceder a este directorio se necesitan derechos de administrador ampliados, aparece la consulta correspondiente.

Así puede restaurar los ficheros que están en la cuarentena:

> **Advertencia**
> Existe el riesgo de pérdida de datos y de daños del sistema operativo del equipo. Use la función **Restaurar objeto seleccionado** solo en casos excepcionales. Restaure únicamente aquellos ficheros que pudieron repararse mediante un nuevo análisis.

✓ Fichero analizado y reparado con nuevo análisis.

▸ Seleccione en el Centro de control la sección *ADMINISTRACIÓN* **> Cuarentena**.

> **Nota**
> Los emails y datos adjuntos solo pueden restaurarse con la opción  y la extensión **.eml*.

Si desea restaurar un fichero en su ubicación original:

▸ Seleccione el fichero y haga clic en el icono (Windows XP:  , a partir de Windows Vista ).

Esta opción no está disponible para emails.

> **Nota**
> Los emails y datos adjuntos solo pueden restaurarse con la opción  y la extensión **.eml*.

↳ Aparece la petición de si desea restaurar el fichero.

▸ Haga clic en **Sí**.

↳ El fichero se restaura en el directorio desde el que se movió a la cuarentena.

Si desea restaurar un fichero en un determinado directorio:

- Seleccione el fichero y haga clic en  .
  - ↪ Aparece la petición de si desea restaurar el fichero.
- Haga clic en **Sí**.
  - ↪ Aparece la ventana predeterminada de Windows para seleccionar directorios.
- Seleccione el directorio en el que va a restaurar el fichero y confirme.
  - ↪ El fichero se restaura en el directorio seleccionado.

4.2.12 Cuarentena: Mover fichero sospechoso a cuarentena

A continuación, le explicamos cómo mover manualmente un fichero sospechoso a cuarentena:

- Seleccione en el Centro de control la sección *ADMINISTRACIÓN* **> Cuarentena**.
- Haga clic en  .
  - ↪ Aparece la ventana predeterminada de Windows para seleccionar ficheros.
- Seleccione el fichero y confirme la operación con **Abrir**.
  - ↪ El fichero se mueve a la cuarentena.

Puede analizar los ficheros de la cuarentena con Avira Scanner (consulte el capítulo: Cuarentena: tratamiento de ficheros (*.qua) en la cuaretena).

4.2.13 Perfil de análisis: Añadir o eliminar un tipo de fichero de un perfil de análisis

De esta manera, se especifica para un perfil de análisis que se analizarán adicionalmente ciertos tipos de fichero o que determinados tipos de fichero quedarán excluidos del análisis (solo posible con la selección manual y perfiles de análisis definidos por el usuario):

- ✓ Se encuentra en el Centro de control, en la sección *SEGURIDAD DEL PC* **> Scanner**.
- Haga clic con el botón derecho del ratón en el perfil de análisis que desea editar.
  - ↪ Aparece un menú contextual.
- Seleccione la entrada **Filtro de ficheros**.
- Despliegue más el menú contextual haciendo clic en el pequeño triángulo de la parte derecha del menú contextual.
  - ↪ Aparecen las entradas **Predeterminado**, **Analizar todos los ficheros** y **Definido por el usuario**.
- Seleccione la entrada **Definido por el usuario**.

↳ Aparece el cuadro de diálogo **Extensiones de fichero** con una lista de todos los tipos de fichero que se analizarán con el perfil de análisis.

Si desea excluir un tipo de fichero del análisis:

- Seleccione el tipo de fichero y haga clic en **Eliminar**.

Si desea añadir un tipo de fichero al análisis:

- Seleccione un tipo de fichero.
- Haga clic en **Insertar** e introduzca la extensión de fichero del tipo de fichero en el campo de entrada.

  Use un máximo de 10 caracteres y no indique el punto inicial. Se admiten comodines (* y ?).

4.2.14 Perfil de análisis: Crear acceso directo en el escritorio para el perfil de análisis

Puede iniciar un análisis directo directamente desde el escritorio por medio de un acceso directo a un perfil de análisis sin tener que activar el Centro de control de su producto Avira.

Así se crea un acceso directo al perfil de análisis en el escritorio:

✓ Se encuentra en el Centro de control, en la sección *SEGURIDAD DEL PC* **> Scanner**.

- Seleccione el perfil de análisis para el que desea crear un enlace o acceso directo.
- Haga clic en el icono  .

  ↳ Se crea el acceso directo en el escritorio.

4.2.15 Eventos: Filtrar eventos

En el Centro de control, en *ADMINISTRACIÓN* **> Eventos**, se muestran todos los eventos generados por los componentes de programa de su producto Avira (de forma parecida a como lo hace el visor de eventos del sistema operativo Windows). Los componentes de programa son los siguientes:

- Web Protection
- Real-Time Protection
- Mail Protection
- FireWall
- Servicio de ayuda
- Programador
- Scanner

- Updater
- ProActiv

Se muestran los siguientes tipos de evento:

- *Información*
- *Advertencia*
- *Error*
- *Detección*

Así se filtran los eventos mostrados:

- Seleccione en el Centro de control la categoría *ADMINISTRACIÓN* **> Eventos**.
- Active las casillas de verificación de los componentes de programa para mostrar los eventos de los componentes activados.

  - O BIEN -

  Desactive las casillas de verificación de los componentes de programa para ocultar los eventos de los componentes desactivados.
- Active las casillas de verificación de los tipos de evento para mostrar estos eventos.

  - O BIEN -

  Desactive las casillas de verificación de los tipos de evento para ocultar estos eventos.

4.2.16 Mail Protection: Excluir direcciones de email del análisis

Así se establecen las direcciones de email (remitente) que deben excluirse del análisis de Mail Protection (listas blancas):

- Seleccione en el Centro de control la sección *SEGURIDAD EN INTERNET* **> Mail Protection**.
  - ↪ En la lista verá los emails recibidos.
- Seleccione el email que desea excluir del análisis de Mail Protection.
- Haga clic en el icono deseado para excluir el email del análisis de Mail Protection:

   La dirección de email seleccionada ya no se analizará en el futuro en busca de virus y programas no deseados.

  - ↪ La dirección del remitente de email se incluye en la lista de exclusiones y ya no se analizará en busca de virus, programas no deseados.

Advertencia
Excluya del análisis de Mail Protection únicamente direcciones de email de remitentes de total confianza.

Nota
En la configuración, en Mail Protection > General > Excepciones, puede introducir más direcciones de email en la lista de exclusiones o eliminar direcciones de dicha lista.

4.2.17 FireWall: Seleccionar nivel de seguridad para el FireWall

Puede seleccionar entre distintos niveles de seguridad. En función de ello, dispondrá de diferentes posibilidades de configuración para las reglas del adaptador.

Dispone de los siguientes niveles de seguridad:

Bajo

Se detecta el desbordamiento y el escaneo de puertos.

Medio

Se descartan los paquetes TCP y UDP sospechosos.

Se impide el desbordamiento y el escaneo de puertos.

(Configuración predeterminada)

Alto

El equipo es invisible en la red.

No se permiten nuevas conexiones exteriores.

Se impide el desbordamiento y el escaneo de puertos.

Usuario

Reglas definidas por el usuario: el programa cambia automáticamente a este nivel de seguridad si se cambiaron reglas del adaptador.

Bloquear todos

Finaliza todas las conexiones de red existentes.

Nota
El ajuste predeterminado del Nivel de seguridad para todas las reglas predefinidas de FireWall de Avira es **Medio.**

El nivel de seguridad para FireWall se configura de la siguiente manera:

- Seleccione en el Centro de control la categoría *SEGURIDAD EN INTERNET* **> FireWall**.
- Sitúe el control deslizante en el nivel de seguridad que desee.

↪ El nivel de seguridad seleccionado se activa de inmediato.

5. Detección

5.1 Información general

Cuando se detectan virus, el producto de Avira puede ejecutar determinadas acciones automáticamente o reaccionar interactivamente. En el modo de acción interactivo, cuando se detectan virus, se abre un cuadro de diálogo en el que controla o inicia el tratamiento posterior de los virus (Eliminar, Omitir, etc.). En el modo automático existe la opción de mostrar un mensaje de advertencia si se detectan virus. En el mensaje se muestra la acción que se ha realizado automáticamente.

En este capítulo se ordena por módulos toda la información sobre los mensajes de una detección.

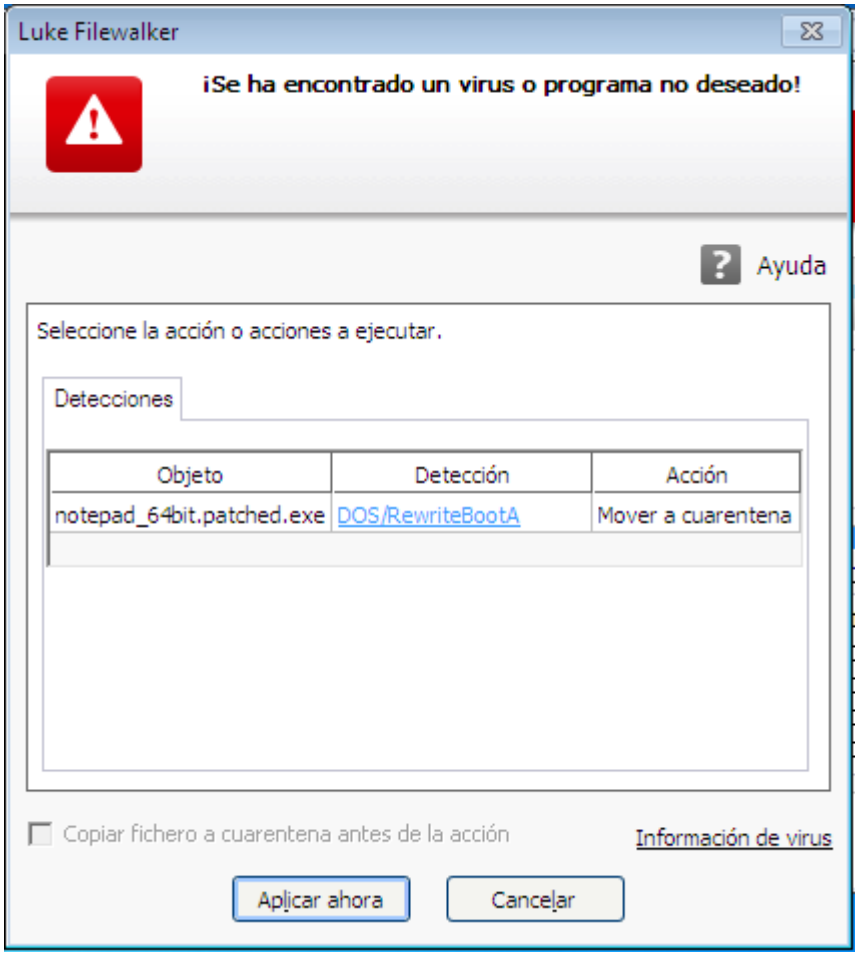
- Véase el capítulo Scanner: modo de acción interactivo
- Véase el capítulo Scanner: modo de acción automático
- Véase el capítulo Scanner: enviar archivos a Protection Cloud
- Véase el capítulo Real-Time Protection
- Véase el capítulo Real-Time Protection: comportamiento sospechoso
- Véase el capítulo Mail Protection: correos electrónicos entrantes
- Véase el capítulo Mail Protection: correos electrónicos salientes
- Véase el capítulo Envío de email: servidor
- Véase el capítulo Envío de email: remitente
- Véase el capítulo Web Protection

5.2 Modo de acción interactivo

Una vez finalizado el análisis de archivos de Scanner, se muestra un mensaje de advertencia con una lista de los ficheros afectados detectados si ha seleccionado como modo de acción para los virus detectados el modo *Interactivo* (véase la sección sobre configuración Scanner > Análisis > Acción al detectar).
Tiene la posibilidad de seleccionar la acción que desea ejecutar para cada archivo afectado mediante un menú contextual. Puede ejecutar las acciones seleccionadas para los ficheros afectados o finalizar Scanner.

Nota
Si el registro está activado, Scanner registra cada detección en el fichero de informe.

5.2.1 Mensaje de advertencia



5.2.2 Detección, Error, Advertencias

En las pestañas **Detección**, **Error** y **Advertencias** se muestran información detallada y opciones de acciones acerca de las detecciones de virus:

- **Detección:**
  - *Objeto:* nombre del archivo afectado.
  - *Detección:* nombre del virus encontrado o el programa no deseado.
  - *Acción:* acción seleccionada que debe realizarse en el archivo afectado.
    En el menú contextual de la acción mostrada puede seleccionar otras acciones para tratar el malware.
- **Error:** mensajes sobre los errores que se han producido durante el análisis.
- **Advertencias:** mensajes de advertencia que se refieren a los virus detectados.

> **Nota**
> En la información sobre herramientas del objeto se muestra la información

siguiente: nombre del archivo afectado y ruta completa, nombre del virus, acción que se va a realizar pulsando el botón **Aplicar ahora**.

Nota
Se muestra como acción que debe ejecutarse por defecto la acción de Scanner. La acción por defecto de Scanner para tratar los archivos afectados puede ajustarse en la sección de configuración Scanner > Análisis > Acción al detectar en el área *Acciones permitidas*.

5.2.3 Acciones del menú contextual

Nota
Si en la detección se ha empleado una técnica heurística (HEUR/), una utilidad de compresión poco habitual (PCK/) o un fichero con una extensión oculta (HEUR-DBLEXT/), en el modo interactivo solo están disponibles las opciones Mover a cuarentena y Omitir. En el modo automático la detección se mueve automáticamente a la cuarentena.
Esta limitación impide que los archivos encontrados que podrían ser una falsa alarma se quiten (eliminen) directamente de su ordenador. El fichero puede recuperarse en cualquier momento usando el Administrador de cuarentenas.
En función de la configuración pueden no estar disponibles diferentes opciones.

Reparar

Si esta opción está activada, Scanner repara el archivo afectado.

Nota
La opción **Reparar** solo se puede activar si es posible reparar el fichero detectado.

Cuarentena

Si esta opción está activada, Scanner mueve el archivo a la cuarentena. El Administrador de cuarentenas puede recuperarlo si tiene valor informativo o, en caso necesario, enviarlo al Centro de investigación de malware de Avira. En función del fichero hay disponibles otras opciones en el Administrador de cuarentenas.

Eliminar

Con esta opción activada, el fichero se borra. Esta tarea es considerablemente más rápida que "Sobrescribir y eliminar".

Sobrescribir y eliminar

Si esta opción está activada, Scanner sobrescribe el archivo con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Cambiar el nombre

Si esta opción está activada, Scanner cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar y volver a cambiar el nombre posteriormente.

Omitir

Si esta opción está activada, se sale del archivo.

Ignorar siempre

Opción de acción en caso de detecciones de Real-Time Protection: Real-Time Protection no ejecuta ninguna acción más. Se permite el acceso al fichero. Todos los demás accesos a ese fichero se admiten y no se notifican hasta que se reinicie el equipo o tenga lugar una actualización del fichero de firmas de virus.

Advertencia
Si selecciona las opciones **Omitir** o **Ignorar siempre**, los archivos afectados permanecen activos en su ordenador. Puede causar daños graves en su ordenador.

5.2.4 Peculiaridades cuando se detectan sectores de arranque infectados, rootkits y malware activo

Cuando se detectan sectores de arranque infectados, hay disponibles opciones de acción para la reparación de los sectores de arranque:

Reparar sector de arranque 722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB

Estas opciones están disponibles para las unidades de disco.

Descargar CD de rescate

Mediante esta opción accede a la página web de Avira, donde puede descargar una herramienta especial para detectar y eliminar los virus de los sectores de arranque.

Si realiza acciones en los procesos en curso, se interrumpen los procesos afectados antes de ejecutar la acción.

5.2.5 Botones y enlaces

Botón/Enlace	Descripción
Aplicar ahora	Las acciones seleccionadas se ejecutan para tratar todos los archivos afectados.
Cancelar	Scanner no realiza ninguna acción más y finaliza. Los archivos afectados permanecen en su sistema.
Ayuda	Por medio de este botón o enlace se abre esta página de la ayuda en pantalla.

Advertencia
Ejecute la acción **Cancelar** solo en casos excepcionales justificados. Si cancela, los archivos afectados permanecen activos en su ordenador. Puede causar daños graves en su ordenador.

5.2.6 Peculiaridades de la detecciónі si Web Protection está desactivado

Si ha desactivado Web Protection, Real-Time Protection avisa del malware activo detectado mediante un aviso emergente mientras se comprueba el sistema. Antes de una reparación, tiene la posibilidad de crear un punto de restauración del sistema.

✓ La función de restauración del sistema debe estar activada en su sistema operativo Windows.

- Haga clic en **Mostrar detalles** en el aviso emergente.
  - ↪ Se abre la ventana *Analizando el sistema*.
- Active **Generar punto de restauración del sistema antes de la reparación**.
- Haga clic en **Aplicar**.
  - ↪ Se ha creado un punto de restauración del sistema. En caso necesario, ahora puede iniciar la recuperación del sistema mediante el sistema operativo Windows.

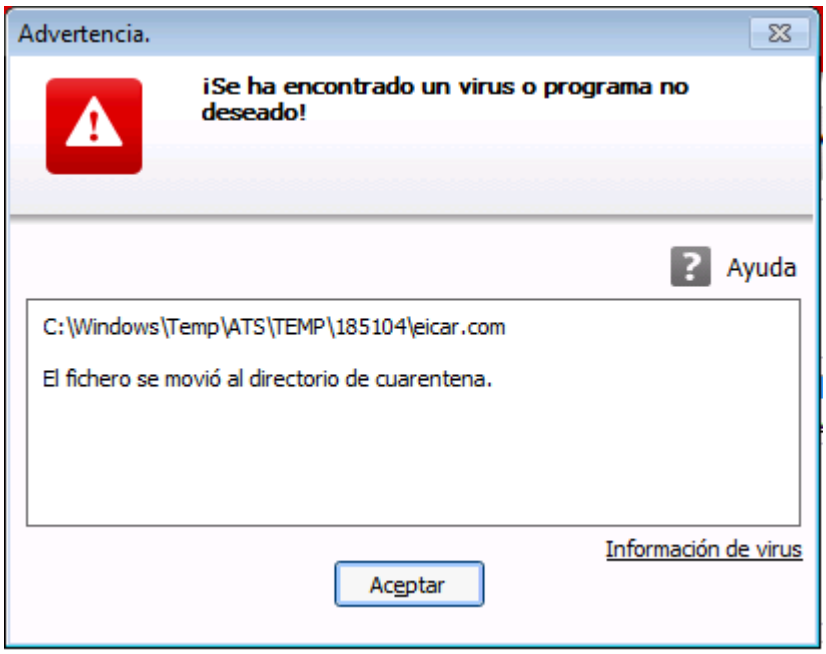
5.3 Modo de acción automático

Durante el análisis de archivos de Scanner, se muestra un mensaje de advertencia cada vez que se detecta un virus si ha seleccionado como modo de acción para los virus detectados el modo *automático* con la opción **Mostrar mensaje de advertencia** (véase la sección sobre configuración Scanner > Análisis > Acción al detectar). En el modo automático con mensaje de advertencia, no existe ninguna posibilidad de selección para

el tratamiento de la detección de los virus. Se ejecuta la acción que se ha seleccionado en la configuración para tratar el virus. En el mensaje se muestra la acción que se ha realizado automáticamente.

> **Nota**
> Si el registro está activado, Scanner registra cada detección en el fichero de informe.

5.3.1 Mensaje de advertencia



5.3.2 Botones y enlaces

Botón/Enlace	Descripción
Ayuda	Por medio de este botón o enlace se abre la página de la ayuda en pantalla.

5.4 Enviar archivos a Protection Cloud

En cada **análisis rápido del sistema** se crea una lista de las ubicaciones de guardado de ficheros. En esta lista se incluyen, por ejemplo, procesos en curso y programas de inicio y de servicio. Los ficheros de programas desconocidos se cargan para el análisis en el sistema Protection Cloud.

Si, durante la instalación personalizada o en la configuración de la **Protección avanzada**, ha activado la opción **Confirmar de manera manual si se envían a Avira ficheros sospechosos**, puede comprobar la lista de los ficheros sospechosos y seleccionar qué archivos quiere cargar en Protection Cloud. Por defecto se marcan todos los archivos sospechosos para cargarlos.

> **Nota**
> Si ha activado el registro **ampliado** durante la configuración de Scanner, el fichero de informe muestra el sufijo *(Cloud)* para identificar las advertencias de Protection Cloud.

5.4.1 Información mostrada

La lista de los ficheros sospechosos que deben cargarse en Protection Cloud.

- *¿Enviar?:* puede seleccionar qué ficheros quiere cargar en Protection Cloud.
- *Fichero:* nombre del archivo sospechoso.
- *Ruta:* ruta del fichero sospechoso.

Enviar archivos de forma automática siempre

Mientras esta opción permanece activa, después de cada **Análisis rápido del sistema** se envía automáticamente y sin confirmación manual a Protection Cloud los ficheros sospechosos para analizarlos.

5.4.2 Botones y enlaces

Botón/Enlace	Descripción
Enviar	Los ficheros seleccionados se envían a Avira Protection Cloud.
Cancelar	Scanner no realiza ninguna acción más y finaliza. Los archivos afectados permanecen en su sistema.
Ayuda	Se abre esta página de la ayuda en pantalla.
¿Qué es Protection Cloud?	Se abre la página web con información sobre Avira Protection Cloud.

Temas relacionados:

- Configuración de Protección avanzada
- Instalación personalizada

- Configuración de los informes
- Vista Informes

5.5 Real-Time Protection

Si Real-Time Protection detecta virus, se impide el acceso al archivo y se muestra una notificación en el escritorio si se ha seleccionado como modo de acción para los virus detectados el modo *Interactivo* o el modo *Automático* con la opción **Mostrar mensaje de advertencia** (véase la sección sobre configuración Real-Time Protection> Análisis > Acción al detectar).

Notificación

En la notificación se muestra la información siguiente:

- Fecha y hora de la detección
- Ruta y nombre del archivo afectado
- Nombre del malware

> **Nota**
> La selección del modo de inicio estándar de Real-Time Protection (inicio normal) y el inicio de sesión rápido en la cuenta de usuario podrían tener como consecuencia al iniciar el equipo que los programas que se ejecutan automáticamente cuando se inicia el sistema no se puedan analizar, ya que se han iniciado antes de la carga completa de Real-Time Protection.

En el modo interactivo tiene las opciones siguientes:

Suprimir

El fichero afectado se transfiere al componente **Scanner**, que procede a borrarlo. No se muestra ningún otro mensaje.

Detalles

El fichero afectado se transfiere al componente **Scanner**, que procede a borrarlo. Scanner avisa de la detección en una ventana en la que aparecen diferentes opciones para tratar el archivo afectado.

> **Nota**
> Tenga en cuenta las instrucciones sobre el tratamiento de virus en Detección > Scanner.

Nota
Para el tratamiento de virus, se muestra la acción que ha seleccionado como acción estándar en la configuración en Real-Time Protection > Análisis > Acción al detectar. Puede seleccionar otras opciones mediante un menú contextual.

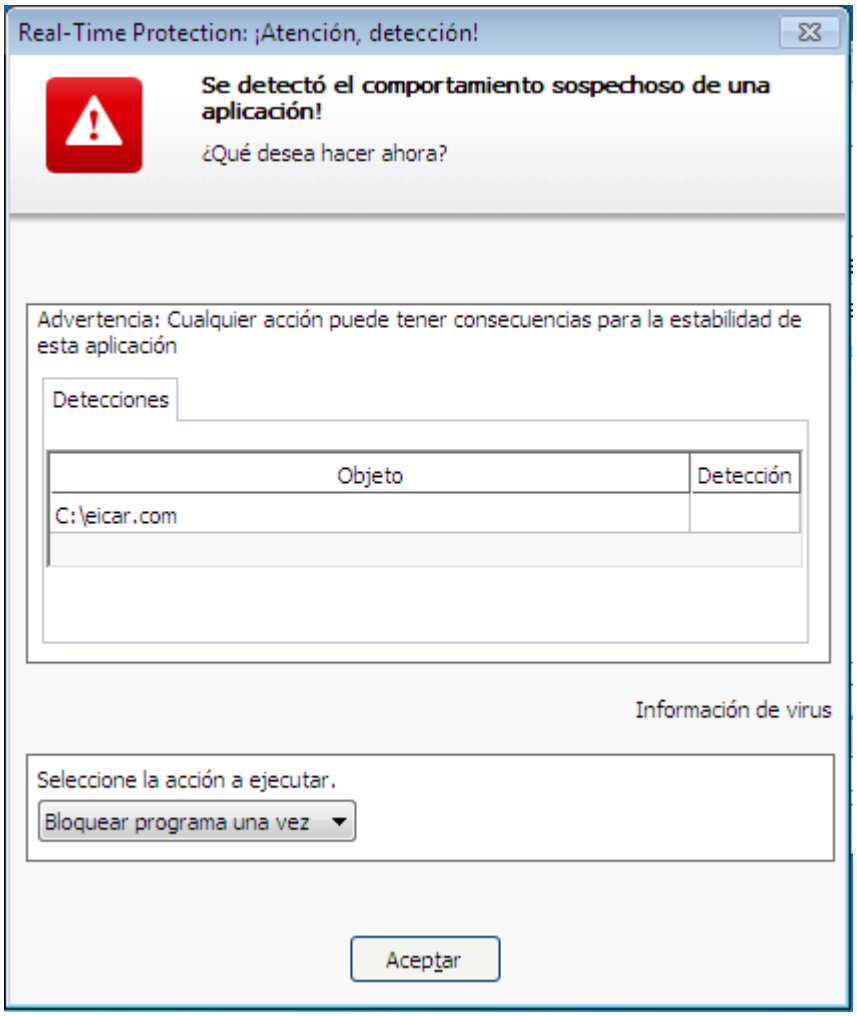
Cerrar

El mensaje se cerrará. Se interrumpe el tratamiento de los virus.

5.6 Comportamiento sospechoso

Si activa el componente ProActiv de Real-Time Protection, se controlan las acciones de las aplicaciones y se comprueba el comportamiento sospechoso típico del malware. Si una aplicación se comporta de manera sospechosa, se muestra un mensaje de advertencia. Puede actuar de diferentes formas frente a la detección.

5.6.1 Mensaje de advertencia de la protección en tiempo real: Se detectó el comportamiento sospechoso de una aplicación!



5.6.2 Nombre y ruta del programa sospechoso detectado

En el cuadro central del mensaje se muestra el nombre y la ruta de la aplicación que está realizando las acciones sospechosas.

5.6.3 Selecciones posibles

Programa de confianza

Si esta opción está activada, se sigue ejecutando la aplicación. El programa se añade a la lista de las aplicaciones autorizadas y se excluye de la monitorización por el componente ProActiv. Al añadir la aplicación autorizada a la lista, se establece el tipo de monitorización *Contenido*. Esto significa que el componente ProActiv solo excluye del control a la aplicación si el contenido no ha cambiado (véase Filtro de aplicación: Aplicaciones permitidas).

Bloquear programa una vez

Si esta opción está activada, se bloquea la aplicación, es decir, finaliza la ejecución de la misma. Las acciones de la aplicación se seguirán monitorizando por el componente ProActiv.

Bloquear siempre este programa

Si esta opción está activada, se bloquea la aplicación, es decir, finaliza la ejecución de la misma. El programa se añade a la lista de las aplicaciones que se deben bloquear y ya no podrá ejecutarse (consulte Filtro de aplicación: Aplicaciones a bloquear).

Omitir

Si esta opción está activada, se sigue ejecutando la aplicación. Las acciones de la aplicación se seguirán monitorizando por el componente ProActiv.

5.6.4 Botones y enlaces

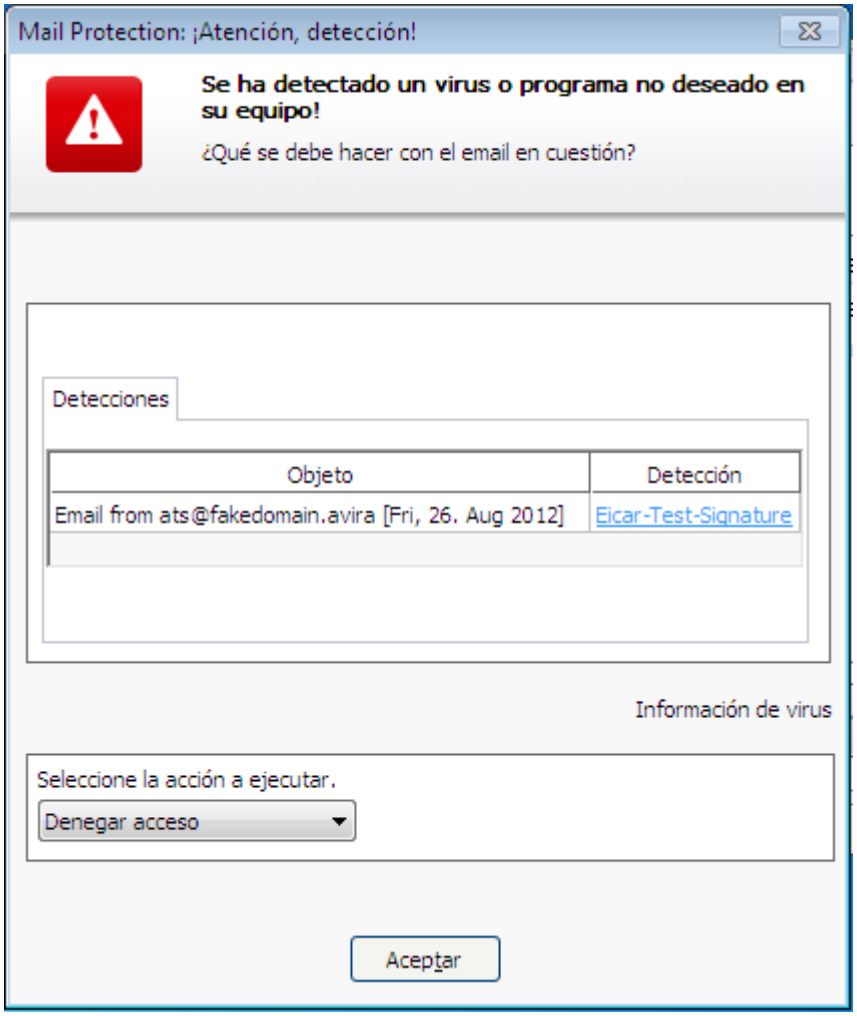
Botón/Enlace	Descripción
Información de virus	Mediante este enlace accede, si hay una conexión a Internet activa, a una página con información adicional sobre este virus o programa no deseado.
Ayuda	Por medio de este botón o enlace se abre esta página de la ayuda en pantalla.

5.7 Correos electrónicos entrantes

Si Mail Protection detecta virus, se emite un mensaje de advertencia si ha seleccionado como modo de acción para los virus detectados el modo *interactivo* (véase la sección sobre configuración Mail Protection > Análisis > Acción al detectar). En el modo interactivo puede seleccionar en el cuadro de diálogo qué debe hacerse con el correo electrónico o el dato adjunto.

El mensaje de advertencia abajo mostrado aparece cuando se detectan virus en un correo electrónico entrante.

5.7.1 Mensaje de advertencia



5.7.2 Detecciones, Error, Advertencias

En las pestañas **Detecciones**, **Error** y **Advertencias** se muestran mensajes e información detallada sobre los correos electrónicos afectados:

- **Detecciones:** Objeto: correo electrónico afectado con el remitente y la hora a la que se ha enviado dicho correo.

  Detección: nombre del virus encontrado o el programa no deseado.
- **Error:** mensajes sobre los errores que se han producido durante la comprobación por parte de Mail Protection.
- **Advertencias:** mensajes de advertencia que se refieren a los objetos afectados.

5.7.3 Selecciones posibles

Nota
Si en la detección se ha empleado una técnica heurística (HEUR/), una utilidad de compresión poco habitual (PCK/) o un fichero con una extensión oculta (HEUR-DBLEXT/), en el modo interactivo solo están disponibles las opciones Mover a cuarentena y Omitir. En el modo automático la detección se mueve automáticamente a la cuarentena.
Esta limitación impide que los archivos encontrados que podrían ser una falsa alarma se quiten (eliminen) directamente de su ordenador. El fichero puede recuperarse en cualquier momento usando el Administrador de cuarentenas.

Mover a cuarentena

Si esta opción está activada, el correo electrónico, junto con todos los datos adjuntos, se mueve a la cuarentena. Se puede enviar posteriormente mediante el Gestor de cuarentena. El email afectado se elimina. El texto principal y los datos adjuntos, si los hay, se sustituyen por un texto predeterminado.

Eliminar email

Si esta opción está activada, se borra el correo electrónico afectado cuando se detecta un virus o un programa no deseado. Un texto predeterminado sustituye el cuerpo de texto y, si fuera el caso, los datos adjuntos.

Eliminar datos adjuntos

Si esta opción está activada, se sustituyen los datos adjuntos afectados por un texto predeterminado. Si está afectado el texto principal del correo electrónico, este se borra y se sustituye también por un texto estándar. El email en sí se entrega.

Mover datos adjuntos a cuarentena

Si esta opción está activada, se mueven los datos adjuntos afectados a la cuarentena y se borran posteriormente (se sustituyen por un texto predeterminado). El cuerpo del texto en sí se entrega. Los datos adjuntos se pueden enviar posteriormente mediante el Gestor de cuarentena.

Omitir

Si esta opción está activada, se envía un correo electrónico afectado a pesar de que se detecta un virus o un programa no deseado.

Advertencia
Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. Seleccione la opción **Omitir** solo en casos excepcionales justificados. Desactive la vista previa en su cliente de correo y ¡nunca abra un fichero adjunto con un doble clic!

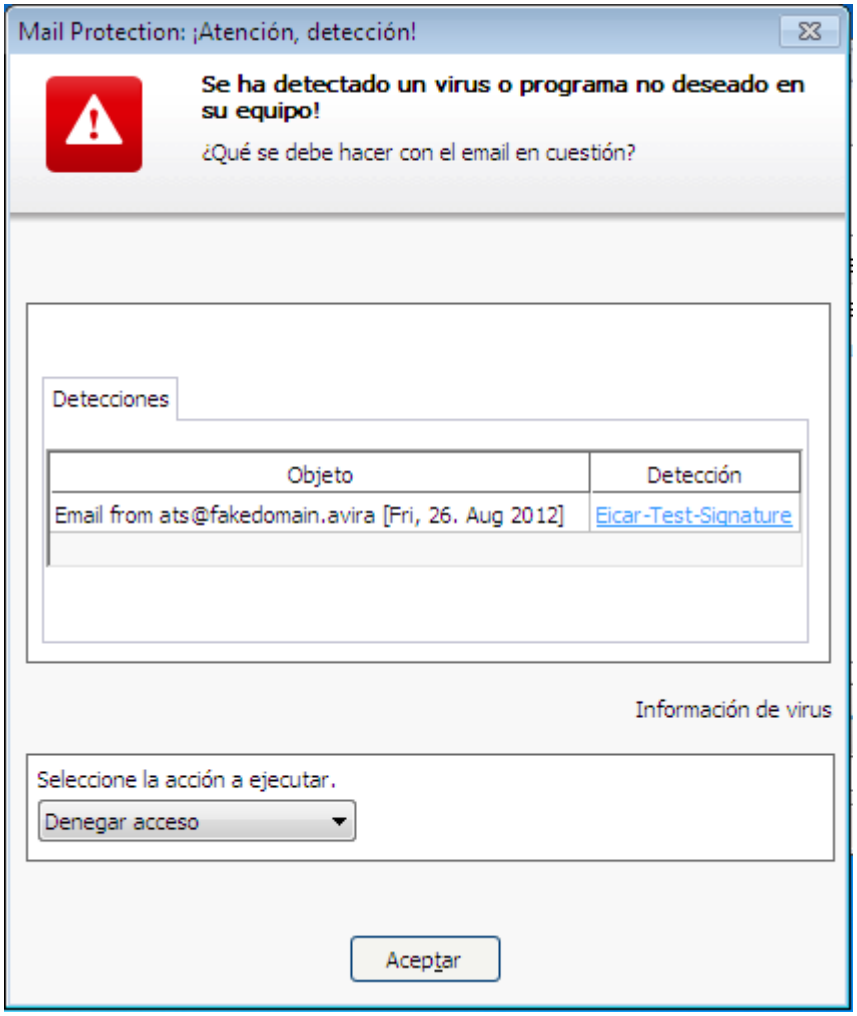
5.7.4 Botones y enlaces

Botón/Enlace	Descripción
Información de virus	Mediante este enlace accede, si hay una conexión a Internet activa, a una página con información adicional sobre este virus o programa no deseado.
Ayuda	Por medio de este botón o enlace se abre esta página de la ayuda en pantalla.

5.8 Correos electrónicos salientes

Si Mail Protection detecta virus, se emite un mensaje de advertencia si ha seleccionado como modo de acción para los virus detectados el modo *interactivo* (véase la sección sobre configuración Mail Protection > Análisis > Acción al detectar). En el modo interactivo puede seleccionar en el cuadro de diálogo qué debe hacerse con el correo electrónico o el dato adjunto.

5.8.1 Mensaje de advertencia



5.8.2 Detecciones, Error, Advertencias

En las pestañas **Detecciones**, **Error** y **Advertencias** se muestran mensajes e información detallada sobre los correos electrónicos afectados:

- **Detecciones:** Objeto: correo electrónico afectado con el remitente y la hora a la que se ha enviado dicho correo.

  Detección: nombre del virus encontrado o el programa no deseado.
- **Error:** mensajes sobre los errores que se han producido durante la comprobación por parte de Mail Protection.
- **Advertencias:** mensajes de advertencia que se refieren a los objetos afectados.

5.8.3 Selecciones posibles

Mover correo a cuarentena (no enviar)

Si esta opción está activada, el correo electrónico, junto con todos los datos adjuntos, se copia en la cuarentena y no se envía. El email permanece en la bandeja de salida del cliente de correo. El programa de correo emite un mensaje de error. En cada proceso de envío posterior de la cuenta de correo se analiza este email para detectar si contiene malware.

Bloquear envío de correo (no enviar)

El email no se envía y permanece en la bandeja de salida del cliente de correo. El programa de correo emite un mensaje de error. En cada proceso de envío posterior de la cuenta de correo se analiza este email para detectar si contiene malware.

Omitir

Si esta opción está activada, se envía el correo electrónico afectado a pesar de que se detecta un virus o un programa no deseado.

Advertencia
Hay posibilidad de que un virus o programa no deseado pueda acceder al equipo del destinatario del email.

5.8.4 Botones y enlaces

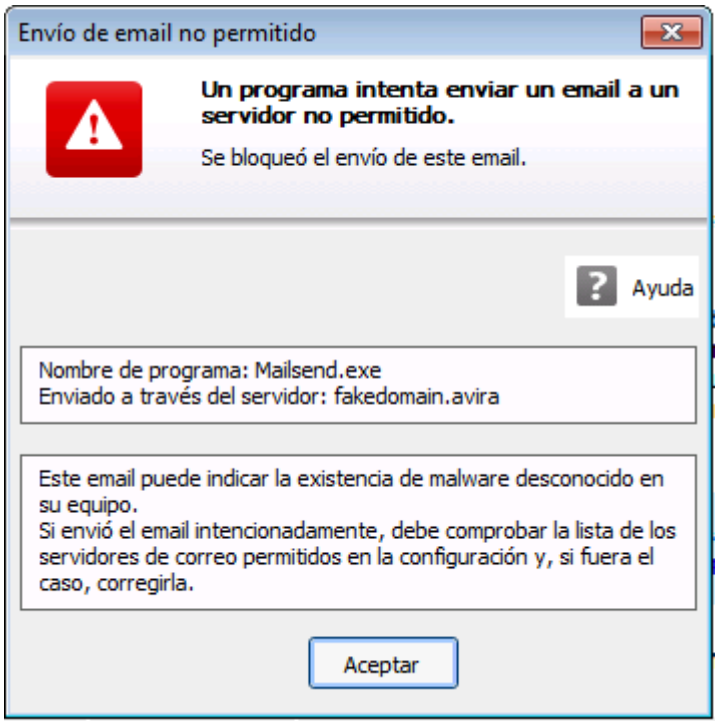
Botón/Enlace	Descripción
Información de virus	Mediante este enlace accede, si hay una conexión a Internet activa, a una página con información adicional sobre este virus o programa no deseado.
Ayuda	Por medio de este botón o enlace se abre esta página de la ayuda en pantalla.

5.9 Remitente

Si utiliza la función AntiBot de Mail Protection, Mail Protection bloquea los correos electrónicos de remitentes no autorizados. La comprobación de los remitentes se realiza a partir de la lista de los remitentes permitidos que ha guardado en la configuración en Mail

Protection > Análisis > AntiBot. El correo electrónico bloqueado se muestra en un cuadro de diálogo.

5.9.1 Mensaje de advertencia



5.9.2 Programa usado, servidor SMTP usado y dirección de correo electrónico del remitente

En el cuadro central del mensaje se muestra la información siguiente:

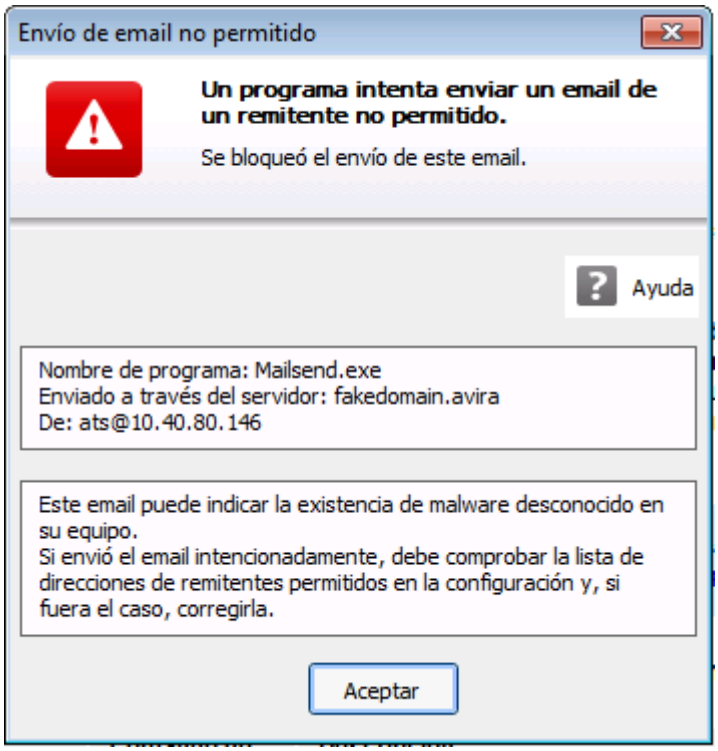
- Nombre del programa que se ha utilizado para enviar el correo electrónico.
- Nombre del servidor SMTP que se ha utilizado para enviar el correo electrónico.
- Dirección de correo electrónico del remitente

Si ha enviado el correo electrónico afectado mediante su programa de correo electrónico, compare la lista de los remitentes permitidos en la configuración en Mail Protection > Detección > AntiBot con las direcciones de los remitentes que utiliza en las cuentas de correo electrónico en su programa cliente de correo electrónico. Si la lista de los remitentes permitidos en la configuración está incompleta, registre en la lista las otras direcciones de los remitentes que utiliza. En la bandeja de salida de su programa cliente de correo electrónico puede encontrar el correo electrónico bloqueado. Para enviar el correo electrónico bloqueado, vuelva a iniciar el envío del correo electrónico después de haber completado la configuración.

5.10 Servidor

Si utiliza la función AntiBot de Mail Protection, Mail Protection bloquea los correos electrónicos enviados por servidores SMTP no autorizados. La comprobación de los servidores SMTP utilizados se realiza a partir de la lista de los servidores permitidos que ha guardado en la configuración en Mail Protection > Análisis > AntiBot. El correo electrónico bloqueado se muestra en un cuadro de diálogo.

5.10.1 Mensaje de advertencia



5.10.2 Programa usado, servidor SMTP usado

En el cuadro central del mensaje se muestra la información siguiente:

- Nombre del programa que se ha utilizado para enviar el correo electrónico.
- Nombre del servidor SMTP que se ha utilizado para enviar el correo electrónico.

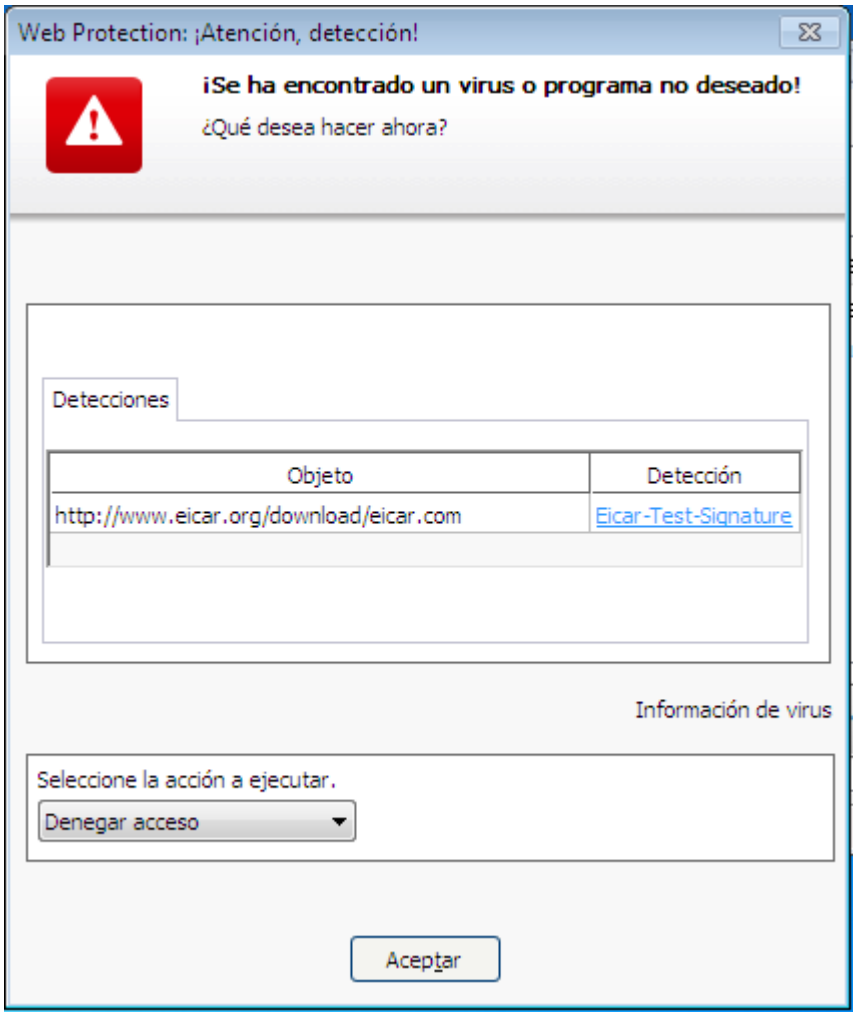
Si ha enviado el correo electrónico afectado mediante su programa de correo electrónico, compare la lista de los servidores permitidos en la configuración en Mail Protection > Detección > AntiBot con los servidores SMTP que utiliza para enviar correos electrónicos. Puede acceder a los servidores SMTP utilizados en su programa cliente de correo electrónico en las cuentas de correo electrónico utilizadas. Si la lista de los servidores permitidos en la configuración está incompleta, registre en la lista los otros servidores SMTP que utiliza. En la bandeja de salida de su programa cliente de correo electrónico puede encontrar el correo electrónico bloqueado. Para enviar el correo electrónico bloqueado, vuelva a iniciar el envío del correo electrónico después de haber completado la configuración.

5.11 Web Protection

Si Web Protection detecta virus, se emite un mensaje de advertencia si ha seleccionado como modo de acción para los virus detectados el modo *interactivo* o el modo *automático* con la opción **Mostrar mensaje de advertencia** (véase la sección sobre configuración Web Protection > Análisis > Acción al detectar). En el modo interactivo puede seleccionar en el cuadro de diálogo qué debe hacerse con los datos transmitidos por el servidor web. En el modo automático con mensaje de advertencia, no existe ninguna posibilidad de selección para el tratamiento de la detección de los virus. En el mensaje puede confirmar la acción que debe realizarse automáticamente o interrumpir Web Protection.

Nota
El cuadro de diálogo abajo mostrado es un mensaje acerca de la detección de virus en el modo interactivo.

Mensaje de advertencia



Detección, Error, Advertencias

En las pestañas **Detección**, **Error** y **Advertencias** se muestran mensajes e información detallada sobre las detecciones de virus:

- **Detección:** URL y nombre del virus encontrado o el programa no deseado.
- **Error:** mensajes sobre los errores que se han producido durante la comprobación por parte de Web Protection.
- **Advertencias:** mensajes de advertencia que se refieren a los virus detectados.

Acciones posibles

Nota
Si en la detección se ha empleado una técnica heurística (HEUR/), una utilidad de compresión poco habitual (PCK/) o un fichero con una extensión oculta (HEUR-DBLEXT/), en el modo interactivo solo están disponibles las opciones Mover a cuarentena y Omitir. En el modo automático la detección se mueve automáticamente a la cuarentena.
Esta limitación impide que los archivos encontrados que podrían ser una falsa alarma se quiten (eliminen) directamente de su ordenador. El fichero puede recuperarse en cualquier momento usando el Administrador de cuarentenas.
En función de la configuración pueden no estar disponibles diferentes opciones.

Denegar acceso

El sitio web requerido por el servidor web y los datos solicitados no son transferidos a su navegador. Un error de acceso denegado ha sido mostrado en su navegador web. Web Protection registra la detección en el fichero de informe si está activada la función de informes.

Aislar (poner en cuarentena)

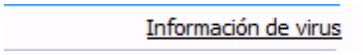
La página web solicitada por el servidor Web o los datos y los ficheros transmitidos no se envían a la cuarentena si se detectan virus o malware. El gestor de cuarentena puede recuperar el fichero afectado si tiene valor informativo o, en caso necesario, enviarlo al Avira Malware Research Center.

Omitir

La página web solicitada por el servidor web o los datos y ficheros transmitidos se pasan por Web Protection a su navegador.

Advertencia
Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. Seleccione la opción **Omitir** solo en casos excepcionales justificados.

Botones y enlaces

Botón/Enlace	Descripción
	Mediante este enlace accede, si hay una conexión a Internet activa, a una página con información adicional sobre este virus o programa no deseado.
	Por medio de este botón o enlace se abre esta página de la ayuda en pantalla.

6. Scanner

6.1 Scanner

Con el módulo Scanner puede llevar a cabo búsquedas selectivas de virus y programas no deseados (búsqueda directa). Dispone de las siguientes opciones para rastrear archivos afectados:

- **Búsqueda directa a través del menú contextual**
  Se recomienda la búsqueda directa a través del menú contextual (botón derecho del ratón, opción **Analizar ficheros seleccionados con Avira**) cuando, por ejemplo, desee analizar archivos y carpetas individuales en Windows Explorer. Otra de las ventajas de este tipo de búsqueda directa es que no es necesario abrir previamente el centro de control.
- **Análisis directo con arrastrar y soltar**
  Tras arrastrar un archivo o un directorio a la ventana del programa del Centro de control, Scanner los analiza, incluidos todos los eventuales subdirectorios. Se recomienda proceder de esta manera si se desea analizar archivos o directorios individuales que estén situados, por ejemplo, en el escritorio.
- **Búsqueda directa a través de un perfil**
  Se recomienda este procedimiento si desea analizar regularmente determinados directorios y unidades (p. ej., su directorio de trabajo o unidades en las que guarda nuevos archivos con regularidad). No es necesario que seleccione estos directorios y unidades para cada análisis, sino que puede realizar la selección cómodamente a través del perfil correspondiente.
- **Búsqueda directa mediante el programador**
  El programador le permite llevar a cabo tareas de análisis con períodos temporales preestablecidos.

Para buscar rootkits, virus del sector de arranque y procesos activos, es necesario aplicar procedimientos específicos. Dispone de las opciones siguientes:

- Búsqueda de rootkits mediante el perfil de búsqueda **Búsqueda de rootkits y Malware activo**
- Búsqueda de procesos activos mediante el perfil de búsqueda **Procesos activos**
- Búsqueda de virus del sector de arranque a través de la opción **Analizar sectores de arranque** en el menú **Extras**

6.2 Luke Filewalker

Durante la búsqueda directa se muestra la ventana de estado **Luke Filewalker**, que informa con detalle del progreso del análisis.

Si en la configuración de Scanner, en el grupo **Acción al detectar**, se ha seleccionado la opción **Interactivo**, cuando se produzca la detección de un virus o un programa no deseado, se le preguntará qué es lo que desea que se haga con él. Si está seleccionada la opción **Automático**, las eventuales detecciones se visualizarán en el informe de Scanner.

Una vez concluida la búsqueda, los resultados de la misma (estadísticas), así como los mensajes de error y advertencia, se mostrarán en otra ventana de diálogo.

6.2.1 Luke Filewalker: Ventana de estado de la búsqueda

Información mostrada

Estado: Existen diversos mensajes de estado:

- *Se inicializa el programa*
- *Se está analizando la existencia de objetos ocultos*
- *Analizando los procesos iniciados*
- *Analizando el fichero*
- *Inicializando archivo*
- *Liberar memoria*

- *Descomprimiendo el fichero*
- *Analizando sectores de arranque*
- *Analizando sectores de arranque maestros*
- *Analizando el registro*
- *El programa se cerrará*
- *El análisis ha finalizado*

Último objeto: Nombre y ruta del fichero que se está analizando en este momento o del último que se analizó

Última detección: Existen diversos tipos de mensajes para la última detección:

- *No se han encontrado virus*
- Nombre del último virus o programa no deseado que se ha encontrado

Ficheros analizados: Número de ficheros analizados

Directorios analizados: Número de directorios analizados

Archivos analizados: Número de archivos analizados

Tiempo requerido: Duración de la búsqueda directa

Analizado hasta el momento: Porcentaje del proceso de búsqueda que ya se ha realizado

Detecciones: Número de virus y programas no deseados detectados

Ficheros sospechosos: Número de ficheros notificados por la heurística

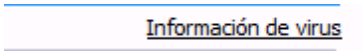
Advertencias: Número de mensajes de advertencia para detecciones de virus

Objetos analizados: Número de objetos analizados durante la búsqueda de rootkits

Objetos ocultos: Número total de objetos ocultos encontrados

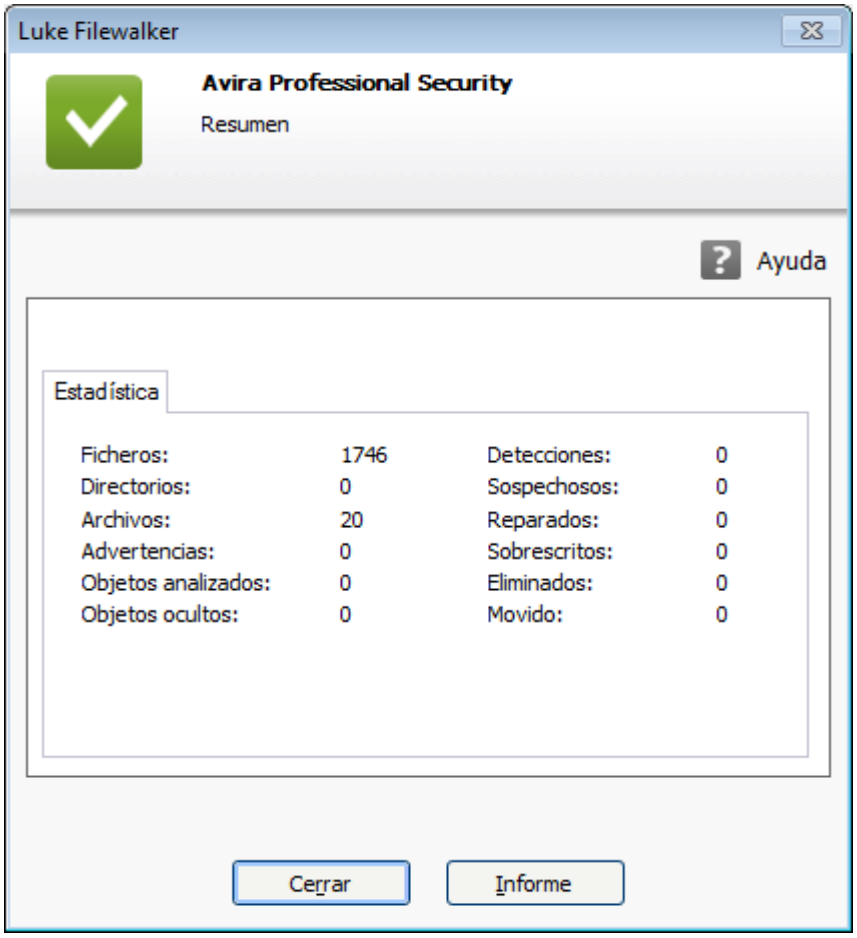
Nota
Los rootkits tienen la propiedad de ocultar procesos u objetos como entradas de registro o ficheros, sin embargo, no todos los objetos ocultos son forzosamente un indicio de la existencia de un rootkit. En el caso de objetos ocultos, también puede tratarse de objetos inofensivos. Si durante la búsqueda se han encontrado objetos ocultos y no existan mensajes de advertencia de detección de virus, debería averiguar a partir del informe de qué objetos se trata y extraer más información sobre los objetos encontrados.

Botones y enlaces

Botón/Enlace	Descripción
	Mediante este enlace accede, si hay una conexión a Internet activa, a una página con información adicional sobre este virus o programa no deseado.
	Se abre esta página de la ayuda en línea.
Detener	Se detiene la búsqueda.
Pausa	La búsqueda se interrumpe momentáneamente y prosigue tras pulsar el botón **Continuar**.
Continuar	La búsqueda interrumpida prosigue.
Finalizar	Se cierra Scanner.

Informe	Se muestra el fichero del informe de la búsqueda.

6.2.2 Luke Filewalker: Estadísticas de la búsqueda



Información que se muestra: estadísticas

Ficheros: Número de ficheros analizados

Directorios: Número de directorios analizados

Archivos: Número de archivos analizados

Advertencias: Número de mensajes de advertencia para detecciones de virus

Objetos analizados: Número de objetos analizados durante la búsqueda de rootkits

Objetos ocultos: Número de objetos ocultos encontrados (rootkits)

Detecciones: Número de virus y programas no deseados detectados

Sospechosos: Número de ficheros notificados por la heurística

Reparados: Número de ficheros reparados

Sobrescritos: Número de ficheros sobrescritos

Eliminados: Número de ficheros eliminados

Movidos: Número de ficheros movidos a cuarentena

Botones y enlaces

Botón/Enlace	Descripción
	Se abre esta página de la ayuda en línea.
Cerrar	Se cierra la ventana del resumen.
Informe	Se muestra el fichero del informe de la búsqueda.

7. Centro de control

7.1 Información general

El Centro de control es un centro de información, configuración y administración. Además delas diversas secciones que puede elegir, ofrece una variedad de opciones que puede seleccionar por medio de la barra de menú.

Barra de menú

En la barra de menú encuentra las siguientes funciones:

Fichero

- Finalizar (Alt+F4)

Vista

- Estado
- Seguridad del PC
  - Scanner
  - Real-Time Protection
- Seguridad en Internet
  - FireWall
  - Web Protection
  - Mail Protection
- Administración
  - Cuarentena
  - Programador
  - Informes
  - Eventos
- Actualizar (F5)

Extras

- Analizar sectores de arranque...
- Lista de detecciones...
- Descargar CD de rescate
- Configuración (F8)

Actualización

- Iniciar actualización...
- Actualización manual...

Ayuda

- Temas
- Ayúdame
- Descargar manual
- Cargar fichero de licencia...
- Enviar feedback
- Acerca de Avira Professional Security

> **Nota**
> La exploración usando el teclado de la barra de menús se activa con la tecla [**Alt**]. Si está activada la exploración, puede desplazarse por el menú usando las teclas de flecha. Con la tecla Intro se activa la opción de menú seleccionada en ese momento.

Secciones

En la barra de menú izquierda encuentra las siguientes secciones:

- Estado

SEGURIDAD DEL PC

- Scanner
- Real-Time Protection

SEGURIDAD EN INTERNET

- FireWall
- Web Protection
- Mail Protection

ADMINISTRACIÓN

- Cuarentena
- Programador
- Informes
- Eventos

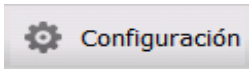
Descripción de las secciones

- **Estado**: en la pantalla de arranque **Estado** encontrará todas las secciones con las que puede supervisar la funcionalidad del producto Avira (consulte Estado).
  - La ventana **Estado** ofrece la posibilidad de ver de un solo vistazo qué módulos están activos y aporta información sobre la última actualización realizada.
- *SEGURIDAD DEL PC*: Aquí encontrará los componentes con los que se analizan los ficheros del sistema informático para detectar la existencia de virus o software malintencionado (malware).
  - La sección **Scanner** permite configurar o iniciar de forma sencilla el análisis directo (consulte Scanner). Los perfiles predefinidos permiten llevar a cabo un análisis con opciones predeterminadas ya adaptadas. Del mismo modo, con ayuda de la selección manual (que se guarda) o con la creación de perfiles definidos por el usuario, es posible adaptar el análisis de detección de virus y programas no deseados a sus propias necesidades.
  - La sección Real-Time Protection muestra información sobre los ficheros comprobados, así como datos estadísticos que pueden restablecerse en cualquier momento, y permite abrir el fichero de informe. Prácticamente con solo pulsar un botón, puede obtener información detallada sobre el último virus o programa no deseado que se haya detectado.
- *SEGURIDAD EN INTERNET*: Aquí encontrará encontrará los componentes con los que se protege el sistema informático frente a virus y malware de Internet, así como frente a los accesos no deseados a la red.
  - La sección **FireWall** le ofrece la posibilidad de establecer la configuración básica del Firewall. Además, se muestran la velocidad de transmisión de datos actual y todas las aplicaciones activas que utilizan una conexión de red (consulte FireWall).
  - La sección Web Protection muestra la información relativa a las direcciones URL comprobadas y a los virus detectados, así como datos estadísticos que pueden restablecerse en cualquier momento, y permite abrir el fichero de informe. Prácticamente con solo pulsar un botón, puede obtener información detallada sobre el último virus o programa no deseado que se haya detectado.
  - La sección **Mail Protection** muestra los correos electrónicos analizados, sus propiedades y otros datos estadísticos. Además, tiene la posibilidad de excluir direcciones de correo electrónico debe excluir en el futuro del análisis de spam y malware. También puede eliminar los emails de la memoria caché de Mail Protection. (consulte Mail Protection).
- *ADMINISTRACIÓN*: Aquí encontrará las herramientas con las que puede aislar y administrar ficheros sospechosos o infectados por virus, así como programar tareas periódicas.
  - En la sección **Cuarentena** se encuentra el denominado Gestor de cuarentena. Es el elemento central para ficheros ya puestos en cuarentena o para ficheros sospechosos que se quieren poner en cuarentena (consulte Cuarentena). Además, existe la posibilidad de enviar un determinado fichero por correo electrónico al Avira Malware Research Center.

- La sección **Programador** permite crear tareas de análisis y actualización, así como tareas de backup programadas, y adaptar o eliminar tareas existentes (consulte Programador).
- La sección **Informes** ofrece la posibilidad de consultar los resultados de las acciones realizadas (consulte Informes).
- La sección **Eventos** ofrece la posibilidad de informarse sobre los eventos que generan los módulos del programa (consulte Eventos).

Botones y enlaces

Existen disponibles los siguientes botones y vínculos.

Botón/Vínculo	Comando de teclas	Descripción
		Se abre el cuadro de diálogo de configuración de la sección.
	F1	Se abre el tema de ayuda en pantalla de la sección.

7.2 Fichero

7.2.1 Finalizar

La opción de menú **Finalizar** del menú **Fichero** cierra el Centro de control.

7.3 Vista

7.3.1 Estado

La pantalla de arranque del Centro de control **Estado** ofrece la posibilidad de ver de una sola mirada si el sistema informático está protegido y qué módulos de Avira están activos. Además, la ventana **Estado** ofrece información sobre la última actualización realizada. Además, se ve si dispone de una licencia válida.

- Seguridad del PC: Real-Time Protection, Último análisis, Última actualización, Su producto está activado
- Seguridad en Internet: Web Protection, Mail Protection, FireWall, Modo de presentación,

> **Nota**
> El control de cuentas de usuarios (UAC) precisa su aprobación para la

activación o desactivación de los servicios Real-Time Protection, FireWall, Web Protection así como Mail Protection en sistemas operativos a partir de Windows Vista.

Seguridad del PC

En esta área recibe información sobre el estado actual de los servicios y las funciones de protección que defienden su sistema local frente a virus y programas no deseados.

Real-Time Protection

En esta área se le muestra información acerca del estado actual de Real-Time Protection.

Puede activar y desactivar Real-Time Protection con el botón **Conectado/Desconectado**. Para más opciones relacionadas con Real-Time Protection, haga clic en la barra de exploración **Real-Time Protection**. Primero recibirá informaciones de estado sobre el último malware detectado y los ficheros infectados. Haga clic en **Configuración** para efectuar configuraciones adicionales.

- **Configuración**: Accede a la configuración donde podrá efectuar configuraciones para los componentes del módulo Real-Time Protection.

Existen las siguientes posibilidades:

Icono	Estado	Opción	Descripción
	*Activado*	**Desactivar**	El servicio Real-Time Protection está activo, es decir, su sistema se encuentra constantemente monitorizado buscando virus o programas no deseados. **Nota** Puede desactivar el servicio Real-Time Protection. Aun así, recuerde que cuando Real-Time Protection está desactivado, ya no está protegido contra virus o programas no deseados. Cualquier fichero puede colarse en el sistema sin previo aviso y es susceptible de causar daños.
	*Desactivado*	**Activar**	El servicio Real-Time Protection está desactivado, es decir, se ha cargado en memoria, pero no está activo. **Nota** No se realiza ningún análisis en busca de virus ni malware. Cualquier fichero puede entrar en el sistema sin previo aviso. No está protegido contra virus o programas no deseados. **Nota** Para estar de nuevo protegido frente a virus y programas no deseados, pulse el botón **Conectado/Desconectado** al lado de Real-Time Protection en el área de Seguridad del PC de la ventana de estado.

	*Servicio detenido*	**Iniciar**	El servicio Real-Time Protection está detenido. **Nota** No se realiza ningún análisis en busca de virus ni malware. Cualquier fichero puede entrar en el sistema sin previo aviso. No está protegido contra virus o programas no deseados. **Nota** Para estar de nuevo protegido frente a virus y programas no deseados, pulse el botón **Conectado/Desconectado**. El estado actual debería indicar ahora *Activado*.
	Desconocido	**Ayuda**	Este estado se muestra cuando ocurre algún problema desconocido. En ese caso, póngase en contacto con nuestro soporte.

Último análisis

En esta área recibe la información sobre el último análisis del sistema. En caso de un análisis completo del sistema se analizan todos los discos duros de su equipo de manera exhaustiva. Durante el análisis se emplean todos los procedimientos de análisis y comprobación con excepción de la comprobación de la integridad de los ficheros del sistema: Análisis estándar de ficheros, comprobación de registro y sectores de arranque, búsqueda de rootkits y malware activo, etc.

Se muestran los siguientes detalles:

- Fecha del último análisis completo

Existen las siguientes posibilidades:

Análisis del sistema	Opción	Descripción
No realizado	**Analizar el sistema**	No se ha realizado un análisis completo del sistema desde la instalación. **Advertencia** El estado del sistema no se ha analizado. Existe la posibilidad de que su equipo contenga virus o programas no deseados. **Nota** Para analizar el equipo haga clic en el botón Analizar el sistema.
Fecha del último análisis completo, p. ej. *18/09/2011*	**Analizar el sistema**	Ha ejecutado un análisis completo del sistema en la fecha indicada. **Nota** Se recomienda la utilización de la tarea de análisis creada por defecto *Análisis completo del sistema*: Active la tarea de análisis Análisis completo del sistema en el programador.
Desconocido	**Ayuda**	Este estado se muestra cuando ocurre algún problema desconocido. En ese caso, póngase en contacto con nuestro soporte.

Última actualización

El estado de la última actualización lo recibe en este cuadro.

Se muestran los siguientes detalles:

- fecha de la última actualización
  - Haga clic en el botón Configuración para efectuar configuraciones adicionales para la actualización automática.

Existen las siguientes posibilidades:

Icono	Estado	Opción	Descripción
	Fecha de la última actualización. P. ej.: *18/07/2011*	**Iniciar actualización**	El programa se ha actualizado en las últimas 24 horas. **Nota** El botón Iniciar actualización permite actualizar su producto Avira a la versión más reciente.
	Fecha de la última actualización. P. ej.: *15/07/2011*	**Iniciar actualización**	Desde la actualización ya han transcurrido 24 horas, pero todavía se encuentra en el ciclo de recordatorio de actualización seleccionado. Este depende de los parámetros de la Configuración. **Nota** El botón Iniciar actualización permite actualizar su producto Avira a la versión más reciente.

	*No realizado*	**Iniciar actualización**	Desde la instalación, todavía no se ha realizado ninguna actualización o bien se ha sobrepasado el ciclo de recordatorio de actualización elegido (consulte Configuración) y no se realizó ninguna actualización o bien el fichero de firmas de virus es anterior al ciclo de recordatorio de actualización seleccionado (consulte Configuración). **Nota** El botón **Iniciar actualización** permite actualizar su producto Avira a la versión más reciente.
		No disponible	Con la licencia caducada no es posible realizar actualizaciones.

Su producto está activado

El estado de la licencia del producto se muestra en este cuadro.

Existen las siguientes posibilidades:

Versión completa

Icono	Estado	Opción	Descripción
	Fecha de validez de la licencia actual para una versión completa, p. ej.: *31/10/2011*	**Renovar**	Dispone de una licencia válida para su producto Avira. A través del botón Renovar se accede a la tienda online de Avira. En ella se puede adaptar la licencia actual a cada necesidad y llevar a cabo una actualización a una versión superior de Avira Premium.
	Fecha de validez de la licencia actual para una versión completa, p. ej.: *31/10/2011*	**Renovar**	Dispone de una licencia válida para su producto Avira. Sin embargo, al período de licencia solo le quedan 30 días o menos. Al pulsar el botón **Renovar** se accede a la tienda online de Avira. En ella se puede prolongar la licencia actual.
	Fecha de caducidad de la licencia: p. ej. *31/08/2011*	**Comprar**	Su licencia para el producto Avira ha caducado. Al pulsar el botón **Comprar**, se accede a la tienda online de Avira. En ella se puede adquirir una licencia nueva. **Advertencia** Si la licencia ha caducado, ya no es posible realizar actualizaciones. Las funciones de protección del programa están desactivadas y ya no se pueden activar.

Licencia de evaluación

Icono	Estado	Opción	Descripción
	Fecha de validez de la licencia de evaluación, p. ej. *31/10/2011*	**Comprar**	Dispone de una licencia de evaluación que permite probar todas las funciones del producto Avira durante un tiempo determinado. Al pulsar el botón **Comprar**, se accede a la tienda online de Avira. En ella se puede adquirir una licencia nueva.
	Fecha de validez de la licencia de evaluación, p. ej. *31/10/2011*	**Renovar**	Dispone de una licencia de evaluación. Sin embargo, al período de licencia solo le quedan 30 días o menos. Al pulsar el botón **Renovar** se accede a la tienda online de Avira. En ella se puede adquirir una licencia nueva.
	Fecha de caducidad de la licencia de evaluación: *31/08/2011*	**Comprar**	Su licencia para el producto Avira ha caducado. Al pulsar el botón **Comprar**, se accede a la tienda online de Avira. En ella se puede adquirir una licencia nueva. **Advertencia** Si la licencia ha caducado, ya no es posible realizar actualizaciones. Las funciones de protección del programa están desactivadas y ya no se pueden activar.

Seguridad en Internet

En esta área recibe información sobre el actual estado de los servicios que defienden su sistema frente a virus y programas no deseados.

- **FireWall**: el servicio controla las vías de comunicación hacia su equipo y desde el mismo.
- **Web Protection**: el servicio analiza los datos que se transmiten al navegar por Internet y se cargan en el explorador web (supervisión de los puertos 80, 8080, 3128).
- **Mail Protection**: El servicio analiza emails y sus datos adjuntos para detectar virus y malware.

- **Modo de presentación**: Si la opción está activada, su producto Avira cambia automáticamente al modo de presentación cuando en el equipo se ejecuta una aplicación a pantalla completa.

Se visualizan opciones adicionales de los servicios en un menú contextual cuando se hace clic en el botón **Configuración** junto a **Conectado/Desconectado**:

- **Configuración**: Accede a la configuración donde podrá efectuar configuraciones para los componentes del servicio.

Existen las siguientes posibilidades: *Servicios*

Icono	Estado	Estado del servicio	Opción	Descripción
	*Aceptar*	Activado	**Desactivar**	Todos los servicios de Seguridad en Internet están activos. **Nota** Puede desactivar un servicio pulsando el botón **CONECTADO/DESCONECTADO**. No obstante, tenga en cuenta que con un servicio desactivado ya no estará protegido completamente contra virus y malware.
	*Limitado*	Desactivado	**Activar**	El servicio está desactivado, es decir, el servicio se ha iniciado pero no está activo. **Advertencia** Su equipo no está completamente monitorizado. Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. **Nota** Para activar el servicio, pulse el botón **Conectado/Desconectado** junto al servicio correspondiente.

	Advertencia	Servicio detenido	**Iniciar**	Se detuvo un servicio. **Advertencia** Su equipo no está completamente monitorizado. Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. **Nota** Haga clic en el botón **CONECTADO/DESCONECTADO** para arrancar el servicio y para que su sistema sea monitorizado. El servicio se inicia y se activa.
		Desconocido	**Ayuda**	Este estado se muestra cuando ocurre algún problema desconocido. En ese caso, póngase en contacto con nuestro soporte.

7.3.2 Modo de presentación

Cuando ejecuta aplicaciones en su equipo que requieren una aplicación a pantalla completa, puede cancelar directamente mensajes de sobremesa e información como ventanas emergentes y notificaciones de productos mediante la activación del modo de presentación. En el modo de presentación se aplican todas las reglas definidas de adaptador y aplicación que ha configurado en Avira FireWall sin que se le notifiquen eventos de red.

Tiene la posibilidad de activar el modo de presentación con un clic sobre el botón **CONECTADO/DESCONECTADO** o de mantener el modo automático. El modo de presentación está preseleccionado con **Automático** y se representa en color verde. Con esta preselección, su producto Avira cambia automáticamente al modo de presentación cuando ejecuta una aplicación a pantalla completa.

- Haga clic en el botón situado a la izquierda junto a **DESCONECTADO** para activar el modo de presentación.
  - ↪ El modo de presentación está conectado y el botón se representa en color amarillo.

Nota
Recomendamos modificar solo temporalmente el estado preseleccionado **DESCONECTADO** con su detección automática de aplicaciones a modo de pantalla completa, ya que no se recibe en el modo de presentación mensajes de sobremesa y advertencias sobre accesos a la red y peligros eventuales claramente visibles.

7.3.3 Scanner

La sección **Scanner** permite configurar o iniciar de forma sencilla el análisis directo, es decir, del análisis a petición. Los perfiles predefinidos permiten llevar a cabo un análisis con opciones predeterminadas ya adaptadas. Del mismo modo, con ayuda de la selección manual o con la creación de perfiles definidos por el usuario, es posible adaptar el análisis de detección de virus y programas no deseados a sus propias necesidades. La acción requerida puede seleccionarse con el icono en la barra de herramientas, mediante comando de teclado o a través del menú contextual. Los análisis se inician mediante la opción Iniciar análisis con el perfil seleccionado.

El aspecto y el uso de los perfiles editables son similares a los del Explorador de Windows. Cada carpeta del directorio principal corresponde a un perfil. Las carpetas o ficheros para analizar llevan una marca de verificación delante de la carpeta o del fichero que se analizará, o bien se les puede añadir la marca.

- Para navegar por las carpetas, hacer doble clic sobre ellas.
- Para cambiar de disco, hacer doble clic sobre su letra.
- Para seleccionar carpetas y unidades, haga clic en la casilla delante del icono de carpeta o unidad o realice la selección por medio del menú contextual.
- Puede navegar por la estructura de menús con la ayuda de la barra y fechas de desplazamiento.

Perfiles predefinidos

Para el análisis dispone de perfiles predefinidos.

Nota
Estos perfiles únicamente son de lectura, no pueden ser alterados ni borrados. Para adaptar un perfil a sus necesidades, seleccione en el caso de un análisis único la carpeta Selección manual o bien Crear nuevo perfil para crear un perfil definido por el usuario, que se puede guardar.

Nota
Las opciones de búsqueda de los perfiles predefinidos pueden configurarse en Configuración > Scanner > Análisis > Ficheros. Puede adaptar estos parámetros a sus necesidades.

Unidades locales

Se analizan todas las unidades locales del sistema para detectar virus o programas no deseados.

Discos duros locales

Se analizan todos los discos duros locales del sistema para detectar virus o programas no deseados.

Unidades extraíbles

Se analizan todas las unidades extraíbles disponibles para detectar virus o programas no deseados.

Directorio de sistema de Windows

Se analiza el directorio de sistema de Windows de su sistema para detectar virus o programas no deseados.

Análisis completo del sistema

Se analizan todos los discos duros locales del equipo para detectar virus o programas no deseados. Durante el análisis se emplean todos los procedimientos de análisis y comprobación con excepción de la comprobación de la integridad de los ficheros del sistema: Análisis estándar de ficheros, comprobación de registro y sectores de arranque, búsqueda de rootkits y malware activo, etc. (consulte Scanner > Información general). Los procedimientos de análisis se ejecutan independientemente de la configuración de Scanner en la configuración en Scanner > Análisis: Configuración adicional.

Análisis rápido del sistema

Se inicia una búsqueda de virus y programas no deseados en las carpetas más importantes del sistema (directorios *Windows*, *Archivos de programa*, *Documents and Settings\Default User*, *Documents and Settings\All Users*).

Mis documentos

La carpeta estándar "*Mis Documentos*" del usuario que inició sesión se analiza en busca de virus y programas no deseados.

Nota
En Windows, "*Mis documentos*" es un directorio en el perfil del usuario que se utiliza como ubicación estándar para guardar documentos. En la configuración estándar, el directorio se encuentra en *C:\Documents and Settings\[Nombre de usuario]\Mis documentos*.

Procesos activos

Todos los procesos activos se analizan en busca de virus y programas no deseados.

Búsqueda de rootkits y malware activo

Se analiza la existencia de rootkits y programas dañinos activos (en ejecución) en el equipo. Se analizan todos los procesos activos.

Nota
En el modo interactivo tiene varias posibilidades para decidir cómo proceder con la detección. En el modo automático, la detección se almacena en el fichero de informe.

Nota
En Windows XP 64 Bit , el análisis de rootkits no está disponible.

7.3.4 Selección manual

Seleccione esta carpeta si desea adaptar el análisis a sus necesidades. Marque los directorios y ficheros que desee analizar.Si su producto Avira se administra vía Avira Management Console, puede introducir en el campo **Selección manual** en **Comandos** varios directorios separados por "?" (p. ej.: `c:\temp?d:\test`).

Nota
El perfil **Selección manual** se utiliza para analizar sin tener que crear un nuevo perfil.

Perfiles definidos por el usuario

La creación de un perfil nuevo se puede hacer por medio de la barra de herramientas, mediante comando de teclado o a través del menú contextual.

Puede guardar los perfiles nuevos con el nombre que desee, y también utilizarlos en el análisis controlado manualmente para la generación de análisis periódicos con el programador.

Barra de herramientas y comandos de teclado

Icono	Comando de teclas	Descripción
	**F3**	**Iniciar búsqueda con el perfil seleccionado** Se analiza el perfil seleccionado para detectar virus o programas no deseados.
	**F6**	**Iniciar análisis con el perfil seleccionado como administrador** Se analiza el perfil seleccionado con derechos administrativos.
	**Insertar**	**Crear perfil nuevo** Se crea un perfil nuevo.
	**F2**	**Renombrar perfil seleccionado** Da un nombre al perfil seleccionado.
	**F4**	**Crear vínculo en el escritorio para el perfil seleccionado** Crea un acceso directo (enlace) en el escritorio para ese perfil.
	**Eliminar**	**Eliminar perfil seleccionado** El perfil seleccionado se elimina definitivamente.

Menú contextual

Para acceder al menú contextual de esta sección, seleccione un determinado perfil con el ratón y mantenga pulsado el botón derecho del ratón.

Iniciar análisis

Se analiza el perfil seleccionado para detectar virus o programas no deseados.

Iniciar análisis (Administrador)

(Esta función solo está disponible a partir de Windows Vista. Necesita derechos de administrador para realizar esta acción.)

Se analiza el perfil seleccionado para detectar virus o programas no deseados.

Crear perfil nuevo

Se crea un perfil nuevo. Seleccione los directorios y ficheros que se deben analizar.

Cambiar nombre de perfil

Da un nombre al perfil seleccionado.

> **Nota**
> Esta entrada no se puede seleccionar en el menú contextual si ha seleccionado un perfil predefinido.

Eliminar perfil

El perfil seleccionado se elimina definitivamente.

> **Nota**
> Esta entrada no se puede seleccionar en el menú contextual si ha seleccionado un perfil predefinido.

Filtro de ficheros

Predeterminado:

Significa que los ficheros se analizarán según los parámetros del grupo Ficheros de la configuración. Puede adaptar esta configuración a sus necesidades. Para acceder a esta, haga clic en el botón o en el enlace Configuración.

Analizar todos los ficheros:

Se analizan todos los ficheros, independientemente de los parámetros de la configuración.

Definido por el usuario:

Se abre un cuadro de diálogo que muestra todas las extensiones de fichero que se analizarán durante un análisis. Se definen entradas de forma estándar para las extensiones. Aquí se pueden añadir y quitar entradas.

> **Nota**
> Esta entrada solo puede seleccionarse en el menú contextual cuando el ratón se pasa por encima de la casilla de marcado.
> Esta opción no está disponible en los perfiles predefinidos.

Seleccionar

Con subdirectorios:

Se analiza todo lo que haya en el nodo seleccionado (marca de color negro).

Sin subdirectorios:

Solo se analizan los ficheros del nodo seleccionado (marca verde).

Solo subdirectorios:

Solo se analizan los subdirectorios en el nodo seleccionado, pero no los ficheros (marca gris y los subdirectorios tienen una marca en negro).

Sin selección:

La selección se cancela y no se analiza el nodo (sin marca).

Nota
Esta entrada solo puede seleccionarse en el menú contextual cuando el ratón se pasa por encima de la casilla de marcado.
Esta opción no está disponible en los perfiles predefinidos.

Crear acceso directo en el escritorio

Crea un acceso directo (enlace) en el escritorio para ese perfil.

Nota
Esta entrada no se puede seleccionar en el menú contextual si ha seleccionado el perfil Selección manual, ya que la configuración de la selección manual no se guarda permanentemente.

7.3.5 Real-Time Protection

La sección **Real-Time Protection** muestra información sobre los ficheros comprobados, así como datos estadísticos que pueden restablecerse en cualquier momento, y además permite abrir el fichero de informe. Prácticamente con solo pulsar un botón, puede obtener información detallada sobre el último virus o programa no deseado que se haya detectado.

Nota
Si no se ha iniciado el servicio de Real-Time Protection, el botón al lado del módulo se representa en color amarillo. También tiene la opción de mostrar el fichero de informe de Real-Time Protection.

Barra de herramientas

Icono	Descripción
	Mostrar fichero de informe Se muestra el fichero de informe de Real-Time Protection.
	Restablecer estadísticas La información estadística de esta sección se restablece.

Información mostrada

Último fichero infectado

Muestra el nombre y la ubicación del último fichero encontrado por Real-Time Protection.

Último malware detectado

Nombre del último virus o programa no deseado que se ha encontrado.

Icono	Descripción
Información de virus	Si existe conexión con Internet, puede pulsar en el icono o en el enlace para mostrar información detallada sobre el virus o programa no deseado.

Último fichero analizado

Muestra el nombre y la ruta del último fichero analizado por Real-Time Protection.

Estadísticas

Número de ficheros

Muestra el número de ficheros analizados hasta el momento.

Número de malware encontrados

Muestra el número de virus y programas no deseados detectados hasta el momento.

Número de ficheros sospechosos

Muestra el número de ficheros notificados por la heurística.

Número de ficheros eliminados

Muestra el número de ficheros borrados hasta el momento.

Número de ficheros reparados

Muestra el número de ficheros reparados hasta el momento.

Números de ficheros movidos

Muestra el número de ficheros movidos hasta el momento.

Número de ficheros a los que se cambió el nombre

Muestra el número de ficheros renombrados hasta el momento.

7.3.6 FireWall

Avira FireWall (sólo Avira Professional Security)

En la sección FireWall, se muestran la velocidad de transmisión de datos actual y todas las aplicaciones activas que utilizan una conexión de red. Esta sección también le permite configurar los parámetros básicos de Avira FireWall: con el control deslizante puede configurar el nivel de seguridad. Para configurar un nivel de seguridad personalizado, debe cambiar a Configuración.

Barra de herramientas

Icono	Descripción
	**Restablecer estadísticas** La información estadística de esta sección se restablece.

Nivel de seguridad

Puede elegir entre las siguientes configuraciones de seguridad:

> **Nota**
> Puede modificar el nivel de seguridad moviendo simplemente el control deslizante a otro valor de la escala de seguridad. El nivel de seguridad seleccionado queda activado inmediatamente. Encontrará más información sobre este tema en el menú de configuración de FireWall: Reglas del adaptador

Bajo

Se detecta el desbordamiento y el escaneo de puertos.

Medio

Se descartan los paquetes TCP y UDP sospechosos.

Se impide el desbordamiento y el escaneo de puertos.

(Configuración predeterminada)

Alto

El equipo es invisible en la red.

No se permiten nuevas conexiones exteriores.

Se impide el desbordamiento y el escaneo de puertos.

Usuario

Reglas definidas por el usuario

Bloquear todos

Finaliza todas las conexiones de red existentes.

Transferencia de datos

En esta sección, se muestra información relativa al tráfico de datos actual que se envía (*Carga*) y que se recibe (*Descarga*). El valor máximo se indica en la esquina superior izquierda del gráfico.

Los paquetes entrantes se representan en rojo, los salientes, en verde. El área en la que se solapan estas dos indicaciones es de color gris.

FireWall de Windows (a partir de Windows 7)

A partir de Windows 7 tiene la opción de gestionar el FireWall de Windows mediante el Centro de control y la configuración.

La sección FireWall le ofrece la posibilidad de comprobar el estado del FireWall de Windows y restaurar la configuración recomendada haciendo clic en el botón **Solucionar problema**.

7.3.7 Web Protection

La sección **Web Protection** muestra la información relativa a las direcciones URL comprobadas y a los virus detectados, así como datos estadísticos que pueden restablecerse en cualquier momento, y permite abrir el fichero de informe. Prácticamente con solo pulsar un botón, puede obtener información detallada sobre el último virus o programa no deseado que se haya detectado.

Barra de herramientas

Icono	Descripción
	**Mostrar fichero de informe** Se muestra el fichero de informe de Web Protection.
	**Restablecer estadísticas** La información estadística de esta sección se restablece.

Información mostrada

Última URL afectada

Muestra la última URL encontrada por Web Protection.

Último virus o programa no deseado detectado

Nombre del último virus o programa no deseado que se ha encontrado.

Icono/enlace	Descripción
	Si existe conexión con Internet, puede pulsar en el icono o en el enlace para mostrar información detallada sobre el virus o programa no deseado.

Última URL analizada

Muestra el nombre y la localización del último fichero analizado por Web Protection.

Estadísticas

Número de URL analizadas

Muestra el número de direcciones URL analizadas hasta ahora.

Número de detecciones

Muestra el número de virus y programas no deseados detectados hasta el momento.

Número de direcciones URL bloqueadas

Muestra el número de direcciones URL bloqueadas hasta ahora.

Número de direcciones URL omitidas

Muestra el número de direcciones URL omitidas hasta ahora.

7.3.8 Mail Protection

La sección **Mail Protection** muestra los correos electrónicos analizados por Mail Protection, sus propiedades y otros datos estadísticos.

Nota
Si no se ha iniciado el servicio de Mail Protection, el botón situado junto al módulo se representa en color amarillo. No obstante, también tiene la opción de mostrar el fichero de informe de Mail Protection. Si en su producto Avira no está disponible este servicio, el botón estará atenuado.

Nota
Por supuesto, la exclusión de determinadas direcciones de email del análisis de malware se refiere únicamente a los emails entrantes. Para desconectar el análisis de los emails salientes, desactive esta opción en la configuración, en Mail Protection > Análisis.

Barra de herramientas

Icono	Descripción
	**Mostrar fichero de informe** Se muestra el fichero de informe de Mail Protection.
	**Mostrar propiedades del email seleccionado** Abre un cuadro de diálogo con información adicional sobre el email seleccionado.
	**No volver a comprobar dirección de email por si fuera malware** La dirección de email seleccionada ya no se analizará en el futuro en cuanto a virus y programas no deseados. Puede restablecer este parámetro en la configuración, en **Mail Protection > General > Excepciones** (consulte Excepciones).
	**Eliminar los emails seleccionados** El email seleccionado se elimina de la memoria caché. Sin embargo, el fichero permanecerá en el programa de email.

	**Restablecer estadísticas** La información estadística de esta sección se restablece.

Emails analizados

Este área muestra los emails analizados por Mail Protection.

Icono	Descripción
	No se ha encontrado ningún virus o programa no deseado.
	Se ha encontrado un virus o un programa no deseado.

Tipo

Indica el protocolo utilizado para recibir o enviar el email:

- POP3: email recibido a través de POP3
- IMAP: email recibido a través de IMAP
- SMTP: email enviado vía SMTP

Remitente/Destinatario

Muestra la dirección del remitente del email.

Asunto

Muestra el asunto del email recibido.

Fecha/Hora

Muestra cuándo se analizó este email en busca de spam.

Nota
Puede ver más información haciendo doble clic sobre el email relevante.

Estadísticas

Acción en email

Muestra la acción que se debe llevar a cabo cuando Mail Protection encuentre un virus o programa no deseado en un email. En el modo interactivo no aparece nada, ya que usted mismo decidirá la acción a tomar en caso de una detección.

> **Nota**
> Puede adaptar este parámetro a sus necesidades en la configuración. Para acceder a esta, haga clic en el botón o en el enlace Configuración.

Datos adjuntos afectados

Muestra la acción que se debe tomar cuando Mail Protection encuentra en un dato adjunto un virus o programa no deseado. En el modo interactivo no aparece nada, ya que usted mismo decidirá la acción a tomar en caso de una detección.

> **Nota**
> Puede adaptar este parámetro a sus necesidades en la configuración. Para acceder a esta, haga clic en el botón o en el enlace Configuración.

Número de emails

Muestra el número de emails analizados por Mail Protection.

Última detección

Nombre del último virus o programa no deseado que se ha encontrado.

Número de detecciones

Muestra el número de virus y programas no deseados detectados y notificados hasta el momento.

Emails sospechosos

Muestra el número de emails notificados por la heurística.

Número de emails recibidos

Muestra el número de emails recibidos.

Número de emails enviados

Muestra el número de emails enviados.

7.3.9 Cuarentena

El **gestor de cuarentena** administra los objetos afectados (ficheros e emails). Su producto Avira puede mover los objetos afectados con un formato especial al directorio de cuarentena. Después, ya no pueden ejecutarse ni abrirse.

> **Nota**
> Para mover objetos al gestor de cuarentena, seleccione la opción

correspondiente a la cuarentena en la **Configuración** de **System Scanner**, **Real-Time Protection** o **Mail Protection**, en **Análisis > Acción al detectar** , mientras trabaja en el **modo automático**.
También puede seleccionar la opción correspondiente a la cuarentena en **modo interactivo**.

Barra de herramientas, comando de teclado y menú contextual

Icono	Comando de teclas	Descripción
	**F2**	**Volver a analizar objeto(s)** El objeto seleccionado se vuelve a analizar en busca de virus y programas no deseados. Se utiliza la configuración del análisis directo.
	**Entrar**	**Propiedades** Abre un cuadro de diálogo con información más detallada sobre el objeto seleccionado. **Nota** También puede abrir la información detallada haciendo doble clic en un objeto.

  (Windows Vista)	**F3**	**Restaurar objeto(s)** Se restaura el objeto seleccionado. Este objeto está entonces en su localización original. **Nota** Esta opción no está disponible para los objetos de tipo email. **Advertencia** ¡Daños graves en el sistema debido a virus o programas no deseados! Si restaura ficheros: lleve a cabo un nuevo análisis para asegurarse de que los ficheros restaurados están limpios. **Nota** A partir de Windows Vista, la restauración de objetos solo es posible con derechos de administrador.
	**F6**	**Restaurar objeto(s) en...** Un objeto seleccionado puede restaurarse en la ruta que desee. Si selecciona esta opción, se abre el cuadro de diálogo "Guardar como" para que seleccione dónde desea guardar el objeto. **Advertencia** ¡Daños graves en el sistema debido a virus o programas no deseados! Si restaura ficheros: lleve a cabo un nuevo análisis para asegurarse de que los ficheros restaurados están limpios.

	**Insertar**	**Añadir objeto(s) a cuarentena** Si cree que un fichero es sospechoso, esta opción permite añadirlo al gestor de cuarentena y, si fuera necesario, cargarlo mediante la opción Enviar objeto(s) a un servidor web del Avira Malware Research Center para su análisis.
	**F4**	**Enviar objeto(s)** El objeto se subirá para su análisis por parte del Avira Malware Research Center a un servidor web del Avira Malware Research Center. Al pulsar **Enviar objeto** se abre en primer lugar un cuadro de diálogo con un formulario para introducir los datos de contacto. Indique los datos completos. Seleccione un tipo: **fichero sospechoso** o **falsa alarma**. Pulse **Aceptar** para cargar el fichero sospechoso. **Nota** El tamaño de los ficheros que se cargan está limitado a 20 MB sin comprimir o a 8 MB comprimido. **Nota** .Para cargar varios ficheros simultáneamente, debe seleccionar todos los ficheros que desea cargar y pulsar el botón **Enviar objeto**.
	**Eliminar**	**Eliminar objeto(s)** El objeto seleccionado se eliminará del gestor de cuarentena. El objeto no puede restaurarse.
		**Copiar objetos en...** El objeto de cuarentena marcado se guarda en la carpeta seleccionada. **Nota** El objeto de cuarentena no es idéntico al fichero restaurado. El objeto de cuarentena está cifrado y no puede ejecutarse ni leerse en su formato original.

	**F7**	**Exportar todas las propiedades** Las propiedades del objeto de cuarentena marcado se exportan a un fichero de texto.
	**F10**	**Abrir el directorio de cuarentena** Abre la carpeta INFECTED.

Nota
Tiene la posibilidad de ejecutar acciones para varios objetos marcados. Para seleccionar varios objetos, mantenga pulsada la tecla Ctrl o la tecla Mayús (selección de elementos consecutivos) mientras selecciona los objetos en el gestor de cuarentena. Para seleccionar todos los objetos mostrados, pulse **Ctrl + A**.
Con la acción **Mostrar propiedades** no se pueden ejecutar acciones para múltiples objetos.

Tabla

Estado

Un objeto colocado en cuarentena puede tener diferentes estados:

Icono	Descripción
	No se ha encontrado ningún virus ni programa no deseado, el objeto está "limpio".
	Se ha encontrado un virus o un programa no deseado.
	Si añadió un fichero sospechoso al gestor de cuarentena por medio de la opción Añadir fichero, el fichero recibe este icono indicador.

Tipo

Denominación	Descripción
Correo electrónico	El objeto detectado es un email.
Archivo	El objeto detectado es un fichero.

Detección

Muestra el nombre del malware detectado.
Las detecciones realizadas mediante heurística se identifican con la extensión HEUR/.

Fuente

Muestra la ruta en la que se encontró el objeto.

Fecha/Hora

Muestra la fecha y hora de la detección.

Información detallada

Nombre del fichero

Ruta completa y nombre de fichero del objeto

Objeto en cuarentena

Nombre de fichero del objeto en cuarentena

Restaurado

SÍ / NO

SÍ: el objeto se restauró.

NO: el objeto no se restauró.

Cargar en Avira

SÍ / NO

SÍ: El objeto ya se ha subido para su análisis por parte del Avira Malware Research Center a un servidor web del Avira Malware Research Center.

NO: El objeto todavía no se ha subido para su análisis por parte del Avira Malware Research Center a un servidor web del Avira Malware Research Center.

Sistema Operativo

Windows XP/Vista Workstation: un producto de escritorio Avira detectó el malware.

Motor de análisis

Número de versión del motor de análisis

Archivo de firmas de virus

Número de versión del fichero de firmas de virus

Detección

Nombre del malware detectado

Fecha/Hora

Fecha y hora de la detección

7.3.10 Programador

El **programador** permite crear tareas programadas de análisis y actualización, y adaptar o eliminar tareas existentes.

En la configuración estándar después de la instalación queda creada la siguiente tarea:

- Tarea de análisis **Análisis rápido del sistema** (configuración predefinida): Cada semana se lleva a cabo de manera automática un análisis rápido del sistema. Durante este análisis, se analiza la existencia de virus o programas no deseados en los ficheros y las carpetas más importantes. Puede modificar esta tarea de análisis. No obstante, se recomienda crear nuevas tareas de análisis que se ajusten a sus necesidades.

Barra de herramientas, comando de teclado y menú contextual

Icono	Comando de teclas	Menú contextual
	Insert	**Insertar nueva tarea** Crea una nueva tarea. Un asistente le guía de forma clara por las configuraciones necesarias.
	Entrar	**Propiedades** Abre una ventana de diálogo con información extendida sobre la tarea seleccionada.
	F2	**Modificar tarea** Abre el asistente para crear o modificar una tarea.
	Supr	**Eliminar tarea** Elimina las tareas seleccionadas de la lista.

		**Mostrar fichero de informe** Muestra el fichero de informe del programador.
	F3	Iniciar tarea Inicia una tarea seleccionada en la lista.
	F4	Detener tarea Detiene una tarea iniciada y seleccionada.

Tabla

Tipo de tarea

Icono	Descripción
	La tarea es una tarea de actualización.
	La tarea es una tarea de análisis.

Nombre

Denominación de la tarea.

Acción

Indica si la tarea es un **análisis** o una **actualización**.

Frecuencia

Indica con qué frecuencia y cuándo debe iniciarse la tarea.

Modo de visualización

Existen los siguientes tipos de visualización:

Invisible: El trabajo se realiza sin ningún tipo de visualización. Ello es válido para tareas de análisis y para tareas de actualización.

Minimizado: La ventana del trabajo solo muestra una barra de progreso.

Maximizado: La ventana con el trabajo se encuentra visible en su totalidad.

Activado

La tarea se activa cuando se activa la casilla de marcado.

> **Nota**
> Si se ha activado como frecuencia de tarea **Inmediatamente**, la tarea se inicia directamente después de la activación. Así se dispone de la posibilidad de reiniciar la tarea según sea necesario.

Estado

Muestra el estado de la tarea:

Preparado: La tarea está lista para ejecutarse.

En ejecución: La tarea se inició y está ejecutándose.

Permite programar tareas con el programador

El asistente de planificación le ayuda a planificar, configurar y crear

- análisis programados para detectar virus y programas no deseados
- actualizaciones programadas vía Internet o intranet

Para los dos tipos, se deben introducir

- el nombre y descripción de la tarea
- cuándo debería comenzar la tarea
- con qué frecuencia debería ejecutarse la tarea
- el modo de visualización de la tarea

Frecuencia de la tarea

Opción	Descripción
Inmediatamente	La tarea se lanza en cuanto finaliza el asistente de planificación.
Diariamente	La tarea se ejecuta diariamente a una cierta hora, a las 22:00, por ejemplo.
Semanalmente	La tarea se inicia semanalmente un día determinado o varios días a una hora determinada, p. ej., martes y viernes, a las 16:26.
Intervalo	Una tarea se ejecuta con un determinado intervalo, por ejemplo, cada 24 horas.

Una vez	La tarea se ejecuta una sola vez en un momento concreto, por ejemplo el 10/04/04 a las 10:04.
Inicio de sesión	Se ejecutará la tarea con cada inicio de sesión de usuario en Windows.

Momento de inicio de la tarea

Puede determinar el día de la semana, la fecha, la hora o el intervalo en que se inicia la tarea. Esto no se muestra si indicó *Inmediatamente* como hora de inicio.

Existen diversas opciones adicionales según el tipo de tarea:

Iniciar tarea adicionalmente al conectarse a Internet (acceso telefónico a redes)

Además de la frecuencia definida, la tarea se lanza al iniciarse la conexión a Internet. Esta opción puede seleccionarse con tareas de actualización que se ejecuten diariamente, semanalmente o a otros intervalos.

Repetir la tarea si el tiempo ya transcurrió

Las tareas del pasado se relanzan si no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.
Esta opción puede seleccionarse con tareas de actualización y de análisis que se ejecuten una sola vez, o bien que se ejecuten diariamente, semanalmente o con otra frecuencia.

Apagar equipo cuando haya finalizado la tarea

El equipo se apaga una vez se haya ejecutado y finalizado la tarea. La opción solamente está disponible para tareas de análisis en el modo de representación minimizado o maximizado.

Nota
Para tareas de análisis puede seleccionar el perfil en el cuadro de diálogo Selección del perfil, tanto perfiles predeterminados predefinidos como perfiles definidos por el usuario . El perfil Selección manual siempre se ejecuta con la selección actual.

7.3.11 Informes

La sección **Informes** ofrece la posibilidad de consultar los resultados de las acciones realizadas por el programa.

Barra de herramientas, comando de teclado y menú contextual

Icono	Comando de teclado	Descripción
	Enter	**Mostrar informe** Abre una ventana en la que se muestra el resultado de la acción seleccionada. Por ejemplo, el resultado de un análisis.
	F3	**Mostrar fichero de informe** Muestra el fichero de informe seleccionado.
	F4	**Imprimir fichero de informes** Abre la caja de diálogo de Windows para imprimir el fichero de informe.
	Supr	**Eliminar informe o informes** Elimina el informe seleccionado, así como el fichero de informe correspondiente.

Tabla

Estado

Icono	Descripción
	Acción Análisis: Última detección.
	Acción Análisis: Detección de virus, o no ha finalizado correctamente.
	Acción Actualización: Actualización finalizada correctamente.
	Acción Actualización: Error de actualización.

Acción

Muestra la acción completada.

Resultado

Muestra el resultado de la acción.

Fecha/Hora

Muestra la fecha y hora en que se creó el informe.

Contenido del informe de un análisis

- *Fecha del análisis:*
  Fecha del análisis.
- *Hora de inicio del análisis:*
  Hora de inicio del análisis.
- *Tiempo de análisis requerido:*
  Muestra la hora en el formato: mm:ss
- *Estado del análisis:*
  Muestra si la tarea de análisis ha sido completada o ha sido cancelada.
- *Última detección:*
  Nombre del último virus o programa no deseado que se ha encontrado.
- *Directorios analizados:*
  Número total de directorios analizados.
- *Ficheros analizados:*
  Número total de ficheros analizados.
- *Archivos analizados:*
  Número de archivos analizados.
- *Objetos ocultos:*
  Número total de objetos ocultos encontrados.
- *Detecciones:*
  Número total de virus y programas no deseados que se han detectado.
- *Sospechosos:*
  Número de ficheros sospechosos.
- *Advertencias:*
  Número de avisos de advertencia sobre detección de virus.
- *Notas:*
  Número de ítems informativos. Por ejemplo, información resultante de un análisis.

- *Reparado:*

  Número total de ficheros reparados.
- *Cuarentena:*

  Número total de ficheros en cuarentena.
- *Cambiados de nombre:*

  Número total de ficheros renombrados.
- *Eliminado:*

  Número de ficheros eliminados.
- *Sobrescritos:*

  Número total de los ficheros sobrescritos.

> **Nota**
> Los rootkits tienen la propiedad de ocultar procesos u objetos como entradas de registro o ficheros, sin embargo, no todos los objetos ocultos son forzosamente un indicio de la existencia de un rootkit. En el caso de objetos ocultos, también puede tratarse de objetos inofensivos. Si durante la búsqueda se han encontrado objetos ocultos y no existen mensajes de advertencia de detección de virus, debería averiguar a partir del informe de qué objetos se trata y extraer más información sobre los objetos encontrados.

7.3.12 Eventos

En **Eventos**, se muestran los eventos generados por los distintos componentes de programa.

Los eventos se guardan en una base de datos. Tiene la posibilidad de limitar el tamaño de la base de datos de eventos o de desactivar la limitación del tamaño de la base de datos (consulte Eventos). En la configuración predeterminada únicamente se guardan los eventos de los últimos 30 días. El visor de eventos se actualiza automáticamente al seleccionar la sección **Eventos**.

> **Nota**
> Si hay más de 20 000 eventos almacenados en la base de datos de eventos, cuando se selecciona la sección el visor no se actualiza. En ese caso, pulse F5 para actualizarlo.

Barra de herramientas, comando de teclado y menú contextual

Icono	Comando de teclas	Descripción
	Entrar	**Mostrar evento seleccionado** Abre una ventana en la que se muestra el resultado de la acción seleccionada. Por ejemplo, el resultado del análisis.
	F3	**Exportar los eventos seleccionados** Exporta los eventos seleccionados.
	Supr	**Eliminar eventos seleccionados** Elimina el evento seleccionado.

Nota
Tiene la posibilidad de ejecutar acciones sobre varios eventos marcados. Para seleccionar varios eventos, mantenga pulsada la tecla Ctrl o la tecla Mayús (selección de elementos consecutivos) mientras selecciona los eventos. Para seleccionar todos los eventos mostrados, pulse Ctrl + A.
Con la acción Mostrar evento seleccionado no se pueden seleccionar múltiples objetos.

Módulos

Con el visor de eventos se pueden visualizar los eventos de los siguientes módulos (en orden alfabético):

Nombre de módulo
Web Protection
Real-Time Protection
Mail Protection
FireWall

Servicio de ayuda
Programador
Scanner
Updater

Si marca la casilla de verificación **Todos**, puede ver los eventos de todos los módulos disponibles. Para ver los eventos de un determinado módulo, marque por favor la casilla situada delante del módulo deseado.

Filtro

En el visor de eventos se muestran los siguientes tipos de evento:

Icono	Descripción
	Información
	Advertencia
	Error
	Detección

Si marca la casilla de verificación **Filtro**  , puede ver todos los eventos. Para mostrar solo un evento concreto, marque la correspondiente casilla de verificación junto al evento.

Tabla

El visor de eventos contiene la siguiente información:

Icono

El icono correspondiente al tipo de evento.

Tipo

Clasificación de eventos: información, advertencia, error y detección.

Módulo

El módulo Avira que registró este evento. Por ejemplo: Real-Time Protection indicando una detección.

Acción

Descripción del evento del módulo respectivo.

Fecha/Hora

Fecha y hora local en que ocurrió el evento.

7.3.13 Actualizar

Actualiza la vista de la sección abierta.

7.4 Extras

7.4.1 Analizar sectores de arranque

Puede analizar también los sectores de arranque de unidades de su equipo con un análisis directo. Esto es recomendable si se encuentra un virus durante un análisis directo y se desea comprobar que los sectores de arranque no están afectados.

Es posible seleccionar más de una unidad manteniendo pulsada la tecla de mayúsculas y seleccionando las unidades requeridas con el ratón.

Nota
Los sectores de arranque se pueden analizar automáticamente con cada análisis directo (consulte Sector de arranque de unidades de análisis).

Nota
A partir de Windows Vista, el análisis de los sectores de arranque solo es posible con derechos de administrador.

7.4.2 Lista de detecciones

Con esta función se obtiene una lista de los nombres de virus y programas no deseados que puede reconocer su producto Avira. Incluye una cómoda función de búsqueda de nombres.

Buscar en la lista de detecciones

Introduzca en el campo *Buscar:* un término de búsqueda o una secuencia de caracteres.

Buscando secuencia de caracteres en el nombre

Se puede introducir una secuencia consecutiva de letras o caracteres y el marcador moverá a la primera posición la lista de nombres que contengan esa secuencia, incluso en el caso de que esta se encuentre en el medio de un nombre (p. ej. "raxa" mostrará "Abraxas").

Buscando desde el primer carácter del nombre

Se puede introducir la letra inicial y los siguientes caracteres con el teclado, y el marcador avanzará alfabéticamente en la lista de nombres (p. ej. "Ra" mostrará "Rabbit").

Si el nombre o la secuencia de caracteres buscados está disponible, la posición se marcará en la lista.

Buscar hacia delante

Inicia la búsqueda en orden alfabético ascendente.

Buscar hacia atrás

Inicia la búsqueda en orden alfabético descendente.

Primer lugar de detección

Se mueve en la lista a la primera posición encontrada.

Entradas de la lista de detecciones

Debajo de este título hay una lista con los nombres de virus o programas no deseados que se pueden reconocer. La mayoría de las entradas de esta lista pueden ser borradas también con su producto Avira. Están ordenadas alfabéticamente (primero caracteres especiales y números, después las letras). Utilice la barra de desplazamiento para moverse hacia arriba o hacia abajo en la lista.

7.4.3 Descargar CD de rescate

El comando de menú **Descargar CD de rescate** inicia una descarga del paquete de CD de rescate de Avira. El paquete contiene un sistema en línea de inicio o arranque para PC, así como un escáner antivirus de Avira con el fichero de firmas de virus y el motor de análisis más recientes. El CD de emergencia de Avira se usa para iniciar y controlar el equipo desde el CD o DVD en caso de haberse dañado el sistema operativo con el fin de recuperar la información o realizar un análisis para detectar la existencia de virus y malware.

Tras la descarga del paquete de CD de rescate de Avira, aparece un cuadro de diálogo en el que puede seleccionar la unidad de CD/DVD para grabar el CD de rescate. También

puede optar por guardar el paquete de CD de rescate de Avira y grabar el CD de emergencia en otro momento.

> **Nota**
> Necesitará una conexión de Internet activa para descargar el paquete de CD de rescate de Avira. También necesitará una unidad de CD-/DVD y un CD o DVD grabable para grabar el CD de emergencia.

7.4.4 Configuración

La opción **Configuración** del menú **Extras** abre la configuración.

7.5 Actualización

7.5.1 Iniciar actualización...

La opción de menú **Iniciar actualización...** del menú **Actualización** inicia una actualización inmediatamente. Se actualizan el fichero de firmas de virus y el motor de búsqueda.

7.5.2 Actualización manual...

La opción de menú **Actualización manual...** del menú **Actualización** abre un cuadro de diálogo para seleccionar y cargar un paquete de actualizaciones del VDF o del motor. Puede descargar el paquete de actualización, que contiene el fichero de firmas de virus y el motor de análisis actuales, en la página web del fabricante:
http://www.avira.es

> **Nota**
> A partir de Windows Vista, solo es posible llevar a cabo una actualización manual con derechos de administrador.

7.6 Ayuda

7.6.1 Temas

La opción de menú **Temas** en el menú **Ayuda** abre la lista de contenidos de la ayuda online.

7.6.2 Ayúdeme

Si dispone de una conexión a Internet activa, la opción de menú **Ayúdeme** en el menú **Ayuda** abre la página de soporte correspondiente del producto en el sitio web de Avira. En ella podrá leer las respuestas a las preguntas más frecuentes, consultar la base de datos de conocimiento o el Servicio al cliente de Avira.

7.6.3 Descargar manual

Si dispone de una conexión a Internet activa, la opción de menú **Descargar manual** en el menú **Ayuda** abre la página de descarga de su producto Avira. En ella encontrará el enlace para descargar el manual más actual de su producto Avira.

7.6.4 Cargar fichero de licencia

La opción de menú **Cargar fichero de licencia** en el menú **Ayuda** abre un cuadro de diálogo que sirve para leer el fichero de licencia *.KEY*.

> **Nota**
> A partir de Windows Vista, solo es posible cargar la licencia con derechos de administrador.

7.6.5 Enviar feedback

Si dispone de una conexión a Internet activa, la opción de menú **Enviar feedback** en el menú **Ayuda** abre la página de feedback de los productos Avira. Aquí encontrará un cuestionario para evaluar nuestros productos con el cual puede comunicar su opinión acerca de la calidad de los productos y sugerencias relacionadas con los productos a Avira.

7.6.6 Acerca de Avira Professional Security

General

Direcciones e información de su producto Avira

Información de versión

Información de versión para archivos dentro del paquete Avira

Información de licencia

Datos de la licencia actual y enlaces con la tienda online (adquisición o renovación de una licencia)

Nota

Puede copiar los datos de licencia en el portapapeles. Haga clic con el botón derecho del ratón en el área Datos de licencia. Se abrirá un menú contextual. En el menú contextual, haga clic en el comando **Copiar en el portapapeles**. Ahora sus datos de licencia se encuentran en el portapapeles y los puede pegar a través del comando de pegar de Windows en emails, formularios o documentos.

8. Configuración

8.1 Configuración

- Información general sobre las opciones de configuración
- Perfiles de configuración
- Botones

Información general sobre las opciones de configuración

Dispone de las opciones de configuración siguientes:

- **System Scanner**: configuración del análisis directo.
  - Opciones de análisis
  - Acción al detectar
  - Acciones adicionales
  - Opciones al analizar archivos
  - Excepciones del análisis directo
  - Heurística del análisis directo
  - Configuración de la función de informe
- **Real-Time Protection**: configuración del análisis en tiempo real.
  - Opciones de análisis
  - Acción al detectar
  - Excepciones del análisis en tiempo real.
  - Heurística del análisis en tiempo real.
  - Configuración de la función de informe
- **Actualización**: configuración de los ajustes de actualización.
  - Descarga mediante el servidor de ficheros
  - Descarga a través de servidor web
  - Configuración de proxy
- **FireWall**: configuración de FireWall.
  - Configuración de las reglas del adaptador
  - Configuración definida por el usuario de las reglas de aplicación
  - Lista de proveedores de confianza (excepciones durante el acceso a la red de las aplicaciones)
  - Configuración avanzada: tiempo de espera para reglas, detener FireWall de Windows, notificaciones
  - Configuración de ventanas emergentes (mensajes de advertencia durante el acceso a la red de las aplicaciones)

- **Web Protection**: configuración de Web Protection.
  - Opciones de análisis, activación y desactivación de Web Protection.
  - Acción al detectar
  - Accesos bloqueados: tipos de fichero y tipos MIME no deseados, filtro web para direcciones URL conocidas no deseadas (malware, suplantación de identidad (phishing), etc.).
  - Excepciones del análisis de Web Protection: URL, tipos de fichero y tipos MIME.
  - Heurística de Web Protection
  - Configuración de la función de informe
- **Mail Protection**: configuración de Mail Protection.
  - Opciones de análisis: activación de la supervisión de cuentas POP3, cuentas IMAP, correos electrónicos salientes (SMTP).
  - Acción al detectar
  - Acciones adicionales
  - Heurística del análisis de Mail Protection
  - Función AntiBot: servidores SMTP permitidos, remitentes de correo electrónico permitidos.
  - Excepciones del análisis de Mail Protection
  - Configuración de la memoria caché, vaciar memoria caché
  - Configuración de un pie de página en correos electrónicos enviados
  - Configuración de la función de informe
- **General**:
  - Categorías de riesgos avanzadas para análisis directo y análisis en tiempo real
  - Protección avanzada: opciones para activar ProActiv y Protection Cloud.
  - Filtro de aplicación: bloquear o permitir aplicaciones.
  - Protección con contraseña para el acceso al Centro de control y a la configuración
  - Seguridad: bloquear funciones de Ejecución automática, bloquear el fichero host de Windows, Protección del producto.
  - WMI: activar compatibilidad con WMI.
  - Configuración del registro de eventos
  - Configuración de las funciones de informe
  - Configuración de los directorios empleados
  - Advertencias:
    Configuración de advertencias de red de los componentes:
    System Scanner
    Real-Time Protection
    Configuración de advertencias por email de los componentes:
    Scanner
    Real-Time Protection
    Updater
  - Configuración de las advertencias acústicas tras la detección de malware

Perfiles de configuración

Para administrar los distintos perfiles de configuración, haga clic en el icono de la bandeja a la derecha de la sección “Configuración predeterminada" (consulte Icono de la bandeja). Hay disponibles diversas opciones que permiten guardar opciones de configuración agrupadas como perfiles: para ello, primero añada una configuración nueva y, a continuación, introduzca en ella los valores que desea; es decir, las reglas que deben aplicarse.

Puede elegir entre la modificación manual o automática de la configuración. Para cambiar automáticamente a la configuración creada, puede seleccionar o definir una regla. Existen diversas formas de definir estas reglas predeterminadas: puede especificar que cada vez que se utilice una puerta de enlace no asignada se produzca un cambio de configuración automático, o que la puerta de enlace predeterminada se defina mediante una dirección IP o MAC (o una dirección IP y una máscara de red).

Si no se han definido reglas para cambiar a otra configuración, puede cambiarla manualmente en el menú contextual del icono de la bandeja. Los perfiles de configuración se administran mediante el menú contextual de las ventanas de configuración:

Menú contextual

Comando de teclas	Menú contextual/descripción
Ins	**Crear nueva configuración** Crea una configuración nueva con valores predeterminados para cada una de las opciones de configuración.
F2	**Cambiar nombre de configuración** Edita el nombre de la configuración.
Supr	**Eliminar configuración** Elimina la configuración seleccionada: en primer lugar, se abre un cuadro de diálogo en el que puede cancelar o confirmar la eliminación de la configuración seleccionada.
F4	**Copiar configuración** Copia la configuración seleccionada.

F6	**Restablecer configuración** Restablece las opciones de configuración de la configuración seleccionada con sus valores predeterminados.
	Reglas: Se muestran las distintas opciones existentes para especificar las reglas de los perfiles de configuración: **Ninguna** No hay ninguna regla válida para cambiar a la configuración seleccionada. El cambio a la configuración correspondiente debe hacerse manualmente. **Regla predeterminada** La configuración seleccionada se usa como configuración predeterminada: se cambia automáticamente a la configuración seleccionada cuando se usa una puerta de enlace que no se ha asignado a ninguna otra configuración. **Puerta de enlace predeterminada** Para la configuración seleccionada, se puede indicar una dirección IP o una dirección MAC de la puerta de enlace predeterminada como regla de cambio. Si se usa la puerta de enlace predeterminada que se ha indicado, se cambia automáticamente a la configuración seleccionada. **Dirección IP** Para la configuración seleccionada, se puede indicar una dirección IP y una máscara de red del adaptador de red como regla de cambio. Si se usa la dirección IP que se ha indicado, se cambia automáticamente a la configuración seleccionada.

Nota
Puede guardar un máximo de ocho configuraciones.

Nota
Si al cambiar la puerta de enlace no se encuentra ninguna regla coincidente, se mantiene activa la última configuración usada.

Botones

Botón	Descripción
Valores predeterminados	Todos los parámetros de la configuración se restablecen con los valores predeterminados. Al restablecer los valores predeterminados, se pierde cualquier cambio efectuado y todas las entradas propias.
Aceptar	Se guardan todas las configuraciones realizadas. Se cierra la configuración. El control de cuentas de usuarios (UAC) precisa su aprobación para aceptar los cambios realizados en sistemas operativos a partir de Windows Vista.
Cancelar	La configuración se cierra sin guardar los ajustes realizados.
Aplicar	Se guardan todas las configuraciones realizadas. El control de cuentas de usuarios (UAC) precisa su aprobación para aceptar los cambios realizados en sistemas operativos a partir de Windows Vista.

8.2 Scanner

La sección **Scanner** de la configuración sirve para configurar el análisis directo, es decir, el análisis a petición.

8.2.1 Análisis

Aquí puede definir el comportamiento básico de la rutina de búsqueda en el caso de un análisis directo. Si selecciona determinadas carpetas para el análisis directo, Scanner analiza en función de la configuración:

- con una cierta profundidad y prioridad,
- también ciertos sectores de arranque y la memoria principal,
- todos o ciertos ficheros seleccionados.

Ficheros

Scanner puede usar un filtro para analizar solo ficheros de una cierta extensión (tipo).

Todos los ficheros

Si esta opción está activada, se analizan todos los ficheros sin tener en cuenta su contenido ni extensión, en busca de virus o programas no deseados. No se utiliza el filtro.

Nota
Si **Todos los ficheros** está activo, no es posible seleccionar el botón **Extensiones de fichero**.

Selección inteligente de ficheros

Si esta opción está activada, el programa selecciona de forma completamente automática los ficheros que deben analizarse. Esto significa que el producto de Avira decide, dependiendo del contenido del archivo, si se debe comprobar la presencia de virus y programas no deseados. Este procedimiento es algo más lento que **Usar lista de extensiones de ficheros**, pero resulta más seguro, ya que no se analiza únicamente en función de la extensión del fichero. Este ajuste está activado de forma estándar y es el recomendado.

Nota
Si **Selección inteligente de ficheros** está activo, no es posible seleccionar el botón **Extensiones de fichero**.

Usar lista de extensiones de ficheros

Si esta opción está activada, solo se analizan ficheros con la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están preseleccionados. Esta lista puede editarse manualmente mediante el botón "**Extensiones de fichero"**.

Nota
Si esta opción está activada y ha eliminado todas las entradas de la lista con extensiones de ficheros, esto se indica como "*Sin extensiones*" debajo del botón **Extensiones de fichero**.

Extensiones de fichero

Con ayuda de este botón se abre un cuadro de diálogo que muestra todas las extensiones de fichero que se incluirán en el análisis en el modo "**Usar lista de extensiones de ficheros"**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota
Tenga en cuenta que la lista predeterminada puede variar entre versiones.

Configuración adicional

Sector de arranque de unidades de análisis

Si esta opción está activada, Scanner solo analiza los sectores de arranque de las unidades seleccionadas para el análisis directo. Este ajuste está activado de forma estándar.

Analizar sectores de arranque maestros

Si esta opción está activada, Scanner solo analiza los sectores de arranque maestros de los discos duros usados en el sistema.

Omitir ficheros offline

Si esta opción está activada, el análisis directo omite por completo los así llamados ficheros offline durante el análisis. Es decir, no se analizan estos archivos en busca de virus y programas no deseados. Los ficheros offline son los que se han trasladado físicamente del disco duro a otro medio, p. ej., una cinta, en un sistema jerárquico de administración de almacenamientos (HSMS, Hierarchical Storage Management System). Este ajuste está activado de forma estándar.

Comprobación de integridad de ficheros del sistema

Si esta opción está activada, en cada análisis directo se analizan de manera especialmente segura los ficheros del sistema Windows más importantes para detectar modificaciones debidas a malware. Si se detecta un fichero modificado, se notifica como detección sospechosa. Esta función requiere mucha capacidad de rendimiento del equipo. Por lo tanto, esta opción está desactivada de forma estándar.

Nota
Esta opción solo está disponible a partir de Windows Vista. Si administra el producto Avira en SMC, esta opción no está disponible.

Nota
Si utiliza herramientas de otros proveedores que modifican archivos de sistema y adaptan la pantalla de arranque o inicio a sus propias necesidades, no debería utilizar esta opción. Ejemplos de este tipo de herramientas son los llamados Skinpacks, TuneUp Utilities o Vista Customization.

Análisis optimizado

Si esta opción está activada, durante el análisis de Scanner se optimiza la capacidad del procesador. Por motivos de rendimiento, el registro durante el análisis optimizado únicamente se lleva a cabo en un nivel estándar.

Nota
Esta opción solo está disponible en equipos con multiprocesador. Si se administra su producto de Avira en SMC, la opción se muestra en todos los casos y se puede activar: si el equipo administrado no dispone de varios procesadores, Scanner no usa la opción.

Seguir enlaces simbólicos

Si esta opción está activada, Scanner sigue durante el análisis todos los accesos directos simbólicos del perfil de análisis o del directorio seleccionado, con el fin de analizar los ficheros vinculados acerca de la presencia de virus y malware.

Nota
La opción no incluye accesos directos a ficheros (accesos directos), sino que se refiere exclusivamente a vínculos simbólicos (creados con mklink.exe) o puntos de unión (creados con junction.exe) que existen en el sistema de ficheros de forma transparente.

Análisis de rootkits al iniciar

Si esta opción está activada, al inicio del análisis Scanner comprueba si hay rootkits activos en el directorio del sistema Windows con un así llamado procedimiento rápido. Este procedimiento no analiza la existencia de rootkits activos en el equipo tan exhaustivamente como lo hace el perfil de análisis "**Búsqueda de rootkits"**, pero su ejecución es considerablemente más rápida. Esta opción modifica solo la configuración de los perfiles que ha creado.

Nota
En Windows XP 64 Bit , el análisis de rootkits no está disponible.

Analizar el registro

Si esta opción está activada, se analiza el registro en búsqueda de indicios de software dañino. Esta opción modifica solo la configuración de los perfiles que ha creado.

Omitir ficheros y rutas en unidades de red

Si esta opción está activada, se excluyen del análisis directo las unidades de red conectadas al equipo. Esta opción es recomendable si los servidores u otras estaciones de trabajo ya disponen de software de protección antivirus. Esta opción está desactivada de forma estándar.

Proceso de análisis

Permitir detener

Si esta opción está activada, es posible finalizar en cualquier momento el análisis de virus o programas no deseados pulsando el botón "**Detener"** de la ventana "**Luke Filewalker**". Si ha desactivado este ajuste, el botón **Detener** de la ventana "**Luke Filewalker**" aparece en gris. Debido a ello no se puede detener el análisis de forma prematura. Este ajuste está activado de forma estándar.

Prioridad del escáner

Scanner distingue entre varios niveles de prioridad. Esto es efectivo únicamente si se ejecutan varios procesos simultáneamente en el equipo. La selección afecta a la velocidad de análisis.

Baja

El sistema operativo únicamente asigna tiempo del procesador a Scanner si ningún otro proceso necesita tiempo del procesador; es decir, mientras solo se esté ejecutando Scanner, la velocidad es la máxima. Por lo general, así se facilita en gran medida el trabajo con otros programas: el equipo reacciona más rápidamente cuando otros programas precisan tiempo de cálculo y en esos casos Scanner continúa ejecutándose en segundo plano.

Media

A Scanner se le asigna una prioridad normal. El sistema operativo asigna a todos los procesos la misma cantidad de tiempo del procesador. Este ajuste está activado de forma estándar y es el recomendado. En ciertas circunstancias, puede afectarse el rendimiento de otras aplicaciones.

Alta

A Scanner se le asigna una prioridad máxima. El trabajo simultáneo con otras aplicaciones es casi imposible. No obstante, Scanner analiza con la mayor velocidad posible.

Acción al detectar

Puede definir acciones que Scanner debe ejecutar si se detecta un virus o un programa no deseado.

Interactivo

Si esta opción está activada, se avisa en un cuadro de diálogo acerca de la detección durante la búsqueda de Scanner. Durante la búsqueda de Scanner, se muestra al finalizar el análisis un mensaje de advertencia con una lista de los ficheros afectados detectados. Tiene la posibilidad de seleccionar la acción que desea ejecutar para cada archivo afectado mediante un menú contextual. Puede ejecutar las acciones seleccionadas para los ficheros afectados o finalizar Scanner.

Nota
En el cuadro de diálogo de Scanner se muestra la acción **Cuarentena**, que debe ejecutarse por defecto.

Acciones permitidas

En esta área puede seleccionar las acciones que se muestran en el cuadro de diálogo cuando se detecta un virus. Para ello, tiene que activar las opciones correspondientes.

Reparar

Scanner repara el archivo afectado, siempre que sea posible.

Cambiar el nombre

Scanner cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar el archivo y volver a cambiar el nombre posteriormente.

Cuarentena

Scanner mueve el archivo a la cuarentena. El gestor de cuarentena puede recuperarlo si tiene valor informativo o, en caso necesario, enviarlo al Avira Malware Research Center. En función del fichero hay disponibles otras opciones en el Gestor de cuarentena.

Eliminar

Se borra el archivo. Esta tarea es considerablemente más rápida que "Sobrescribir y eliminar".

Omitir

Se sale del archivo.

Sobrescribir y eliminar

Scanner sobrescribe el fichero con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Predeterminado

Mediante este botón define la acción por defecto de Scanner para tratar los archivos afectados. Marque una acción y haga clic en el botón **"Predeterminado"**. En el modo de notificación combinado, solo se puede ejecutar la acción predeterminada que se ha seleccionado para los ficheros afectados. En el modo de notificación personalizado y experto, aparece seleccionada la acción predeterminada que se ha seleccionado para los ficheros afectados.

Nota
No se puede seleccionar la acción **Reparar** como acción predeterminada.

Nota
Si ha seleccionado como acción predeterminada **Eliminar** o **Sobrescribir y eliminar** y quiere establecer el modo de notificación combinado, tenga en cuenta lo siguiente: en caso de detección mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a la cuarentena.

Automático

Si esta opción está activada, cuando se detecta un virus o un programa no deseado, no aparece ningún cuadro de diálogo en el que se pueda seleccionar una acción. Scanner reacciona en función de la configuración que ha realizado en esta sección.

Copiar fichero a cuarentena antes de la acción

Si esta opción está activada, Scanner crea una copia de seguridad (backup) antes de realizar la acción principal o secundaria deseada. La copia de seguridad se guarda en la cuarentena, donde se puede recuperar el fichero si tiene valor informativo. Además, puede enviar la copia de seguridad al Avira Malware Research Center para examinarla posteriormente.

Mostrar mensajes de advertencia

Si esta opción está activada, cuando se detecta un virus o un programa no deseado, aparece un mensaje de advertencia con las acciones que se van a ejecutar.

Acción principal

La acción principal es aquella que se ejecuta cuando Scanner detecta un virus o un programa no deseado. Si se ha seleccionado la opción "**Reparar**", pero no es posible reparar el fichero afectado, se ejecuta la acción seleccionada en "**Acción secundaria**".

Nota
Solo puede seleccionarse la opción **Acción secundaria** si se ha seleccionado en **Acción principal** el ajuste **Reparar**.

Reparar

Si esta opción está activada, Scanner repara automáticamente los archivos afectados. Si Scanner no puede reparar el fichero afectado, ejecuta la acción seleccionada en Acción secundaria.

Nota
Se recomienda la reparación automática, pero eso significa que Scanner puede modificar los ficheros en el equipo.

Cambiar el nombre

Si esta opción está activada, Scanner cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar y volver a cambiar el nombre posteriormente.

Cuarentena

Si esta opción está activada, Scanner mueve el archivo a la cuarentena. Estos ficheros pueden repararse posteriormente o, si fuera necesario, enviarse al Centro de investigación de malware de Avira.

Eliminar

Si esta opción está activada, se borra el fichero. Esta tarea es considerablemente más rápida que **Sobrescribir y eliminar** (véase más abajo).

Omitir

Si esta opción está activada, está permitido acceder al archivo y salir de él.

Advertencia
El archivo afectado permanece activo en su ordenador. Puede causar daños graves en su ordenador.

Sobrescribir y eliminar

Si esta opción está activada, Scanner sobrescribe el archivo con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Acción secundaria

Solo puede seleccionarse la opción "**Acción secundaria"** si se ha seleccionado en "**Acción principal"** el ajuste **Reparar**. Con esta opción se decide qué debe hacerse si el fichero afectado no puede repararse.

Cambiar el nombre

Si esta opción está activada, Scanner cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar y volver a cambiar el nombre posteriormente.

Cuarentena

Si esta opción está activada, Scanner mueve el archivo a la cuarentena. Estos ficheros pueden repararse posteriormente o, si fuera necesario, enviarse al Centro de investigación de malware de Avira.

Eliminar

Si esta opción está activada, se borra el fichero. Esta tarea es considerablemente más rápida que "Sobrescribir y eliminar".

Omitir

Si esta opción está activada, está permitido acceder al archivo y salir de él.

Advertencia
El archivo afectado permanece activo en su ordenador. Puede causar daños graves en su ordenador.

Sobrescribir y eliminar

Si esta opción está activada, Scanner sobrescribe el archivo con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Nota
Si ha seleccionado como acción principal o secundaria **Eliminar o Sobrescribir y eliminar**, tenga en cuenta lo siguiente: en caso de detección mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a la cuarentena.

Acciones adicionales

Iniciar programa tras detección

Tras el análisis directo, Scanner abre un archivo cualquiera (por ejemplo, un programa) si se ha detectado al menos un virus o un programa no deseado, p. ej., un programa de correo electrónico, para que pueda informar a otros usuarios o al administrador.

Nota
Por motivos de seguridad, solo es posible iniciar un programa tras una detección si hay un usuario conectado en un equipo. El fichero se inicia con los derechos con los que cuenta el usuario conectado. Si no hay conectado ningún usuario, esta acción no se ejecuta.

Nombre de programa

En este campo de entrada puede introducir el nombre y la ruta correspondiente del programa que Scanner debe iniciar tras una detección.

...

El botón abre una ventana en la que puede navegar hasta el fichero con la ayuda del explorador de ficheros.

Argumentos

En este campo de entrada puede registrar, en caso necesario, parámetros de línea de comandos del programa que debe iniciarse.

Registro de eventos

Usar registro de eventos

Si está opción está activada, tras un análisis correcto, Scanner transmite un mensaje del evento con los resultados del análisis al registro de eventos de Windows. Se puede acceder a los eventos en el registro de eventos de Windows. Esta opción está desactivada de forma estándar.

Archivos

Cuando Scanner analiza archivos comprimidos, utiliza un análisis recursivo: también se descomprimen los archivos comprimidos que estén incluidos en otros archivos comprimidos y se analizan en busca de virus y programas no deseados. Los archivos comprimidos se analizan, se descomprimen y se analizan de nuevo.

Analizar archivos

Si esta opción está activada, se analizan los archivos comprimidos seleccionados de la lista. Este ajuste está activado de forma estándar.

Todos los tipos de archivo

Si esta opción está activada, se marcan y analizan todos los archivos comprimidos de la lista.

Extensiones inteligentes

Si esta opción está activada, Scanner detecta si un fichero está comprimido, incluso si su extensión no lo refleja y analiza el archivo. De todas formas, esto significa que se deben abrir todos los ficheros, lo que reduce la velocidad de análisis. Ejemplo: si un archivo *.zip tiene la extensión de fichero *.xyz, Scanner descomprime también este archivo y lo analiza. Este ajuste está activado de forma estándar.

Nota
Solo se analizan aquellos tipos de archivos comprimidos marcados en la lista de archivos comprimidos.

Limitar nivel de recursividad

El proceso de descomprimir y analizar ficheros profundamente entrelazados puede requerir gran cantidad de tiempo y recursos. Si esta opción está activada, se limita la profundidad del análisis en ficheros comprimidos múltiples veces (máximo nivel de recursividad). Esto ahorra tiempo y recursos del equipo.

Nota
Para encontrar un virus o programa no deseado dentro de un archivo comprimido, Scanner debe analizar hasta el nivel de recursividad donde se encuentre el virus o programa no deseado.

Nivel máximo de recursividad

Para introducir el máximo nivel de recursividad, se debe activar la opción **Limitar nivel de recursividad**.
Puede introducir directamente el nivel de recursividad pertinente o cambiarlo con las teclas de flecha que hay a la derecha del campo de entrada. Los valores permitidos se encuentran entre el 1 y el 99. Se recomienda el valor estándar de 20.

Valores predeterminados

Mediante este botón se restablecen los valores predefinidos cuando se analizan archivos comprimidos.

Lista de archivos

En esta área puede establecer qué ficheros comprimidos debe analizar Scanner. Para ello, debe seleccionar las entradas relevantes.

Excepciones

Ficheros a excluir Scanner

La lista de esta ventana contiene los ficheros y rutas que no deben de incluirse en el análisis en busca de virus o programas no deseados por parte de Scanner.

Introduzca las mínimas excepciones posibles y solo ficheros que considere que, independientemente de la causa, no deberían incluirse en un análisis de rutina. Le recomendamos analizar antes los ficheros y programas no deseados incluidos en esta lista.

Nota
La suma de las entradas de la lista no puede superar el máximo de 6000 caracteres.

Advertencia
Estos ficheros no se toman en cuenta en el análisis.

Nota
Los ficheros incluidos en esta lista se anotan en el fichero de informe.
Compruebe la presencia de estos ficheros no comprobados de vez en cuando en el fichero de informe, ya que quizás la razón por la que ha retirado un fichero de la comprobación ya no existe. En este caso, debería retirarse el nombre de estos ficheros de la lista.

Campo de entrada

En esta ventana, puede introducir el nombre del fichero que no desea incluir en el análisis directo. De forma predeterminada no hay ningún fichero indicado.

El botón abre una ventana en la que puede seleccionar el fichero o la ruta deseada. Cuando introduce un fichero con su ruta completa, solo este fichero se excluye del análisis. Si se introduce un nombre de fichero sin una ruta, todos los ficheros con ese nombre (independientemente de donde se encuentren) se excluyen del análisis.

Añadir

Este botón permite incluir en la ventana el fichero introducido en el campo de entrada.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Nota
Si administra el producto de Avira en AMC, puede utilizar variables en las indicaciones de rutas en caso de excepciones de ficheros. Puede encontrar una lista de las variables que se pueden utilizar en Variables: excepciones de Real-Time Protection y Scanner.

Heurística

Esta sección de configuración trata sobre la configuración de la heurística del motor de análisis.

Los productos de Avira integran heurísticas muy potentes con las que se puede detectar de forma proactiva el malware desconocido, es decir, antes de que se cree una firma de virus especial contra el parásito y se envíe una actualización de la protección frente a los virus. Los virus se detectan gracias a un análisis y un examen exhaustivos del código afectado de acuerdo con las funciones habituales del malware. Si el código analizado cumple estas características, se considera sospechoso. Sin embargo, esto no significa necesariamente que el código sea malware; también se pueden producir falsas alarmas. El usuario es responsable de decidir qué debe hacerse con el código afectado, p. ej., basándose en sus conocimientos de si la fuente que contiene el código afectado es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto de Avira integra una heurística de macrovirus muy potente. Si esta opción está activada, durante una posible reparación se borran todas las macros del

documento afectado o bien se muestra una notificación acerca de los documentos sospechosos, es decir, se muestra una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Advanced Heuristic Analysis and Detection (AHeAD)

Activar AHeAD

Su programa de Avira incorpora en la tecnología AHeAD de Avira una heurística muy potente que puede detectar también el malware desconocido (nuevo). Si esta opción está activada, aquí puede ajustar hasta qué punto es "precisa" esta heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si esta opción está activada, se detecta en menor medida el malware desconocido, pero se reduce el riesgo de posibles falsos positivos.

Nivel de detección medio

Si esta opción está activada, se garantiza una protección equilibrada con pocos falsos positivos. Este ajuste está activado de forma estándar si ha seleccionado que se aplique esta heurística.

Nivel de detección alto

Si esta opción está activada, el malware desconocido se detecta en mayor medida, pero se debe contar con falsos positivos.

8.2.2 Informe

Scanner dispone de una completa funcionalidad para crear informes. Así puede obtener información muy precisa de los resultados del análisis directo. El fichero de informe contiene todas las entradas del sistema, así como advertencias y mensajes del análisis directo.

> **Nota**
> Para que pueda establecer qué acciones ha tomado Scanner al detectar un virus o programa no deseado, es importante crear siempre un fichero de informe.

Protocolización

Desactivado

Si esta opción está activada, Scanner no informa de las acciones y resultados de un análisis directo.

Predeterminado

Si esta opción está activada, Scanner informa del nombre y ruta de los ficheros afectados. Además, en el fichero de informe aparece la configuración del análisis, información de la versión y del titular de la licencia.

Extendido

Si esta opción está activada, Scanner informa de alertas e instrucciones, además de la información habitual. El fichero de informe muestra el sufijo "(Cloud)" para identificar las advertencias de Protection Cloud.

Completo

Si esta opción está seleccionada, Scanner informa de todos los ficheros analizados. Además, se incluyen en el informe todos los ficheros, así como alertas y mensajes.

Nota
Si tiene que enviarnos algún fichero de informe para resolver algún problema, hágalo de este modo.

8.3 Real-Time Protection

La sección Real-Time Protection de la configuración sirve para configurar el análisis en tiempo real.

8.3.1 Análisis

Normalmente querrá monitorizar su sistema de forma constante. Para ello, utilice Real-Time Protection (análisis en tiempo real = escáner en acceso). Así puede, entre otras cosas, analizar todos los ficheros que se copian o abren en el equipo "sobre la marcha" para detectar la presencia de virus y programas no deseados.

Ficheros

Real-Time Protection puede usar un filtro para analizar solo ficheros de una cierta extensión (tipo).

Todos los ficheros

Si esta opción está activada, se analizan todos los ficheros sin tener en cuenta su contenido ni extensión, en busca de virus o programas no deseados.

Nota
Si **Todos los ficheros** está activo, no es posible seleccionar el botón **Extensiones de fichero**.

Selección inteligente de ficheros

Si esta opción está activada, el programa selecciona de forma completamente automática los ficheros que deben analizarse. Esto significa que el programa decide, dependiendo del contenido del archivo, si se debe comprobar la presencia de virus y programas no deseados en los ficheros. Este procedimiento es algo más lento que **Usar lista de extensiones de ficheros**, pero resulta más seguro, ya que no se analiza únicamente en función de la extensión del fichero.

Nota
Si **Selección inteligente de ficheros** está activo, no es posible seleccionar el botón **Extensiones de fichero**.

Usar lista de extensiones de ficheros

Si esta opción está activada, solo se analizan ficheros con la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están preseleccionados. Esta lista puede editarse manualmente mediante el botón "**Extensiones de fichero"**. Este ajuste está activado de forma estándar y es el recomendado.

Nota
Si esta opción está activada y ha eliminado todas las entradas de la lista con extensiones de ficheros, esto se indica como "*Sin extensiones*" debajo del botón **Extensiones de fichero**.

Extensiones de fichero

Con ayuda de este botón se abre un cuadro de diálogo que muestra todas las extensiones de fichero que se incluirán en el análisis en el modo "**Usar lista de extensiones de ficheros"**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota
Tenga en cuenta que la lista de extensiones de ficheros puede variar entre versiones.

Unidades

Supervisar unidades de red

Si esta opción está activada, se analizan las unidades de red (unidades mapeadas) como p. ej., volúmenes del servidor, unidades de red punto a punto.

Nota
Para no afectar al rendimiento del equipo excesivamente, únicamente debería activarse la opción **Supervisar unidades de red** en casos excepcionales.

Advertencia
Si la opción está desactivada, las unidades de red **no** se supervisan. Ya no está protegido contra virus ni programas no deseados.

Nota
Al ejecutar ficheros desde unidades de red, Real-Time Protection los analiza, independientemente del parámetro configurado en la opción **Supervisar unidades de red**. En algunos casos, los ficheros en unidades de red se analizan al abrirlos, aunque esté desactivada la opción **Supervisar unidades de red**. El motivo es que a estos ficheros se accede con el permiso 'Ejecutar fichero'. Si desea excluir estos ficheros o también los ficheros que se ejecuten en unidades de red de la supervisión de Real-Time Protection, debe incluir estos ficheros en la lista de ficheros omitidos (consulte: Excepciones).

Activar almacenamiento en caché

Si esta opción está activada, los ficheros supervisados en unidades de red se ponen a disposición del caché de Real-Time Protection. La supervisión de unidades de red sin función de caché ofrece más seguridad, pero es más lenta que la supervisión de unidades de red con caché.

Archivos

Analizar archivos

Si esta opción está activada, se analizan los ficheros comprimidos. Los archivos comprimidos se analizan, se descomprimen y se analizan de nuevo. Esta opción está desactivada de forma estándar. Se limita el análisis de archivos mediante el nivel de recursividad, la cantidad de ficheros que se analizan y el tamaño del archivo comprimido. Puede establecer el nivel de recursividad, la cantidad de ficheros que se analizan y el tamaño máximo del archivo comprimido.

Nota
Esta opción está desactivada de forma estándar, ya que sobrecarga mucho al procesador. En general, se recomienda que los archivos comprimidos se comprueben con el análisis directo.

Nivel máx. recursividad

Cuando Real-Time Protection analiza archivos comprimidos utiliza un análisis recursivo: también se descomprimen los archivos comprimidos que estén incluidos en

otros archivos comprimidos y se analizan en busca de virus y programas no deseados. Puede definir el nivel de recursividad. El valor predeterminado para el nivel de recursividad es 1 y es el recomendado: se analizan todos los ficheros que se encuentran directamente en el archivo principal.

Núm. máximo de ficheros

Cuando se analizan archivos, el análisis se limita a una cantidad máxima de ficheros. El valor predeterminado para la cantidad máxima de ficheros que se analizarán es 10 y es el valor recomendado.

Tamaño máximo (KB)

Cuando se analizan archivos, el análisis se limita a un tamaño máximo del archivo que se va a descomprimir. Se recomienda el valor estándar de 1000 KB.

Acción al detectar

Puede definir acciones que Real-Time Protection debe ejecutar si se detecta un virus o un programa no deseado.

Interactivo

Si esta opción está activada, aparece una notificación en el escritorio en caso de una detección por parte de Real-Time Protection. Tiene la posibilidad de eliminar el malware encontrado o adoptar otras posibles acciones para el tratamiento de virus mediante el botón "**Detalles**". Las acciones se muestran en un cuadro de diálogo. Esta opción está activada de forma estándar.

Reparar

Real-Time Protection repara el archivo afectado, siempre que sea posible.

Cambiar el nombre

Real-Time Protection cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar el archivo y volver a cambiar el nombre posteriormente.

Cuarentena

Real-Time Protection mueve el archivo a la cuarentena. El gestor de cuarentena puede recuperarlo si tiene valor informativo o, en caso necesario, enviarlo al Avira Malware Research Center. En función del fichero, hay disponibles otras opciones en el Gestor de cuarentena (véase Gestor de cuarentena).

Eliminar

Se borra el archivo. Esta tarea es considerablemente más rápida que **Sobrescribir y eliminar** (véase más abajo).

Omitir

Está permitido acceder al archivo y salir de él.

Sobrescribir y eliminar

Real-Time Protection sobrescribe el fichero con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Advertencia
Si Real-Time Protection está ajustada en **Analizar al escribir**, no se crea el fichero afectado.

Predeterminado

Con ayuda de este botón, puede seleccionar la acción que debe estar activada por defecto en el cuadro de diálogo cuando se detecta un virus. Marque la acción debe estar activada por defecto y haga clic en el botón "**Predeterminado**".

Nota
No se puede seleccionar la acción **Reparar** como acción predeterminada.

Puede encontrar más información aquí.

Automático

Si esta opción está activada, cuando se detecta un virus o un programa no deseado, no aparece ningún cuadro de diálogo en el que se pueda seleccionar una acción. Real-Time Protection reacciona en función de la configuración que ha realizado en esta sección.

Copiar fichero a cuarentena antes de la acción

Si esta opción está activada, Real-Time Protection crea una copia de seguridad (backup) antes de realizar la acción principal o secundaria deseada. La copia de seguridad se guarda en la cuarentena. El gestor de cuarentena puede recuperarla si tiene valor informativo. Además, puede enviar la copia de seguridad al Centro de investigación de malware de Avira. En función del fichero, hay disponibles otras opciones en el Gestor de cuarentena (véase Gestor de cuarentena).

Mostrar mensajes de advertencia

Si esta opción está activada, cuando se detecta un virus o un programa no deseado, aparece un mensaje de advertencia.

Acción principal

La acción principal es aquella que se ejecuta cuando Real-Time Protection detecta un virus o un programa no deseado. Si se ha seleccionado la opción "**Reparar**", pero no es posible reparar el fichero afectado, se ejecuta la acción seleccionada en "**Acción secundaria**".

Nota
Solo puede seleccionarse la opción **Acción secundaria** si se ha seleccionado en **Acción principal** el ajuste **Reparar**.

Reparar

Si esta opción está activada, Real-Time Protection repara automáticamente los archivos afectados. Si Real-Time Protection no puede reparar el fichero afectado, ejecuta la acción seleccionada en **Acción secundaria**.

Nota
Se recomienda la reparación automática, pero eso significa que Real-Time Protection puede modificar los ficheros en el equipo.

Cambiar el nombre

Si esta opción está activada, Real-Time Protection cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar y volver a cambiar el nombre posteriormente.

Cuarentena

Si esta opción está activada, Real-Time Protection mueve el archivo al directorio de cuarentena. Estos ficheros pueden repararse posteriormente o, si fuera necesario, enviarse al Centro de investigación de malware de Avira.

Eliminar

Si esta opción está activada, se borra el fichero. Esta tarea es considerablemente más rápida que "Sobrescribir y eliminar".

Omitir

Si esta opción está activada, está permitido acceder al archivo y salir de él.

Advertencia
El archivo afectado permanece activo en su ordenador. Puede causar daños graves en su ordenador.

Sobrescribir y eliminar

Si esta opción está activada, Real-Time Protection sobrescribe el fichero con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Denegar acceso

Si esta opción está activada, Real-Time Protection registra la detección en el fichero de informe si está activada la función de informes. Además, Real-Time Protection registra una entrada en el registro de eventos si está activada esta opción.

Advertencia
Si Real-Time Protection está ajustada en **Analizar al escribir**, no se crea el fichero afectado.

Acción secundaria

Solo puede seleccionarse la opción "**Acción secundaria"** si se ha marcado en "**Acción principal"** la opción "**Reparar**". Con esta opción se decide qué debe hacerse si el fichero afectado no puede repararse.

Cambiar el nombre

Si esta opción está activada, Real-Time Protection cambia el nombre del archivo. Por tanto, ya no es posible acceder directamente a estos ficheros (p. ej., haciendo doble clic). Es posible reparar y volver a cambiar el nombre posteriormente.

Cuarentena

Si esta opción está activada, Real-Time Protection mueve el archivo a la cuarentena. Estos ficheros pueden repararse posteriormente o, si fuera necesario, enviarse al Centro de investigación de malware de Avira.

Eliminar

Si esta opción está activada, se borra el fichero. Esta tarea es considerablemente más rápida que "Sobrescribir y eliminar".

Omitir

Si esta opción está activada, está permitido acceder al archivo y salir de él.

Advertencia
El archivo afectado permanece activo en su ordenador. Puede causar daños graves en su ordenador.

Sobrescribir y eliminar

Si esta opción está activada, Real-Time Protection sobrescribe el fichero con un patrón estándar y, a continuación, lo borra. El archivo no se puede recuperar.

Denegar acceso

Si esta opción está activada, no se crea el fichero afectado. Real-Time Protection registra la detección únicamente en el fichero de informe si está activada la función de informes. Además, Real-Time Protection registra una entrada en el registro de eventos si está activada esta opción.

Nota
Si ha seleccionado como acción principal o secundaria **Eliminar** o **Sobrescribir y eliminar**, tenga en cuenta lo siguiente: en caso de detección

mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a la cuarentena.

Acciones adicionales

Usar registro de eventos

Si esta opción esta activada, se añade una entrada en el registro de eventos de Windows con cada detección. Se puede acceder a los eventos en el registro de eventos de Windows. Este ajuste está activado de forma estándar.

Excepciones

Estas opciones permiten configurar los objetos de excepción para Real-Time Protection (análisis en tiempo real). Los objetos en cuestión no se tienen en cuenta en el análisis en tiempo real. Mediante la lista de procesos omitidos, Real-Time Protection puede omitir sus accesos a ficheros durante el análisis en tiempo real. Esto resulta útil en el caso de bases de datos o de soluciones de copia de seguridad.

Tenga en cuenta lo siguiente al indicar los procesos y los ficheros que deben omitirse: la lista se procesa de arriba a abajo. Cuanto más larga es la lista, más tiempo se requiere para procesar la lista en cada acceso. Por lo tanto, se recomienda que las listas sean lo más cortas posible.

Procesos a excluir por Real-Time Protection

Todos los accesos de los procesos a ficheros que constan en esta lista se excluyen de la supervisión por parte de la Real-Time Protection.

Campo de entrada

En este campo se introduce el nombre del proceso que no debe considerarse durante el análisis en tiempo real. De forma predeterminada no hay ningún proceso indicado.

La ruta y el nombre de fichero del proceso indicados no pueden superar un máximo de 255 caracteres. Puede introducir un máximo de 128 procesos. Las entradas de la lista no puede superar el máximo de 6000 caracteres.

Durante la introducción del proceso,se aceptan caracteres Unicode. Por ello, puede indicar nombres de procesos o directorios que contienen caracteres especiales.

Las unidades se deben indicar de la siguiente forma: `[letra de la unidad]:\`

El carácter de dos puntos (:) solo puede utilizarse para indicar unidades.

Al introducir el proceso, puede utilizar los comodines * (varios caracteres) y ? (un único carácter):

```
C:\Archivos de programa\Aplicación\aplicación.exe
C:\Archivos de programa\Aplicación\aplicaci?.exe
C:\Archivos de programa\Aplicación\aplic*.exe
C:\Archivos de programa\Aplicación\*.exe
```

Para evitar que los procesos queden excluidos de forma global de la supervisión de la Real-Time Protection, se consideran no válidos los datos formados exclusivamente por los siguientes caracteres: * (asterisco), ? (signo de interrogación), / (barra), \ (barra invertida), . (punto), : (dos puntos).

Tiene la posibilidad de excluir procesos sin la indicación completa de la ruta de supervisión de Real-Time Protection: `aplicación.exe`.

No obstante, esto es válido exclusivamente para procesos cuyos ficheros ejecutables se encuentren en unidades del disco duro.

La indicación completa de la ruta se requiere en procesos cuyos ficheros ejecutables se encuentren en unidades conectadas, p. ej., unidades de red. Tenga en cuenta al respecto las indicaciones generales de la anotación de excepciones en unidades de red conectadas.

No indique ninguna excepción en procesos cuyos ficheros ejecutables se encuentren en unidades dinámicas. Las unidades dinámicas se utilizan para soportes de datos extraíbles como CD, DVD o lápices USB.

Advertencia
Tenga en cuenta que todos los accesos a ficheros iniciados por procesos y anotados en la lista se excluyen del análisis en busca de virus y programas no deseados.

Al pulsar este botón, se abre una ventana en la que puede seleccionar un fichero ejecutable.

Procesos

Mediante el botón "**Proceso"** se abre la ventana "*Selección de proceso"* en la que se muestran los procesos en curso.

Añadir

Con este botón, puede añadir el proceso seleccionado al campo que aparece en la ventana.

Eliminar

Con este botón, puede borrar el proceso seleccionado que aparece en la ventana.

Ficheros omitidos por la Real-Time Protection

Todos los accesos a objetos que constan en esta lista se excluyen de la supervisión por parte de la Real-Time Protection.

Campo de entrada

En este campo se introduce el nombre del fichero que no debe considerarse durante Real-Time Protection. De forma predeterminada no hay ningún fichero indicado.

Las entradas de la lista no pueden superar el máximo de 6000 caracteres.

Al introducir los ficheros que deben omitirse, puede utilizar los comodines * (varios caracteres) y ? (un único carácter). También se pueden excluir extensiones de fichero por separado (incluidos los comodines):

```
C:\Directorio\*.mdb
*.mdb
*.md?
*.xls*
C:\Directorio\*.log
```

Los nombres de los directorios deben acabar con una barra invertida (\).

Si se excluye un directorio, todos sus subdirectorios se excluyen automáticamente.

Por cada unidad puede indicar como máximo 20 excepciones con la ruta completa (empezando por la letra de la unidad).

Ejemplo: `C:\Archivos de programa\Aplicación\Nombre.log`

El número máximo de excepciones sin ruta completa es de 64. Ejemplo:

```
*.log
 \Equipo1\C\Directorio1
```

En el caso de unidades dinámicas que se integran (montan) como directorio en otra unidad, debe usar el alias del sistema operativo para la unidad integrada en la lista de excepciones:
p. ej., `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Si usa el punto de montaje (mount point) propiamente dicho, p. ej., `C:\DynDrive`, la unidad dinámica se analiza de todos modos. El fichero de informe de Real-Time Protection determinar el nombre del alias del sistema operativo que se debe usar.

Si se pulsa este botón, se abre una ventana en la que puede seleccionar el fichero que quiere que se omita.

Añadir

Este botón permite incluir en la ventana el fichero introducido en el campo de entrada.

Eliminar

Con el botón Eliminar, puede borrar el fichero seleccionado que aparece en la ventana.

Al indicar excepciones, tenga en cuenta lo siguiente:

Para excluir objetos a los que se tiene acceso con nombres de fichero DOS cortos (convención de nombres DOS 8.3), el nombre del fichero en cuestión también debe incluirse en la lista.

Un nombre de fichero que contenga un comodín no puede acabar con una barra invertida. Por ejemplo:
`C:\Archivos de programa\Aplicación\Aplic*.exe\`
Esta entrada no es válida y no se trata como una excepcion.

Para las **excepciones en unidades de red conectadas** debe considerarse lo siguiente: si usa la letra de unidad de la unidad de red conectada, los ficheros y directorios indicados NO se excluyen del análisis de Real-Time Protection. Si la ruta UNC de la lista de excepciones difiere de la ruta UNC que se usa para la conexión con la unidad de red (indicación de la dirección IP en la lista de excepciones, indicación del nombre del equipo para la conexión con la unidad de red), los directorios y ficheros indicados NO se excluyen del análisis de Real-Time Protection. El fichero de informe de Real-Time Protection permite determinar la ruta UNC que se debe usar:
`\\<Nombre del equipo>\<Recurso compartido>\` -O- `\\<Dirección IP>\<Recurso compartido>\`

Mediante el fichero de informe de Real-Time Protection puede determinar las rutas que usa Real-Time Protection al analizar la existencia de ficheros afectados. Use en principio las mismas rutas en la lista de excepciones. Proceda del modo siguiente: establezca la función de registro de Real-Time Protection en la configuración, en Informe en **Completo**. Si Real-Time Protection está activada, acceda a los ficheros, directorios, unidades incorporadas o unidades de red conectadas. Ahora puede leer la ruta que debe usarse en el fichero de informe de Real-Time Protection. El fichero de informe se activa en el Centro de control en Real-Time Protection.

Si administra el producto de Avira en AMC, puede utilizar variables en las indicaciones de rutas en caso de excepciones de procesos y ficheros. Puede encontrar una lista de las variables que se pueden utilizar en Variables: Excepciones de la Real-Time Protection y Scanner.

Ejemplos de procesos que deben omitirse

- `aplicación.exe`
  El proceso de aplicación.exe queda excluido del análisis de Real-Time Protection, independientemente de en qué unidad del disco duro y en qué directorio se encuentre aplicación.exe.
- `C:\Archivos de programas1\aplicación.exe`
  El proceso del fichero aplicación.exe, que se encuentra en la ruta C:\Archivos de programa1, queda excluido del análisis de Real-Time Protection.
- `C:\Archivos de programas1\*.exe`
  Todos los procesos de ficheros ejecutables, que se encuentran en la ruta C:\Archivos de programa1, quedan excluidos del análisis de Real-Time Protection.

Ejemplos de ficheros que deben omitirse

- `*.mdb`
  Todos los ficheros con la extensión de fichero '*mdb*' quedan excluidos del análisis de Real-Time Protection.
- `*.xls*`
  Todos los ficheros con la extensión de fichero '*xls*' quedan excluidos del análisis de Real-Time Protection, p. ej., archivos con las extensiones de fichero *.xls* y *xlsx*.
- `C:\Directorio\*.log`
  Todos los ficheros log con la extensión de fichero 'log' que se encuentran en la ruta *C:\Directorio* quedan excluidos del análisis de Real-Time Protection.
- `\\Nombre del equipo1\Recurso compartido1\`
  Quedan excluidos del análisis de Real-Time Protection todos los ficheros a los que se accede con una conexión '*\\Nombre del equipo1\Recurso compartido1*'. Se trata generalmente de una unidad de red conectada que accede a otro ordenador con directorio compartido mediante el nombre de equipo '*Nombre del equipo1*' y el nombre de recurso compartido '*Recurso compartido1*'.
- `\\1.0.0.0\Recurso compartido1\*.mdb`
  Quedan excluidos del análisis de Real-Time Protection todos los ficheros con la extensión 'mdb' a los que se accede con una conexión '*\\1.0.0.0\Recurso compartido1*'. Se trata generalmente de una unidad de red conectada que accede a otro ordenador con directorio compartido con la dirección IP '1.0.0.0' y el nombre de recurso compartido '*Recurso compartido1*'.

Heurística

Esta sección de configuración trata sobre la configuración de la heurística del motor de análisis.

Los productos de Avira integran heurísticas muy potentes con las que se puede detectar de forma proactiva el malware desconocido, es decir, antes de que se cree una firma de virus especial contra el parásito y se envíe una actualización de la protección frente a los virus. Los virus se detectan gracias a un análisis y un examen exhaustivos del código afectado de acuerdo con las funciones habituales del malware. Si el código analizado cumple estas características, se considera sospechoso. Sin embargo, esto no significa necesariamente que el código sea malware; también se pueden producir falsas alarmas. El usuario es responsable de decidir qué debe hacerse con el código afectado, p. ej., basándose en sus conocimientos de si la fuente que contiene el código afectado es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto de Avira integra una heurística de macrovirus muy potente. Si esta opción está activada, durante una posible reparación se borran todas las macros del documento afectado o bien se muestra una notificación acerca de los documentos

sospechosos, es decir, se muestra una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Advanced Heuristic Analysis and Detection (AHeAD)

Activar AHeAD

Su programa de Avira incorpora en la tecnología AHeAD de Avira una heurística muy potente que puede detectar también el malware desconocido (nuevo). Si esta opción está activada, aquí puede ajustar hasta qué punto es "precisa" esta heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si esta opción está activada, se detecta en menor medida el malware desconocido, pero se reduce el riesgo de posibles falsos positivos.

Nivel de detección medio

Si esta opción está activada, se garantiza una protección equilibrada con pocos falsos positivos. Este ajuste está activado de forma estándar si ha seleccionado que se aplique esta heurística.

Nivel de detección alto

Si esta opción está activada, el malware desconocido se detecta en mayor medida, pero se debe contar con falsos positivos.

8.3.2 Informe

Real-Time Protection cuenta con una completa función de registro que puede proporcionar al usuario o al administrador información exacta acerca del tipo y la forma de una detección.

Protocolización

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Si esta opción está activada, Real-Time Protection no crea ningún registro. Renuncie a realizar el registro solo en casos excepcionales, por ejemplo, solo si realiza pruebas con muchos virus o programas no deseados.

Predeterminado

Si esta opción está activada, Real-Time Protection incluye información importante (sobre la detección, advertencias y errores) en el fichero de registro; la información de menor importancia se ignora para mayor claridad. Este ajuste está activado de forma estándar.

Extendido

Si esta opción está activada, Real-Time Protection registra también información secundaria en el fichero de informe.

Completo

Si esta opción está activada, Real-Time Protection registra toda la información (también el tamaño y el tipo del archivo, la fecha, etc.) en el fichero de informe.

Limitar fichero de informe

Limitar tamaño a n MB

Si esta opción está activada, el fichero de informe se limita a un tamaño determinado; valores posibles: 1 a 100 MB. Cuando se limita el fichero de informe, se reserva un espacio aproximado de 50 kilobytes, con el fin de limitar la carga del equipo. Si el archivo de registro supera el tamaño indicado en 50 kilobytes, se borran automáticamente las entradas grandes antiguas hasta que el tamaño indicado se haya reducido en menos de 50 kilobytes.

Guardar fichero de informe antes de reducir

Si esta opción está activada, se guarda el fichero de informe antes de reducirlo. Consulte la ubicación del archivo en Directorio de informes.

Escribir configuración en fichero de informe

Si esta opción está activada, la configuración empleada del análisis en tiempo real se registra en el fichero de informe.

Nota
Si no ha indicado ninguna limitación del fichero de informe, se crea de forma automática un nuevo fichero de informe cuando este haya alcanzado un tamaño de 100 MB. Se conservan hasta tres copias de seguridad de los ficheros de informe antiguos. Se conservan hasta tres copias de seguridad de los ficheros de informe antiguos. Las copias de seguridad más antiguas son las que primero se borran.

8.4 Variables: Excepciones de Real-Time Protection y de Scanner

Si administra el producto de Avira en AMC, puede utilizar variables cuando se introducen las excepciones de la Real-Time Protection y Scanner. Al guardar la configuración en el equipo administrado, las variables se sustituyen por valores adecuados al sistema operativo y el idioma del sistema operativo.

Es posible emplear las variables siguientes:

8.4.1 Variables en Windows XP 32-Bit (**inglés)

Variable	Variables en Windows XP 32-Bit (**inglés)
%WINDIR%	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\Documents and Settings\All Users* **
%PROGRAMFILES%	*C:\Program Files* **
%PROGRAMFILES(x86)%	*C:\Program Files (x86)* **
%SYSTEMROOT%	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\Documents and Settings\All Users\Avira\AntiVir Desktop* **

Las rutas marcadas con **** varían en función del idioma. Se han utilizado como ejemplos las rutas de sistemas operativos en inglés.

8.4.2 Variables en Windows 7 32-Bit/ 64-Bit (**inglés)

Variable	Windows 7 32-Bit (**inglés)	Windows 7 64-Bit (**inglés)
%WINDIR%	*C:\Windows*	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\ProgramData*	*C:\ProgramData*
%PROGRAMFILES%	*C:\Program Files* **	*C:\Program Files* **

%PROGRAMFILES(x86)%	*C:\Program Files (x86) **	*C:\Program Files (x86) **
%SYSTEMROOT%	*C:\Windows*	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop **	*C:\Program Files (x86)\Avira\Antivir Desktop **
%AVAPPDATA%	*C:\ProgramData\Avira\AntiVir Desktop*	*C:\ProgramData\Avira\AntiVir Desktop*

Las rutas marcadas con **** varían en función del idioma. Se han utilizado como ejemplos las rutas de sistemas operativos en inglés.

8.5 Actualización

En la sección **Actualización** puede configurar la ejecución automática de las actualizaciones y la conexión a los servidores de descarga. Tiene la posibilidad de ajustar diferentes intervalos de actualización, así como la activación y la desactivación de las actualizaciones automáticas.

> **Nota**
> Si configura su producto de Avira en la Consola de administración de Avira, no está disponible la configuración de la actualización automática.

Actualización automática

Activar

Si esta opción está activada, se ejecutan actualizaciones automáticas en el intervalo de tiempo indicado y para los eventos activados.

Todos n días/horas/minutos

En este campo puede indicar el intervalo con el que deberán ejecutarse las actualizaciones automáticas. Para modificar el intervalo de actualización, seleccione una de las entradas de datos en el campo y modifíquela mediante los botones de flecha a la derecha del campo de introducción.

Iniciar tarea adicionalmente al conectarse a Internet

Si esta opción está activada, además del intervalo de actualización configurado, la tarea de actualización se ejecuta en cada inicio de una conexión a Internet.

Repetir la tarea si el tiempo ya transcurrió

Si esta opción está activada, se realizan las tareas de actualización pasadas que no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.

Descarga

A través de servidor web

La actualización se ejecuta a través de un servidor web mediante conexión HTTP. Podrá utilizar un servidor web del fabricante o un servidor web en Intranet que recibe los ficheros de actualización de un servidor web del fabricante en Internet.

Nota
Encontrará una configuración adicional para la actualización a través de un servidor web en: Configuración > Seguridad del PC > Actualización > Servidor web.
Configure el servidor web y, si es necesario, el servidor proxy cuando active esta opción.

A través de servidor de ficheros/carpetas compartidas

La actualización se produce a través de un servidor de ficheros en Intranet que recibe los ficheros de actualización de un servidor de descargas del fabricante en Internet.

Nota
Encontrará configuraciones adicionales para la actualización a través de un servidor de ficheros en: Configuración > Seguridad del PC > Actualización > Servidor de ficheros.
Configure el servidor web y, si fuera el caso, el servidor proxy cuando active esta opción.

8.5.1 Servidor de ficheros

Si hay varios ordenadores en una red, su producto de Avira puede descargar una actualización de un servidor de ficheros en Intranet, que recibe los ficheros de actualización de un servidor de descargas del fabricante en Internet. De esta forma, es posible garantizar la actualidad de los productos de Avira en todos los equipos sin consumir muchos recursos. (Opciones disponibles solo si el modo experto está activado.)

Nota
La sección de configuración solo está activada si en Configuración > Seguridad del PC > Actualización se ha seleccionado la opción **A través de servidor de ficheros/carpetas compartidas**.

Descarga

Servidor de ficheros

Indique el servidor de ficheros en el que se encuentran los archivos de actualización de su producto de Avira, así como los directorios necesarios '*/release/update/*'. Se precisa la siguiente información: `file://<dirección IP del servidor de ficheros>/release/update/`. El directorio '*release*' debe ser accesible para todos los usuarios.

...

El botón abre una ventana en la que puede seleccionar el directorio de descarga deseado.

Inicio de sesión en servidor

Nombre de inicio de sesión

Introduzca un nombre de usuario para conectarse al servidor. Utilice una cuenta de usuario con derechos de acceso al directorio utilizado y compartido en el servidor.

Contraseña

Introduzca aquí la contraseña de la cuenta de usuario utilizada. Los caracteres introducidos se enmascaran con *.

Nota
Si no introduce ningún dato en el área *Inicio de sesión en servidor*, no se utiliza autenticación durante el acceso al servidor de ficheros. En este caso, el usuario debe de tener suficientes derechos en el servidor de ficheros.

8.5.2 Servidor Web

Servidor web

La actualización puede realizarse desde un servidor de web en Internet o Intranet.

Conexión al servidor web

Utilizar la conexión existente (red)

Este ajuste se muestra cuando su conexión se utiliza a través de una red.

Utilizar la siguiente conexión

Este ajuste se muestra si define su conexión de forma individual.

El Updater detecta automáticamente las conexiones disponibles. Las conexiones que no están disponibles aparecen en color gris y no pueden activarse. Puede crear una conexión de acceso telefónico a redes, por ejemplo, manualmente mediante una entrada de la agenda en Windows.

Usuario

Introduzca el nombre de usuario de la cuenta seleccionada.

Contraseña

Introduzca la contraseña de esta cuenta. Como medida de seguridad, los caracteres que introduce en este campo se sustituyen por asteriscos (*).

Nota
Si ha olvidado el nombre de usuario o la contraseña de una cuenta de Internet, contacte con su proveedor de servicios de Internet.

Nota
La marcación telefónica automática de Updater por medio de herramientas de marcación telefónica (p. ej., SmartSurfer, Oleco...) todavía no está disponible.

Finalizar la conexión de acceso telefónico a redes que se inició para la actualización

Si la opción está activada, la conexión de acceso telefónico a redes abierta para la actualización se cierra automáticamente tan pronto como la descarga finaliza correctamente.

Nota
Esta opción solo está disponible con Windows XP. A partir de Window Vista, la conexión de acceso telefónico a redes abierta para la actualización siempre finaliza en cuanto la descarga se haya ejecutado.

Descarga

Servidor priorit.

En este campo se indica la dirección (URL) del servidor wb al cual se envía la solicitud de actualización en primer lugar, así como el directorio de actualización necesario. Si este servidor no está disponible, la solicitud se pasa a los servidores estándar indicados. Es válida la siguiente indicación del servidor web: `http://<Dirección del servidor web>[:Puerto]/actualizar`. Si no introduce ningún puerto, se utiliza el puerto 80.

Servidor predeterminado

Aquí se introducen las direcciones (URL) de los servidores web desde los cuales se descargan las actualizaciones, así como el directorio de actualización '`update`'. Es válida la siguiente indicación del servidor web: `http://<Dirección del servidor web>[:Puerto]/actualizar`. Si no introduce ningún puerto, se utiliza el puerto 80. De forma estándar, constan los servidores web disponibles de Avira para

actualizar. No obstante, también puede utilizar servidores web propios, por ejemplo en Intranet. En caso de indicar más de un servidor web, los servidores se separan mediante comas.

Predeterminado

El botón restablece las direcciones predefinidas.

Configuración del proxy

Servidor proxy

No usar servidor proxy

Si esta opción está activada, su conexión a Internet no se lleva a través de un servidor proxy.

Utilizar la configuración del sistema de Windows

Si esta opción está activada, un servidor proxy establece su conexión al servidor web mediante la configuración de sistema de Windows. El sistema de Windows para utilizar un servidor proxy se configura en **Panel de control > Opciones de Internet > Conexiones > Configuración de LAN**. En Internet Explorer también se puede acceder a Opciones de Internet en el menú **Herramientas**.

Advertencia
Si utiliza un servidor proxy que requiere autenticación, indique los datos completos en la opción **Conexión a través de este servidor proxy**. La opción **Utilizar la configuración del sistema de Windows** solo se puede utilizar para servidores proxy sin autenticación.

Conexión a través de este servidor proxy

Si su conexión al servidor web se configura a través de un servidor proxy, introduzca aquí la información necesaria.

Dirección

Introduzca el nombre del equipo o la dirección IP del servidor proxy que desea usar para conectar al servidor web.

Puerto

Introduzca el número de puerto del servidor proxy que desea utilizar para conectar con el servidor web.

Nombre de inicio de sesión

Introduzca un nombre de usuario para entrar al servidor proxy.

Contraseña de inicio de sesión

Introduzca aquí la contraseña correspondiente para el registro en el servidor proxy. Como medida de seguridad, los caracteres que introduce en este campo se sustituyen por asteriscos (*).

Ejemplos:

Dirección: `proxy.domain.de` Puerto: `8080`

Dirección: `192.168.1.100` Puerto: `3128`

8.6 FireWall

8.6.1 Configurar el FireWall

Avira Professional Security le permite configurar Avira FireWall o Windows Firewall:

- Avira FireWall
- Avira FireWall en AMC
- FireWall de Windows

8.6.2 Avira FireWall

La sección **FireWall** en **Configuración > Seguridad en Internet** sirve para configurar Avira FireWall en los sistemas operativos hasta Windows 7.

Reglas del adaptador

Para FireWall de Avira un adaptador representa un dispositivo de hardware simulado (p. ej., Miniport, Bridge Connection, etc.) o un dispositivo de hardware real (p. ej., una tarjeta de red).

FireWall de Avira muestra las reglas de todos los adaptadores existentes en el equipo para los que se ha instalado un controlador.

- Protocolo ICMP
- Escaneado de puertos TCP
- Escaneado de puertos UDP
- Reglas entrantes
- Reglas salientes
- Botones

Las reglas del adaptador predefinidas dependen del nivel de seguridad. Puede cambiar el *Nivel de seguridad* en la sección **Seguridad en Internet > FireWall** del Centro de control o ajustar las reglas del adaptador a sus necesidades. Si ha adaptado las reglas del

adaptador a sus necesidades, en la sección FireWall del centro de control en el área *Nivel de seguridad* el regulador se ajusta a **Personalizada**.

> **Nota**
> El ajuste predeterminado del Nivel de seguridad para todas las reglas predefinidas de FireWall de Avira es **Medio**.

Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP) se emplea en redes para intercambiar mensajes de error e informativos. El protocolo se utiliza también para mensajes de estado mediante Ping o Tracert.
Con esta regla se pueden definir los tipos de ICMP entrantes y salientes que deben bloquearse, ajustar los parámetros para el desbordamiento y definir el comportamiento si existen paquetes ICMP fragmentados. Esta regla sirve para evitar los denominados ataques en desbordamiento ICPM que pueden causar una carga o sobrecarga del procesador del ordenador atacado, ya que se contesta a todos los paquetes.

Reglas predefinidas para el protocolo ICMP

Configuración	Reglas
Bajo	Bloquea tipos entrantes: **sin tipo**. Bloquea tipos salientes: **sin tipo**. Asumir desbordamiento si el retraso entre paquetes es inferior a **50** milisegundos. **Rechazar** paquetes ICMP fragmentados.
Medio	Las mismas reglas que para el ajuste *Bajo*.
Alto	Bloquea tipos entrantes: **varios tipos**. Bloquea tipos salientes: **varios tipos**. Asumir desbordamiento si el retraso entre paquetes es inferior a **50** milisegundos. **Rechazar** paquetes ICMP fragmentados.

Bloquea tipos entrantes: sin tipo/varios tipos.

Al hacer clic en el enlace, se abre una lista con los tipos de paquetes ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP entrantes que desee bloquear.

Bloquea tipos salientes: sin tipo/varios tipos.

Al hacer clic en el enlace, se abre una lista con los tipos de paquetes ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP salientes que desee bloquear.

Sospechar desbordamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede introducir el máximo retraso permitido de ICMP.

Paquetes ICMP fragmentados

Al hacer clic en el enlace, tiene la posibilidad de "**rechazar**" y "**no rechazar**" los paquetes ICMP fragmentados.

Escaneado de puertos TCP

Con esta regla se define cuándo FireWall debe suponer que existe un escaneado de puertos TCP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneado de puertos TCP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles de un equipo a través de los cuales se lanzan ataques posiblemente mucho más dañinos.

Reglas predeterminadas para el escaneado de puertos TCP

Configuración	Reglas
Bajo	Suponer que existe escaneado de puertos TCP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos TCP, **escribir en fichero de informe** la dirección IP del atacante y **no añadir** las reglas para bloquear el ataque.
Medio	Suponer que existe escaneado de puertos TCP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos TCP, **escribir en fichero de informe** la dirección IP del atacante y **añadir** las reglas para bloquear el ataque.
Alto	Las mismas reglas que para el ajuste *Medio*.

Puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos TCP.

Ventana de tiempo de escaneado de puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos TCP.

Base de datos de eventos

Al hacer clic en este enlace, puede decidir si se registra o no en la base de datos de eventos la dirección IP del atacante.

Regla

Al hacer clic en este enlace, tiene la opción de decidir si se añade o no la regla de bloqueo de ataques por escaneo de puertos TCP.

Escaneado de puertos UDP

Con esta regla se define cuándo FireWall debe suponer que existe un escaneado de puertos UDP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneado de puertos UDP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles de un equipo a través de los cuales se lanzan ataques posiblemente mucho más dañinos.

Reglas predeterminadas para el escaneado de puertos UDP

Configuración	Reglas
Bajo	Suponer que existe escaneado de puertos UDP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos UDP, **escribir en fichero de informe** la dirección IP del atacante y **no añadir** las reglas para bloquear el ataque.
Medio	Suponer que existe escaneado de puertos UDP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos TCP, **escribir en fichero de informe** la dirección IP del atacante y **añadir** las reglas para bloquear el ataque.
Alto	La misma regla que para el ajuste *Medio*.

Puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos UDP.

Ventana de tiempo de escaneado de puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos UDP.

Base de datos de eventos

Al hacer clic en este enlace, puede decidir si se registra o no en la base de datos de eventos la dirección IP del atacante.

Regla

Al hacer clic en este enlace, tiene la opción de decidir si se añade o no la regla de bloqueo de ataques por escaneo de puertos UDP.

Reglas entrantes

Las reglas entrantes sirven para controlar el tráfico entrante mediante FireWall de Avira.

Advertencia
Cuando se filtra un paquete, las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Reglas predeterminadas para el monitor de tráfico TCP

Configuración	Reglas
Bajo	No se bloquea el tráfico entrante por parte de FireWall de Avira.
Medio	• **Permitir conexión TCP establecida en puerto 135** **Permitir** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{135}** y el puerto remoto en **{0-65535}**. Aplicar para **paquetes en las conexiones existentes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • **Denegar paquetes TCP en puerto 135** **Denegar** los paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{135}** y el puerto remoto en **{0-65535}**. Aplicar para **todos los paquetes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • **Monitorizar el tráfico de datos conforme a TCP** **Permitir** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar al **inicio del establecimiento de la conexión y a paquetes de conexiones existentes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • **Denegar todos los paquetes TCP** **Denegar** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar para **todos los paquetes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Alto	**Monitorizar tráfico de datos TCP admitido** **Permitir** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar para **paquetes en las conexiones existentes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Aceptar/denegar paquetes TCP

Al hacer clic en el enlace, tiene la opción de decidir si desea permitir o denegar paquetes TCP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Puertos locales

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos locales y también rangos de puertos completos.

Puertos remotos

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos remotos y también rangos de puertos completos.

Método de aplicación

Al hacer clic en este enlace, puede decidir si la regla se aplica a paquetes de conexiones existentes, en el inicio de las conexiones y a paquetes de conexiones existentes o a todas las conexiones.

Base de datos de eventos

Al hacer clic en este enlace, puede decidir si se debe generar una base de datos de eventos cuando el paquete cumpla con la regla.

Extendido

La opción **Ampliado** permite el filtrado basándose en el contenido. Por ejemplo, se pueden rechazar los paquetes que contienen datos específicos con un determinado

desplazamiento. Si no desea utilizar esta opción, no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: bytes

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico.

Filtrado por contenido: máscara

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene la máscara específica.

Filtrado por contenido: desplazamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del contenido filtrado. El desplazamiento se calcula desde donde termina el encabezamiento TCP.

Reglas predeterminadas para el monitor de tráfico UDP

Configuración	Reglas
Bajo	-
Medio	• **Monitorizar el tráfico de datos conforme a UDP** **Permitir** paquetes UDP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar a **puertos abiertos** para **todos los flujos de datos**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • **Denegar todos los paquetes UDP** **Denegar** paquetes UDP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar en **todos los puertos** para **todos los flujos de datos**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Alto	**Monitorizar tráfico de datos UDP admitido** **Permitir** paquetes UDP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{53, 67, 68, 88,...}**. Aplicar a **puertos abiertos** para **todos los flujos de datos**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Aceptar/denegar paquetes UDP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes UDP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Puertos locales

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos locales y también rangos de puertos completos.

Puertos remotos

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos remotos y también rangos de puertos completos.

Método de aplicación

Puertos

Al hacer clic en este enlace, puede elegir la aplicación de esta regla a todos los puertos o solo a los abiertos.

Flujos de datos

Al hacer clic en este enlace, puede elegir la aplicación de esta regla a todos los flujos de datos o solo a los flujos de datos salientes.

Base de datos de eventos

Al hacer clic en este enlace, puede decidir si se debe generar una base de datos de eventos cuando el paquete cumpla con la regla.

Extendido

La opción **Ampliado** permite el filtrado basándose en el contenido. Por ejemplo, se pueden rechazar los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción, no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: bytes

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico.

Filtrado por contenido: máscara

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene la máscara específica.

Filtrado por contenido: desplazamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del contenido filtrado. El desplazamiento se calcula desde donde termina el encabezamiento UDP.

Reglas predeterminadas para el monitor de tráfico ICMP

Configuración	Reglas
Bajo	-
Medio	**No descartar paquetes ICMP sobre la base de la dirección IP** **Permitir** paquetes ICMP de la dirección **0.0.0.0** con la máscara **0.0.0.0**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.
Alto	La misma regla que para el ajuste *Medio*.

Aceptar/denegar paquetes ICMP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes ICMP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 deseada.

Base de datos de eventos

Al hacer clic en este enlace, puede decidir si se debe generar una base de datos de eventos cuando el paquete cumpla con la regla.

Extendido

La opción **Ampliado** permite el filtrado basándose en el contenido. Por ejemplo, se pueden rechazar los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción, no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: bytes

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico.

Filtrado por contenido: máscara

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene la máscara específica.

Filtrado por contenido: desplazamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del contenido filtrado. El desplazamiento se calcula desde donde termina el encabezamiento ICMP.

Reglas predeterminadas para los paquetes IP

Configuración	Reglas
Bajo	-
Medio	-
Alto	**Denegar todos los paquetes IP** **Denegar** paquetes **IPv4** de la dirección **0.0.0.0** con la máscara **0.0.0.0**. **No escribir en fichero de informe** cuando el paquete cumpla la regla.

Permitir/denegar

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes IP especialmente definidos.

IPv4/IPv6

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Base de datos de eventos

Al hacer clic en este enlace, puede decidir si se debe generar una base de datos de eventos cuando el paquete cumpla con la regla.

Reglas salientes

Las reglas salientes sirven para controlar el tráfico saliente mediante FireWall de Avira. Puede definir una regla saliente para los siguientes protocolos: IP, ICMP, UDP y TCP.

Advertencia
Cuando se filtra un paquete, las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Botones

Botón	Descripción
Añadir	Permite crear una nueva regla. Al hace clic en este botón, aparece el cuadro de diálogo "Añadir nueva regla". En este cuadro de diálogo puede seleccionar nuevas reglas.
Suprimir	Elimina la regla seleccionada.
Subir	La regla seleccionada se desplaza una posición hacia arriba, por lo que aumenta su prioridad.
Bajar	La regla seleccionada se desplaza una posición hacia abajo, por lo que disminuye su prioridad.

Cambiar el nombre	Permite cambiar el nombre de la regla seleccionada.

Nota
Puede añadir nuevas reglas para cada adaptador o para todos los adaptadores del equipo. Para añadir una regla del adaptador para todos los adaptadores, seleccione **Puesto de trabajo** en la estructura del adaptador que se muestra y haga clic en el botón **Añadir**. Consulte Añadir nueva regla.

Nota
Para cambiar la posición de una regla, también puede arrastrarla con el ratón a la posición pertinente.

Añadir nueva regla

En esta ventana puede seleccionar nuevas reglas entrantes y salientes. La regla seleccionada se adopta con los datos predeterminados en la ventana **Reglas del adaptador** y ahí puede continuar especificándose. Además de las reglas entrantes y salientes, dispone de otras reglas.

Posibles reglas

Permitir red punto a punto

Permite conexiones punto a punto: comunicación TCP entrante en el puerto 4662 y comunicación UDP entrante en el puerto 4672.

Puerto TCP

Al hacer clic en el enlace, aparece un cuadro de diálogo en el que puede indicar el puerto TCP permitido.

Puerto UDP

Al hacer clic en el enlace, aparece un cuadro de diálogo en el que puede indicar el puerto UDP permitido.

Permitir conexiones VMWARE

Permite la comunicación entre sistemas VMWare.

Bloquear dirección IP

Bloquea todo el tráfico de una determinada dirección IP.

Versión IP

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Bloquear subred

Bloquea todo el tráfico de una determinada dirección IP y una máscara de subred.

Versión IP

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP deseada.

Máscara de subred

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la máscara de subred deseada.

Permitir dirección IP

Permite todo el tráfico de una determinada dirección IP.

Versión IP

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP deseada.

Permitir subred

Permite todo el tráfico de una determinada dirección IP y una máscara de subred.

Versión IP

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP deseada.

Máscara de subred

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la máscara de subred deseada.

Permitir servidor web

Permite la comunicación de un servidor web en el puerto 80: comunicación TCP entrante en el puerto 80.

Puerto

Al hacer clic en el enlace, aparece un cuadro de diálogo en el que puede indicar el puerto usado por el servidor web.

Permitir conexiones VPN

Permite conexiones VPN (Virtual Private Network) con una IP determinada: tráfico de datos UDP entrante en x puertos, tráfico de datos TCP entrante en x puertos, tráfico de datos IP entrante con los protocolos ESP(50), GRE (47).

Versión IP

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP deseada.

Permitir conexión de "escritorio remoto"

Permite conexiones de "escritorio remoto" (Remote Desktop Protocol) en el puerto 3389.

Puerto

Al hacer clic en el enlace, aparece un cuadro de diálogo en el que puede indicar el puerto que se usa para la conexión de escritorio remoto permitida.

Permitir conexiones VNC

Permite conexiones VNC (Virtual Network Computing) en el puerto 5900

Puerto

Al hacer clic en el enlace, aparece un cuadro de diálogo en el que puede indicar el puerto que se usa para la conexión VNC permitida.

Permitir uso compartido de ficheros e impresoras

Permite el acceso al uso compartido de impresoras y ficheros: tráfico de datos TCP entrante en los puertos 137, 139 y tráfico de datos UDP entrante en el puerto 445 desde cualquier dirección IP.

Posibles reglas entrantes

- **Regla IP entrante**
- **Regla ICMP entrante**
- **Regla UDP entrante**
- **Regla TCP entrante**

- **Regla de protocolo IP entrante**

Posibles reglas salientes

- **Regla IP saliente**
- **Regla ICMP saliente**
- **Regla UDP saliente**
- **Regla TCP saliente**
- **Regla de protocolo IP saliente**

> **Nota**
> Las opciones de las posibles reglas entrantes y salientes son idénticas a las opciones de las reglas predefinidas de los correspondientes protocolos (consulte FireWall > Reglas del adaptador).

Botones

Botón	Descripción
Aceptar	La regla seleccionada se incorpora como nueva regla del adaptador.
Cancelar	La ventana se cierra sin añadir ninguna regla nueva.

Reglas de aplicación

Reglas de aplicación para el usuario

En esta lista se incluyen todos los usuarios del sistema. Si ha iniciado sesión como administrador, puede seleccionar un usuario para el que desea crear reglas. Si no es un usuario con privilegios, solo puede ver el usuario identificado actualmente.

Aplicación

Esta tabla muestra la lista de aplicaciones para las que se han definido reglas. Esta lista de aplicaciones contiene la configuración de cada aplicación que se ha ejecutado y que tenía una regla asociada desde que se ha instalado Avira FireWall.

Vista Normal

Columna	Descripción
Aplicación	Nombre de la aplicación
Conexiones activas	Número de las conexiones activas abiertas por la aplicación.
Acción	Muestra la acción que Avira FireWall realiza automáticamente cuando la aplicación utiliza la red de cualquier forma. Si hace un clic en el enlace, puede cambiar a otro tipo de acción. Es posible seleccionar los tipos de acción **Preguntar**, **Permitir** o **Rechazar**. La acción predeterminada es **Preguntar.**

Configuración avanzada

Si desea regular de forma personalizada los accesos de red de una aplicación, puede crear reglas de aplicación específicas basadas en los filtros de paquete de manera similar a las reglas del adaptador.

- En **Configuración > Seguridad en Internet > FireWall > Configuración** cambie la configuración de *Reglas de aplicación*: active la opción **Configuración avanzada** y guarde la configuración mediante **Aplicar** o **Aceptar**.
  - En **Configuración > Seguridad en Internet > FireWall > Reglas de aplicación** en la lista de las reglas de aplicación se muestra una columna adicional, **Filtrado** con la entrada **Simple**.

Columna	Descripción
Aplicación	Nombre de la aplicación.
Conexiones activas	Número de las conexiones activas abiertas por la aplicación.

Acción	Muestra la acción que FireWall de Avira realiza automáticamente cuando la aplicación utiliza la red de cualquier forma. En la configuración **Filtrado - Simple** puede cambiar a otro tipo de acción haciendo clic en el enlace. Es posible seleccionar los tipos de acción **Preguntar**, **Permitir** y **Rechazar**. En la configuración **Filtrado - Ampliado** se muestra el tipo de acción **Reglas**. Mediante el enlace **Reglas** se abre la ventana **Reglas de aplicación avanzadas**, donde puede guardar reglas de aplicación específicas.
Filtrado	Muestra el tipo de filtrado. Si hace un clic en el enlace, puede cambiar a otro tipo de filtrado. **Simple**: en el filtrado simple la acción indicada se ejecuta en cualquier actividad de red de la aplicación de software. **Ampliado**: durante el filtrado se ejecutan las reglas que se hayan guardado en la configuración avanzada.

- Si quiere crear reglas de aplicación especificadas para una aplicación, en **Filtrado** cambie a la entrada **Ampliado**.
  - ↪ En la columna **Acción** se muestra ahora la entrada **Reglas**.
- Haga clic en **Reglas** para acceder a la ventana para la creación de reglas de aplicación específicas.

Reglas de aplicación especificas en la configuración avanzada

Con las reglas de aplicación especificadas puede permitir o rechazar el tráfico de datos especificado de la aplicación, así como permitir o rechazar la escucha pasiva de determinados puertos. Dispone de las opciones siguientes:

Permitir/rechazar la inyección de código

La inyección de código es una técnica con la que se ejecuta un código en el ámbito de direcciones de otro proceso obligando a ese proceso a cargar una biblioteca de vínculos dinámicos (DLL). El malware, entre otros, utiliza la técnica de inyección de código para ejecutar su propio código de forma encubierta por otro programa. De este modo, es posible encubrir accesos a Internet ante FireWall. De forma estándar se permite la inyección de código a todas las aplicaciones firmadas.

Permitir o rechazar la escucha pasiva de puertos de la aplicación

Permitir o rechazar el tráfico de datos:

Permitir o rechazar los paquetes IP entrantes y/o salientes

Permitir o rechazar los paquetes TCP entrantes y/o salientes

Permitir o rechazar los paquetes UDP entrantes y/o salientes

Puede crear tantas reglas como desee para cada aplicación. Las reglas de aplicación se ejecutan en el orden mostrado (puede encontrar más información en Reglas de aplicación avanzadas).

Nota
Si modifica el filtrado de **Ampliado** a **Simple** en una regla de aplicación, las reglas de aplicación ya creadas no se eliminan definitivamente en la configuración avanzada, sino que solo se desactivan. Si vuelve a cambiar al filtrado **Ampliado**, las reglas de aplicación ya creadas se activan de nuevo y se muestran en la ventana de la configuración avanzada para **Reglas de aplicación**.

Detalles de aplicación

En esta sección puede ver los detalles de la aplicación seleccionada en la lista de aplicaciones.

- *Nombre*: nombre de la aplicación.
- *Ruta*: ruta hasta el archivo ejecutable de la aplicación.

Botones

Botón	Descripción
Añadir aplicaciones	Permite la creación de una nueva regla. Si hace clic en este botón, se abre un cuadro de diálogo. Aquí puede seleccionar la aplicación para la que se va a crear una nueva regla.
Suprimir regla	Elimina la regla de aplicación seleccionada.
Mostrar detalles	En la ventana *Propiedades* se muestra información detallada acerca de la aplicación que ha seleccionado en la lista.
Volver a cargar	Refresca la lista de aplicaciones y simultáneamente descarta los cambios que haya hecho en las reglas.

Reglas de aplicación avanzadas

En la ventana **Reglas de aplicación avanzadas** puede crear reglas específicas para el tráfico de datos de aplicaciones y para la escucha de puertos. Para crear una regla nueva, pulse el botón **Añadir**. En la parte inferior de la ventana puede ampliar la especificación de la regla. Puede crear tantas reglas como desee para cada aplicación. Las reglas se ejecutan en el orden mostrado. Los botones **Subir** y **Bajar** permiten cambiar el orden de las reglas.

> **Nota**
> Para cambiar la posición de una regla de aplicación, también puede arrastrarla con el ratón a la posición pertinente.

Detalles de aplicación

En la zona de detalles de aplicación se muestra información sobre la aplicación seleccionada:

- *Nombre*: nombre de la aplicación.
- *Ruta*: ruta hasta el archivo ejecutable de la aplicación.

Opciones de las reglas

Permitir/rechazar la inyección de código

Si hace clic en el enlace, puede determinar si se permite o deniega la inyección de código en la aplicación seleccionada.

Tipo de regla: tráfico/escuchar

Si hace clic en el enlace, puede determinar si la regla se crea para el tráfico de datos o la escucha de puertos.

Acción: permitir/rechazar

Si hace clic en el enlace, puede determinar la acción que se ejecuta con la regla.

Puerto

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar el puerto local al que se refiere la regla de escucha. También puede indicar varios puertos o rangos de puertos.

Paquetes salientes, entrantes, todos los paquetes

Si hace clic en el enlace, puede determinar si la regla de tráfico supervisa todos los paquetes, solo los salientes o solo los entrantes.

Paquetes IP/Paquetes TCP/Paquetes UDP

Si hace clic en el enlace, puede determinar el protocolo que supervisa la regla de tráfico.

Opción Paquetes IP

Dirección IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP deseada.

Máscara IP

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IP deseada.

Opciones Paquetes TCP/Paquetes UDP

Dirección IP local

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP local deseada.

Máscara IP local

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IP local deseada.

Dirección IP remota

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IP remota deseada.

Máscara IP remota

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IP remota deseada.

Puerto local

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos locales o también rangos de puertos.

Puerto remoto

Si hace clic en el enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos remotos o también rangos de puertos completos.

No escribir en fichero de informe/escribir en fichero de informe

Si hace clic en el enlace, puede determinar si el programa adopta una entrada en el fichero de informe cuando coincida la regla.

Botones

Botón	Descripción
Añadir	Se crea una regla de aplicación nueva.
Suprimir	Se elimina la regla de aplicación seleccionada.
Subir	La regla de aplicación seleccionada se desplaza una posición hacia arriba, por lo que aumenta su prioridad.
Bajar	La regla de aplicación seleccionada se desplaza una posición hacia abajo, por lo que disminuye su prioridad.
Cambiar nombre	Edita la regla seleccionada, de modo que pueda introducirse un nuevo nombre de regla.
Aplicar	Los cambios realizados se aplican y Avira FireWall los usa directamente.
Aceptar	Los cambios realizados se aplican y Avira FireWall los usa directamente. Se cierra la ventana de configuración de las reglas de aplicación.
Cancelar	Se cierra la ventana de configuración de las reglas de aplicación sin aplicar los cambios realizados.

Proveedores de confianza

En *Proveedores de confianza* se muestra una lista de fabricantes de software de confianza.

Puede quitar o añadir fabricantes de la lista mediante la opción **Confiar siempre en este proveedor** en la ventana emergente **Evento de red**. Puede permitir de forma predeterminada el acceso a la red de las aplicaciones firmadas por los proveedores que se enumeran si activa la opción **Permitir automáticamente aplicaciones creadas por proveedores de confianza**.

Proveedores de confianza para usuario

En esta lista constan todos los usuarios del sistema. Si ha iniciado sesión como administrador, puede seleccionar un usuario cuya lista de proveedores de confianza desee ver o actualizar. Si no cuenta con privilegios, la lista solo muestra el usuario que ha iniciado sesión.

Permitir automáticamente aplicaciones creadas por proveedores de confianza

Si esta opción está activada, se permite automáticamente el acceso a la red a las aplicaciones con firma de proveedores conocidos y de confianza. Esta opción está activada de forma estándar.

Proveedor

La lista muestra todos los proveedores clasificados como de confianza.

Botones

Botón	Descripción
Quitar	La entrada seleccionada se quita de la lista de proveedores de confianza. Para quitar el proveedor seleccionado definitivamente de la lista, haga clic en "**Aplicar"** o "**Aceptar"** en la ventana de la configuración.
Volver a cargar	Se deshacen los cambios realizados: se carga la última lista guardada.

Nota
Si quita proveedores de la lista y, a continuación, pulsa el botón **Aplicar**, los proveedores se eliminan definitivamente de la lista. El cambio no se puede deshacer con **Volver a cargar**. Sin embargo, existe la posibilidad de volver a añadir un proveedor a la lista de proveedores de confianza mediante la opción **Confiar siempre en este proveedor** de la ventana emergente **Evento de red**.

Nota
FireWall da prioridad a las reglas de aplicación frente a las entradas de la lista de proveedores de confianza: si ha creado una regla de aplicación y el proveedor de la aplicación aparece en la lista de proveedores de confianza, la regla de aplicación se ejecuta.

Configuración

Configuración avanzada

Activar FireWall

Si esta opción está activada, Avira FireWall se encuentra activo y protege su equipo frente a los peligros procedentes de Internet y de otras redes.

Desactivar Firewall de Windows al iniciar

Si esta opción está activada, Firewall de Windows está desactivado al iniciar el equipo. Esta opción está activada de forma estándar.

Tiempo de espera excesivo de la regla

Bloquear siempre

Si esta opción está activada, se conserva la regla creada automáticamente, por ejemplo, durante un escaneo de puertos.

Quitar regla después de n segundos

Si esta opción está activada, una regla creada automáticamente, por ejemplo, durante un escaneo de puertos, se elimina tras el periodo indicado. Esta opción está activada de forma estándar. En este campo puede indicar los segundos después los cuales se elimina la regla.

Notificaciones

En *Notificaciones* se determina para qué eventos desea recibir una notificación en el escritorio de FireWall.

Escaneo de puertos

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall detecte un escaneo de puertos.

Desbordamiento

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall detecte un ataque por desbordamiento.

Aplicaciones bloqueadas

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall deniegue la actividad de red de una aplicación, es decir, la bloquee.

IP bloqueada

Si esta opción está activada, recibirá una notificación en el escritorio cuando el FireWall deniegue el tráfico de datos de una dirección IP.

Reglas de aplicación

Las opciones del área *Reglas de aplicación* permiten establecer las opciones de configuración para las reglas de aplicación en la sección FireWall > Reglas de aplicación.

Configuración avanzada

Si esta opción está activada, puede regular de forma personalizada los distintos accesos a la red de una aplicación.

Parámetros básicos

Si esta opción está activada, solo se puede configurar una única acción para los distintos accesos a la red de la aplicación.

Configuración de ventanas emergentes

Configuración de ventanas emergentes

Comprobar el bloque de inicio del proceso

Si esta opción está activada, tiene lugar un análisis más preciso de la pila de procesos. FireWall parte de la base de que cualquier proceso de la pila que no sea de confianza es el proceso a través de cuyo proceso secundario se accede a la red. Por ello, en este caso se abre una ventana emergente propia para cada proceso que no sea de confianza en la pila de procesos. Esta opción está desactivada de forma estándar.

Mostrar varios cuadros de diálogo por proceso

Si esta opción está activada, cada vez que una aplicación intenta establecer una conexión de red, se abre una ventana emergente. Otra opción es que la información solo aparezca en el primer intento de conexión. Esta opción está desactivada de forma estándar.

Guardar acción para esta aplicación

Siempre activado

Si esta opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está activada de forma predeterminada.

Siempre desactivado

Si esta opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está desactivada de forma predeterminada.

Permitir aplicaciones firmadas

Si esta opción está activada, cuando las aplicaciones firmadas de determinados fabricantes acceden a la red, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está activada automáticamente. Los denominados

"Proveedores de confianza" proporcionan las aplicaciones firmadas (consulte Proveedores de confianza).

Recordar último estado

Si esta opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" se usa del mismo modo que con el último evento de red. Si en el último evento de red se ha activado la opción "**Guardar acción para esta aplicación**", la opción estará activa en el siguiente evento de red. Si en el último evento de red se ha desactivado la opción "**Guardar acción para esta aplicación"**, la opción estará desactivada en el siguiente evento de red.

Mostrar detalles

En este grupo de opciones de configuración, puede configurar la presentación de información detallada en la ventana **Evento de red**.

Mostrar detalles a petición

Si esta opción está activada, la información detallada de la ventana "**Evento de red**" solo se muestra a petición, es decir, la presentación de la información detallada tiene lugar tras pulsar el botón "**Mostrar detalles**" en la ventana "**Evento de red**".

Mostrar siempre detalles

Si esta opción está activada, se muestra siempre la información detallada de la ventana "**Evento de red**".

Recordar último estado

Si la opción está activada, la presentación de información detallada se usa del mismo modo que en el evento de red anterior. Si en el último evento de red se ha mostrado o solicitado información detallada, en el siguiente evento de red se muestra dicha información. Si en el último evento de red no se ha mostrado o se ha ocultado la información detallada, en el siguiente evento de red no se muestra dicha información.

8.6.3 Avira FireWall bajo AMC

La configuración de FireWall está adaptada a las necesidades específicas de una administración a través de la Consola de administración de Avira. Existen opciones avanzadas y limitaciones de opciones de configuración individuales:

- La configuración de FireWall se aplica a todos los usuarios de las estaciones de trabajo.
- Reglas del adaptador: para adaptadores individuales se pueden configurar los niveles de seguridad mediante menús contextuales.
- Reglas de aplicación: es posible permitir o bloquear el acceso a red de aplicaciones. No existe la posibilidad de crear reglas de aplicación específicas.

Cuando su producto de Avira se administra a través de la Consola de administración de Avira, las siguientes opciones de configuración de FireWall en el Centro de control quedan desactivadas en las estaciones de trabajo:

- Configuración de los niveles de seguridad de FireWall
- Configuración de las reglas de adaptador y las reglas de aplicación

Opciones generales

Configuración avanzada

Activar FireWall

Si esta opción está activada, FireWall de Avira se encuentra activo y protege su equipo frente a los peligros procedentes de Internet y de otras redes.

Desactivar Firewall de Windows al iniciar

Si esta opción está activada, Firewall de Windows está desactivado al iniciar el equipo. Esta opción está activada de forma estándar.

Modo de aprendizaje

Si esta opción está activada, el modo de aprendizaje de FireWall de Avira está activo.

Tiempo de espera excesivo de la regla

Bloquear siempre

Si esta opción está activada, se conserva la regla creada automáticamente, por ejemplo, durante un escaneo de puertos.

Quitar regla después de n segundos

Si esta opción está activada, una regla creada automáticamente, por ejemplo, durante un escaneo de puertos, se elimina tras el periodo indicado. Esta opción está activada de forma estándar.

Regla general del adaptador

Las conexiones de red configuradas se conocen como adaptadores. Se pueden definir reglas del adaptador para las siguientes conexiones de red de cliente:

- Adaptador **predeterminado**: LAN o Internet de alta velocidad
- **Inalámbrico**
- Conexión por **marcación**

Puede ajustar reglas del adaptador predefinidas para cada adaptador disponible a través del menú contextual del adaptador (en **Regla general del adaptador**, haga clic con el botón derecho del ratón en **Puesto de trabajo** o **Predeterminado, Inalámbrico, Marcación**, etc):

- **Configurar nivel de seguridad en "Bajo"**
- **Configurar nivel de seguridad en "Medio"**
- **Configurar nivel de seguridad en "Alto"**

También existe la posibilidad de adaptar y personalizar reglas del adaptador individuales.

> **Nota**
> El ajuste predeterminado del Nivel de seguridad para todas las reglas predefinidas de FireWall de Avira es **Medio**.

- Protocolo ICMP
- Escaneado de puertos TCP
- Escaneado de puertos UDP
- Reglas entrantes
- Regla de protocolo IP
- Reglas salientes
- Botón

Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP) se emplea en redes para intercambiar mensajes de error e informativos. El protocolo se utiliza también para mensajes de estado mediante Ping o Tracert.
Con esta regla se pueden definir los tipos de ICMP entrantes y salientes que deben bloquearse, ajustar los parámetros para el desbordamiento y definir el comportamiento si existen paquetes ICMP fragmentados. Esta regla sirve para evitar los denominados ataques en desbordamiento ICPM que pueden causar una carga o sobrecarga del procesador del ordenador atacado, ya que se contesta a todos los paquetes.

Reglas predefinidas para el protocolo ICMP:

Configuración	Reglas
Bajo	Bloquea tipos entrantes: **sin tipo**. Bloquea tipos salientes: **sin tipo**. Asumir desbordamiento si el retraso entre paquetes es inferior a **50** milisegundos. **Rechazar** paquetes ICMP fragmentados.
Medio	La misma regla que para el ajuste Bajo.
Alto	Bloquea tipos entrantes: **varios tipos**. Bloquea tipos salientes: **varios tipos**. Asumir desbordamiento si el retraso entre paquetes es inferior a **50** milisegundos. **Rechazar** paquetes ICMP fragmentados.

Bloquea tipos entrantes: sin tipo/varios tipos.

Al hacer clic en el enlace, se abre una lista con los tipos de paquetes ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP entrantes que desee bloquear.

Bloquea tipos salientes: sin tipo/varios tipos.

Al hacer clic en el enlace, se abre una lista con los tipos de paquetes ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP salientes que desee bloquear.

Desbordamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede introducir el máximo retraso permitido de ICMPA.

Paquetes ICMP fragmentados

Al hacer clic en el enlace, tiene la posibilidad de aceptar o rechazar los paquetes ICMP fragmentados.

Escaneado de puertos TCP

Con esta regla se define cuándo FireWall debe suponer que existe un escaneado de puertos TCP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneado de puertos TCP, que pueden detectar puertos

abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles de un equipo a través de los cuales se lanzan ataques posiblemente mucho más dañinos.

Reglas predeterminadas para el escaneado de puertos TCP:

Configuración	Reglas
Bajo	Suponer que existe escaneado de puertos TCP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos TCP, **escribir en fichero de informe** la dirección IP del atacante y **no añadir** las reglas para bloquear el ataque.
Medio	Suponer que existe escaneado de puertos TCP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos TCP, **escribir en fichero de informe** la dirección IP del atacante y **añadir** las reglas para bloquear el ataque.
Alto	La misma regla que para el ajuste *Medio*.

Puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos TCP.

Ventana de tiempo de escaneado de puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos TCP.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se registra o no en el fichero de informe la dirección IP del atacante.

Regla

Al hacer clic en este enlace, tiene la opción de decidir si se añade o no la regla de bloqueo de ataques por escaneo de puertos TCP.

Escaneado de puertos UDP

Con esta regla se define cuándo FireWall debe suponer que existe un escaneado de puertos UDP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneado de puertos UDP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles de un equipo a través de los cuales se lanzan ataques posiblemente mucho más dañinos.

Reglas predeterminadas para el escaneado de puertos UDP:

Configuración	Reglas
Bajo	Suponer que existe escaneado de puertos UDP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos UDP, **escribir en fichero de informe** la dirección IP del atacante y **no añadir** las reglas para bloquear el ataque.
Medio	Suponer que existe escaneado de puertos UDP si se escanean **50** o más puertos en **5000** milisegundos. Si se detecta un análisis de puertos TCP, **escribir en fichero de informe** la dirección IP del atacante y **añadir** las reglas para bloquear el ataque.
Alto	La misma regla que para el ajuste *Medio*.

Puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos UDP.

Ventana de tiempo de escaneado de puertos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos UDP.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se registra o no en el fichero de informe la dirección IP del atacante.

Regla

Al hacer clic en este enlace, tiene la opción de decidir si se añade o no la regla de bloqueo de ataques por escaneo de puertos UDP.

Reglas entrantes

Las reglas entrantes sirven para controlar el tráfico entrante mediante FireWall de Avira.

Advertencia
Cuando se filtra un paquete, las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Reglas predeterminadas para el monitor de tráfico TCP:

Configuración	Reglas
Bajo	No se bloquea el tráfico entrante por parte de FireWall de Avira.

Medio	• Permitir conexión TCP establecida en puerto 135 **Permitir** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{135}** y el puerto remoto en **{0-65535}**. Aplicar para **paquetes en las conexiones existentes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. **Avanzado**: Descartar paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • Denegar paquetes TCP en puerto 135 **Denegar** los paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{135}** y el puerto remoto en **{0-65535}**. Aplicar para **todos los paquetes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • Monitorizar el tráfico de datos conforme a TCP **Permitir** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar al **inicio del establecimiento de la conexión y a paquetes de conexiones existentes.** **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • Denegar todos los paquetes TCP **Denegar** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar para **todos los paquetes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Alto	Monitorizar tráfico de datos TCP admitido **Permitir** paquetes TCP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar para **paquetes en las conexiones existentes**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Aceptar/denegar paquetes TCP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes TCP especialmente definidos.

IPv4/IPv6

Al hacer clic en el enlace, puede seleccionar entre IPv4 e IPv6.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Puertos locales

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos locales y también rangos de puertos completos.

Puertos remotos

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos remotos y también rangos de puertos completos.

Método de aplicación

Al hacer clic en este enlace, puede decidir si la regla se aplica a paquetes de conexiones existentes, en el inicio de las conexiones y a paquetes de conexiones existentes o a todas las conexiones.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se debe generar un fichero de informe cuando el paquete cumpla con la regla.

La opción **Ampliado** permite el filtrado basándose en el contenido. Por ejemplo, se pueden rechazar los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción, no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico.

Filtrado por contenido: máscara

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del contenido filtrado. El desplazamiento se calcula desde donde termina el encabezamiento TCP.

Reglas predeterminadas para el monitor de tráfico UDP:

Configuración	Reglas
Bajo	-
Medio	• Monitorizar el tráfico de datos conforme a UDP **Permitir** paquetes UDP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar a **puertos abiertos** para **todos los flujos de datos**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**. • Denegar todos los paquetes UDP **Denegar** paquetes UDP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{0-65535}**. Aplicar en **todos los puertos** para **todos los flujos de datos**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.
Alto	Monitorizar tráfico de datos UDP admitido **Permitir** paquetes UDP de la dirección **0.0.0.0** con la máscara **0.0.0.0** si el puerto local se encuentra en **{0-65535}** y el puerto remoto en **{53, 67, 68, 123}**. Aplicar a **puertos abiertos** para **todos los flujos de datos**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.

Aceptar/denegar paquetes UDP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes UDP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Puertos locales

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos locales y también rangos de puertos completos.

Puertos remotos

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar uno o varios puertos remotos y también rangos de puertos completos.

Método de aplicación

Al hacer clic en este enlace, puede elegir la aplicación de esta regla a todos los puertos o solo a los abiertos.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se debe generar un fichero de informe cuando el paquete cumpla con la regla.

La opción **Ampliado** permite el filtrado basándose en el contenido. Por ejemplo, se pueden rechazar los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción, no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico.

Filtrado por contenido: máscara

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del contenido filtrado. El desplazamiento se calcula desde donde termina el encabezamiento UDP.

Reglas predeterminadas para el monitor de tráfico ICMP:

Configuración	Reglas
Bajo	-
Medio	No descartar paquetes ICMP sobre la base de la dirección IP **Permitir** paquetes ICMP de la dirección **0.0.0.0** con la máscara **0.0.0.0**. **No escribir en fichero de informe** cuando el paquete cumpla la regla. Avanzado: Seleccionar los paquetes que tengan los siguientes bytes **<vacío>** con la máscara **<vacío>** con desplazamiento **0**.
Alto	La misma regla que para el ajuste *Medio*.

Aceptar/denegar paquetes ICMP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes ICMP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se debe generar un fichero de informe cuando el paquete cumpla con la regla.

La opción **Ampliado** permite el filtrado basándose en el contenido. Por ejemplo, se pueden rechazar los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción, no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico.

Filtrado por contenido: máscara

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Al hacer clic en el enlace, se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del contenido filtrado. El desplazamiento se calcula desde donde termina el encabezamiento ICMP.

Reglas predeterminadas para los paquetes IP:

Configuración	Reglas
Bajo	-
Medio	-
Alto	Denegar todos los paquetes IP **Denegar** paquetes **IPv4** de la dirección **0.0.0.0** con la máscara **0.0.0.0** **No escribir en fichero de informe** cuando el paquete cumpla la regla.

Aceptar/denegar paquetes IP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes IP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se debe generar un fichero de informe cuando el paquete cumpla con la regla.

Reglas posibles para la monitorización de paquetes IP basándose en protocolos IP:

Paquetes IP

Al hacer clic en este enlace, tiene la opción de decidir si desea permitir o denegar paquetes IP especialmente definidos.

Dirección IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la dirección IPv4 o IPv6 deseada.

Máscara IP

Si hace clic en este enlace, se abre un cuadro de diálogo en el que puede indicar la máscara IPv4 o IPv6 deseada.

Protocolo

Al hacer clic en este enlace, se abre un cuadro de diálogo en el que puede seelccionar el protocolo IP requerido.

Fichero de informe

Al hacer clic en este enlace, puede decidir si se debe generar un fichero de informe cuando el paquete cumpla con la regla.

Reglas salientes

Las reglas salientes sirven para controlar el tráfico saliente mediante FireWall de Avira. Puede definir una regla saliente para los siguientes protocolos: IP, ICMP, UDP y TCP. Consulte Añadir nueva regla.

Advertencia
Cuando se filtra un paquete, las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Botones

Botón	Descripción
Añadir	Permite crear una nueva regla. Al hace clic en este botón, aparece el cuadro de diálogo "Añadir nueva regla". En este cuadro de diálogo puede seleccionar nuevas reglas.
Suprimir	Elimina la regla seleccionada.

Subir	La regla seleccionada se desplaza una posición hacia arriba, por lo que aumenta su prioridad.
Bajar	La regla seleccionada se desplaza una posición hacia abajo, por lo que disminuye su prioridad.
Cambiar el nombre	Permite cambiar el nombre de la regla seleccionada.

Nota
Puede añadir nuevas reglas para cada adaptador o para todos los adaptadores del equipo. Para añadir una regla del adaptador para todos los adaptadores, seleccione **Puesto de trabajo** en la estructura del adaptador que se muestra y haga clic en el botón **Añadir**. Consulte Añadir nueva regla.

Nota
Para cambiar la posición de una regla, también puede arrastrarla con el ratón a la posición pertinente.

Lista de aplicaciones

En Lista de aplicaciones puede crear reglas para los accesos a red de aplicaciones. Puede añadir aplicaciones a la lista y establecer mediante un menú contextual las reglas **Permitir** y **Rechazar** para la aplicación seleccionada:

- Se permiten los accesos a red de aplicaciones con la regla **Permitir**.
- Se rechazan los accesos a red de aplicaciones con la regla **Rechazar**.

Al añadir aplicaciones, se establece la regla **Permitir**.

Lista de aplicaciones

Esta tabla muestra la lista de aplicaciones para las que se han definido reglas. Los símbolos indican si los accesos a red de las aplicaciones están permitidos o bloqueados. Puede modificar las reglas de las aplicaciones mediante un menú contextual.

Botones

Botón	Descripción
Agregar mediante ruta	El botón abre un cuadro de diálogo en el que puede seleccionar aplicaciones. La aplicación se añade a la lista de aplicaciones con la regla "**Permitir**". Si utiliza la opción "**Agregar mediante ruta"**, la aplicación agregada se identifica mediante FireWall a través de la ruta y el nombre de archivo.
Agregar mediante md5	El botón abre un cuadro de diálogo en el que puede seleccionar aplicaciones. La aplicación se añade a la lista de aplicaciones con la regla "**Permitir**". Si utiliza la opción "**Agregar mediante md5"**, todas las aplicaciones agregadas se identifican inequívocamente mediante la suma de comprobación MD5. Esto permite que FireWall detecte cambios en los contenidos del fichero. Si se modifica una aplicación, por ejemplo debido a una actualización, la aplicación con la regla establecida se borra automáticamente de la lista de aplicaciones. La aplicación debe añadirse nuevamente a la lista después de la modificación y la regla deseada debe establecerse de nuevo.
Añadir grupo	El botón abre un cuadro de diálogo en el que puede seleccionar un directorio. Todas las aplicaciones en la ruta seleccionada se añaden a la lista de aplicaciones con la regla "**Permitir**".
Suprimir	Se elimina la regla de aplicación seleccionada.
Eliminar todos	Se eliminan todas las reglas de aplicación.

Proveedores de confianza

En **Proveedores de confianza** se muestra una lista de fabricantes de software de confianza. Se permiten los accesos de red de aplicaciones de los productores de software contenidos en la lista. Puede quitar o añadir productores a la lista.

Proveedor

La lista muestra todos los proveedores clasificados como de confianza.

Botones

Botón	Descripción
Añadir	El botón abre un cuadro de diálogo en el que puede seleccionar aplicaciones. Se determina el fabricante de la aplicación y se añade a la lista de proveedores de confianza.
Añadir grupo	El botón abre un cuadro de diálogo en el que puede seleccionar un directorio. Se determinan los fabricantes de todas las aplicaciones en la ruta seleccionada y se añaden a la lista de proveedores de confianza.
Quitar	La entrada seleccionada se quita de la lista de proveedores de confianza. Para quitar el proveedor seleccionado definitivamente de la lista, haga clic en "**Aplicar**" o "**Aceptar**" en la ventana de la configuración.
Eliminar todas	Se eliminan todas las entradas de la lista de proveedores de confianza.
Volver a cargar	Se deshacen los cambios realizados: se carga la última lista guardada.

Nota
Si quita proveedores de la lista y, a continuación, pulsa el botón **Aplicar**, los proveedores se eliminan definitivamente de la lista. El cambio no se puede deshacer con **Volver a cargar**.

Nota
FireWall da prioridad a las reglas de aplicación frente a las entradas de la lista de proveedores de confianza: si ha creado una regla de aplicación y el proveedor de la aplicación aparece en la lista de proveedores de confianza, la regla de aplicación se ejecuta.

Configuración adicional

Opciones disponibles solo si el modo experto está activado.

Notificaciones

En Notificaciones se determina para qué eventos desea recibir una notificación en el escritorio de FireWall.

Escaneo de puertos

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall detecte un escaneo de puertos.

Desbordamiento

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall detecte un ataque por desbordamiento.

Aplicaciones bloqueadas

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall deniegue la actividad de red de una aplicación, es decir, la bloquee.

IP bloqueada

Si esta opción está activada, recibe una notificación en el escritorio cuando FireWall deniegue el tráfico de datos de una dirección IP.

Configuración de ventanas emergentes

Comprobar el bloque de inicio del proceso

Si esta opción está activada, tiene lugar un análisis más preciso de la pila de procesos. FireWall parte de la base de que cualquier proceso de la pila que no sea de confianza es el proceso a través de cuyo proceso secundario se accede a la red. Por ello, en este caso se abre una ventana emergente propia para cada proceso que no sea de confianza en la pila de procesos. Esta opción está desactivada de forma estándar.

Mostrar varios cuadros de diálogo por proceso

Si esta opción está activada, cada vez que una aplicación intenta establecer una conexión de red, se abre una ventana emergente. Otra opción es que la información solo aparezca en el primer intento de conexión. Esta opción está desactivada de forma estándar.

Configuración de visualización

Guardar acción para esta aplicación

Siempre activado

Si esta opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está activada de forma predeterminada. Esta opción está activada de forma estándar.

Siempre desactivado

Si esta opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está desactivada de forma predeterminada.

Permitir aplicaciones firmadas

Si esta opción está activada, cuando las aplicaciones firmadas de determinados fabricantes acceden a la red, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está activada automáticamente. Los fabricantes son: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun,Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Recordar último estado

Si esta opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" se usa del mismo modo que con el último evento de red. Si en el último evento de red se ha activado la opción "**Guardar acción para esta aplicación**", la opción estará activa en el siguiente evento de red. Si en el último evento de red se ha desactivado la opción "**Guardar acción para esta aplicación"**, la opción estará desactivada en el siguiente evento de red.

Mostrar detalles

En este grupo de opciones de configuración, puede configurar la presentación de información detallada en la ventana **Evento de red**.

Mostrar detalles a petición

Si esta opción está activada, la información detallada de la ventana "**Evento de red**" solo se muestra a petición, es decir, la presentación de la información detallada tiene lugar tras pulsar el botón "**Mostrar detalles**" en la ventana "**Evento de red**".

Mostrar siempre detalles

Si esta opción está activada, se muestra siempre la información detallada de la ventana "**Evento de red**".

Recordar último estado

Si esta opción está activada, la presentación de información detallada se usa del mismo modo que en el evento de red anterior. Si en el último evento de red se ha mostrado o solicitado información detallada, en el siguiente evento de red se muestra dicha información. Si en el último evento de red no se ha mostrado o se ha ocultado la información detallada, en el siguiente evento de red no se muestra dicha información.

8.6.4 Firewall de Windows

La sección **FireWall** en **Configuración > Seguridad en Internet** sirve para configurar el FireWall de Windows en los sistemas operativos a partir de Windows 7.

FireWall de Windows

Activar el FireWall de Windows administrado por Avira

Con la opción activada, el FireWall de Windows se controla mediante Avira.

Perfiles de red

Perfiles de red

Sobre la base de los perfiles de red, el FireWall de Windows bloquea el acceso de programas y aplicaciones no autorizados en su ordenador:

- Red privada: para redes domésticas o de oficina
- Red pública: para redes públicas
- Red de dominio: para redes con un controlador de dominio

Puede administrar estos perfiles desde la configuración de su producto Avira en **Seguridad en Internet > FireWall de Windows > Perfiles de red**.

Para más información sobre estos perfiles de red, visite la página web oficial de Microsoft.

Advertencia
El FireWall de Windows aplica las mismas normas para todas las redes que pertenecen al mismo perfil. Esto significa que si permite un programa o una aplicación, estos también tendrán acceso a todas las redes que utilizan el mismo perfil.

Red privada

Configuración para la red privada

La configuración para la red privada administra el acceso que otros ordenadores o equipos tienen a su ordenador en su red doméstica o de oficina. Esta configuración permite de serie que los usuarios de la red privada vean su ordenador y puedan acceder al mismo.

Activar

Con la opción activada, se conecta el FireWall de Windows y se controla mediante Avira.

Bloquear todas las conexiones entrantes

Con la opción activada, el FireWall de Windows rechazará todos los intentos no deseados de conectarse a su ordenador, incluidas las conexiones entrantes de aplicaciones admitidas.

Notificarme cuando se bloquee una nueva aplicación

Con la opción activada, cada vez que un programa o una aplicación se bloquee recibirá la correspondiente notificación.

Desactivar (no recomendado)

Con la opción activada, se desconectará el FireWall de Windows. Esta opción no se recomienda porque pone en riesgo a su ordenador.

Red pública

Configuración para la red pública

La configuración para la red pública administra el acceso que otros ordenadores o equipos tienen a su ordenador en redes públicas. Esta configuración no permite de serie que los usuarios de la red pública vean su ordenador y puedan acceder al mismo.

Activar

Con la opción activada, se conecta el FireWall de Windows y se controla mediante Avira.

Bloquear todas las conexiones entrantes

Con la opción activada, el FireWall de Windows rechazará todos los intentos no deseados de conectarse a su ordenador, incluidas las conexiones entrantes de aplicaciones admitidas.

Notificarme cuando se bloquee una nueva aplicación

Con la opción activada, cada vez que un programa o una aplicación se bloquee recibirá la correspondiente notificación.

Desactivar (no recomendado)

Con la opción activada, se desconectará el FireWall de Windows. Esta opción no se recomienda porque pone en riesgo a su ordenador.

Red de dominio

Configuración para la red de dominio

La configuración para la red de dominio administra el acceso que otros ordenadores o equipos tienen a su ordenador, si su ordenador está conectado a una red autentificada mediante un controlador de dominio. Esta configuración permite de serie que los usuarios autentificados de los dominios vean su ordenador y puedan acceder al mismo.

Activar

Con la opción activada, se conecta el FireWall de Windows y se controla mediante Avira.

Bloquear todas las conexiones entrantes

Con la opción activada, el FireWall de Windows rechazará todos los intentos no deseados de conectarse a su ordenador, incluidas las conexiones entrantes de aplicaciones admitidas.

Notificarme cuando se bloquee una nueva aplicación

Con la opción activada, cada vez que un programa o una aplicación se bloquee recibirá la correspondiente notificación.

Desactivar (no recomendado)

Con la opción activada, se desconectará el FireWall de Windows. Esta opción no se recomienda porque pone en riesgo a su ordenador.

> **Nota**
> Esta opción solo está disponible si su ordenador está conectado a una red que dispone de un controlador de dominio.

Reglas de aplicación

Si hace clic en el enlace bajo **FireWall de Windows > Reglas de aplicación**, se le redirigirá al menú **Aplicaciones y características permitidas** de la configuración del FireWall de Windows.

Configuración avanzada

Si hace clic en el enlace bajo **FireWall de Windows > Configuración avanzada**, se le redirigirá al menú **FireWall de Windows con seguridad avanzada** de la configuración del FireWall de Windows.

8.7 Web Protection

La sección **Web Protection** en **Configuración > Seguridad en Internet** sirve para configurar Web Protection.

8.7.1 Análisis

Con Web Protection se protege de virus y malware que llegan a su equipo a través de páginas web que carga en su explorador web desde Internet. En la sección **Análisis** puede ajustar el comportamiento de Web Protection.

Análisis

Activar Web Protection

Si esta opción está activada, la función Web Protection no está activa.

Compatibilidad de IPv6

Si esta opción está activada, Web Protection es compatible con la versión 6 del protocolo de Internet. Esta opción no está disponible para instalaciones nuevas o cambios en la instalación de Windows 8.

Protección sobre la marcha

Gracias a *Protección sobre la marcha* tiene la posibilidad de realizar ajustes para bloquear los I-Frames, también denominados Inlineframes. Los I-Frames son elementos HTML, es decir, elementos de las páginas de Internet que limitan una área de una página web. Con los I-Frames se puede cargar y mostrar otro contenido web -sobre todo, otras URL- como documentos independientes en una subventana del navegador. Los I-Frames se utilizan en especial para la publicidad en forma de banners. En algunos casos, los I-Frames se emplean para ocultar malware. En estos casos, el área del I-Frame en el navegador apenas es visible o está oculta. Con la opción **Bloquear I-Frames sospechosos** tiene la posibilidad de controlar y bloquear la carga de I-Frames.

Bloquear I-Frames sospechosos

Si esta opción está activada, se comprueban en función de determinados criterios los I-Frames de las páginas web solicitadas. Si hay I-Frames sospechosos en una página web solicitada, se bloquea el I-Frame. En la ventana del I-Frame se muestra un mensaje de error.

Acción al detectar

Puede definir acciones que Web Protection debe ejecutar si se detecta un virus o un programa no deseado.

Interactivo

Si esta opción está activada, durante el análisis directo y si se detecta un virus o un programa no deseado, aparece un cuadro de diálogo en el que puede seleccionar cómo proceder con el fichero afectado. Este ajuste está activado de forma estándar.

Mostrar barra de progreso

Si esta opción está activada, aparece un mensaje en el escritorio con una barra de progreso de la descarga si la descarga del contenido de las páginas web supera un tiempo de espera de 20 segundos. Este mensaje en el escritorio sirve especialmente como función de control de las descargas de páginas web con un volumen elevado de datos: al navegar con Web Protection, el contenido de las páginas web no se carga de forma consecutiva en el navegador de Internet, dado que se buscan virus y malware antes de mostrarlo en el navegador de Internet. Esta opción está desactivada de forma estándar.

Acciones permitidas

En esta área puede seleccionar las acciones que se muestran en el cuadro de diálogo cuando se detecta un virus o un programa no deseado. Para ello, tiene que activar las opciones correspondientes.

Denegar acceso

El sitio web requerido por el servidor web y los datos solicitados no son transferidos a su navegador. Un error de acceso denegado ha sido mostrado en su navegador web. Web Protection registra la detección en el fichero de informe si está activada la función de informes.

Mover a cuarentena

La página web solicitada por el servidor Web o los datos y los ficheros transmitidos no se envían a la cuarentena si se detectan virus o malware. El gestor de cuarentena puede recuperar el fichero afectado si tiene valor informativo o, en caso necesario, enviarlo al Avira Malware Research Center.

Omitir

La página web solicitada por el servidor web o los datos y ficheros transmitidos se pasan por Web Protection a su navegador.

Predeterminado

Con ayuda de este botón, puede seleccionar la acción que debe estar activada por defecto en el cuadro de diálogo cuando se detecta un virus. Marque la acción debe estar activada por defecto y haga clic en el botón "Predeterminado".

Puede encontrar más información aquí.

Automático

Si esta opción está activada, cuando se detecta un virus o un programa no deseado, no aparece ningún cuadro de diálogo en el que se pueda seleccionar una acción. Web Protection reacciona en función de la configuración que ha realizado en esta sección.

Mostrar mensajes de advertencia

Si esta opción está activada, cuando se detecta un virus o un programa no deseado, aparece un mensaje de advertencia con las acciones que se van a ejecutar.

Acción principal

La acción primaria es aquella que se ejecuta cuando Web Protection detecta un virus o un programa no deseado.

Denegar acceso

El sitio web requerido por el servidor web y los datos solicitados no son transferidos a su navegador. Un error de acceso denegado ha sido mostrado en su navegador web. Web Protection registra la detección en el fichero de informe si está activada la función de informes.

Mover a cuarentena

La página web solicitada por el servidor Web o los datos y los ficheros transmitidos no se envían a la cuarentena si se detectan virus o malware. El gestor de cuarentena puede recuperar el fichero afectado si tiene valor informativo o, en caso necesario, enviarlo al Avira Malware Research Center.

Omitir

La página web solicitada por el servidor web o los datos y ficheros transmitidos se pasan por Web Protection a su navegador. Está permitido acceder al archivo y salir de él.

Advertencia
El archivo afectado permanece activo en su ordenador. Puede causar daños graves en su ordenador.

Accesos bloqueados

En **Accesos bloqueados**, puede indicar los tipos de fichero y MIME (tipos de contenido de los datos transmitidos) que Web Protection debe bloquear. Con el filtro Web es posible bloquear URL no deseadas conocidas, como p. ej., URL con suplantación de identidad y malware. Web Protection impide la transmisión de datos desde Internet a su ordenador.

Tipos de fichero y tipos MIME bloqueados por Web Protection

Web Protection bloquea todos los tipos de fichero y MIME (tipos de contenido de los datos transmitidos) de la lista.

Campo de entrada

En este campo puede introducir los nombres de los tipos de fichero y MIME que Web Protection debe bloquear. Para los tipos de fichero, introduzca la extensión del archivo, p. ej., **.htm**. Para los tipos MIME, indique el tipo de medio y, en caso necesario, el subtipo. Ambos datos se separan mediante una barra, p. ej., **vídeo/mpeg** o **audio/x-wav**.

Nota
Los ficheros ya guardados en su sistema informático como ficheros temporales de Internet quedan bloqueados por Web Protection, pero el explorador de Internet local puede descargarlos de su equipo. Los ficheros temporales de Internet son ficheros que guarda el explorador de Internet en el equipo para poder mostrar las páginas web con mayor rapidez.

Nota
La lista de los tipos de fichero y MIME que deben bloquearse se omite en las entradas en la lista de los tipos de fichero y MIME omitidos en Excepciones.

Nota
Al indicar los tipos de fichero y MIME, no puede utilizar comodines (comodín * para varios caracteres o ? para un solo carácter).

Tipos MIME: ejemplos de tipos de medios

- `texto` = para ficheros de texto.
- `imagen` = para ficheros de gráficos.
- `vídeo` = para ficheros de vídeo.
- `audio` = para ficheros de sonido.
- `aplicación` = para ficheros que están asociados a un programa determinado.

Ejemplos: tipo de fichero y MIME omitidos

- `aplicación/octet-stream` = Web Protection bloquea los ficheros del tipo MIME aplicación/octet-stream (archivos ejecutables *.bin, *.exe, *.com, *dll, *.class).
- `aplicación/olescript` = Web Protection bloquea los ficheros del tipo MIME aplicación/olescript (ficheros de script ActiveX *.axs).
- `.exe` = Web Protection bloquea todos los ficheros con la extensión .exe (archivos ejecutables).
- `.msi` = Web Protection bloquea todos los ficheros con la extensión .msi (archivos de Windows Installer).

Añadir

Con este botón puede adoptar el tipo MIME o de fichero introducido en el campo de entrada en la ventana.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Filtro Web

El filtro web cuenta con una base de datos interna que se actualiza diariamente en la que se clasifican las URL de acuerdo con criterios del contenido.

Activar filtro web

Si esta opción está activada, se bloquean todas las URL que pertenecen a las categorías seleccionadas en la lista Filtro Web.

Lista del filtro Web

En la lista del filtro Web puede seleccionar las categorías de contenido cuyas URL debe bloquear Web Protection.

Nota
La lista del filtro Web se omite en las entradas en la lista de las URL omitidas en Excepciones.

Nota
En **URLs de spam** se clasifican las URL que se distribuyen con los correos electrónicos no solicitados. La categoría **Estafa / Engaño** incluye páginas web con 'casos de suscripciones' y otras ofertas de servicios cuyos costes oculta el proveedor.

Excepciones

Con estas opciones puede excluir del análisis de Web Protection los tipos MIME (tipos de contenido de los datos transmitidos) y los tipos de fichero para las URL (direcciones de Internet). Web Protection omite los tipos MIME y las URL indicados, es decir, no se analiza la presencia de virus y malware en estos datos cuando se transmiten a su ordenador.

Tipos MIME omitidos de Web Protection

En este campo puede seleccionar los tipos MIME (tipos de contenido de los datos transmitidos) que deben excluirse del análisis de Web Protection.

Tipos de fichero / MIME omitidos de Web Protection (personalizado)

Se excluyen del análisis de Web Protection todos los tipos de fichero y MIME (tipos de contenido de los datos transmitidos) de la lista.

Campo de entrada

En este campo puede introducir los nombres de los tipos de fichero y MIME que deben excluirse del análisis de Web Protection. Para los tipos de fichero, introduzca la extensión del archivo, p. ej., `.htm`. Para los tipos MIME, indique el tipo de medio y, en caso necesario, el subtipo. Ambos datos se separan mediante una barra, p. ej., `vídeo/mpeg` o `audio/x-wav`.

Nota
Al indicar los tipos de fichero y MIME, no puede utilizar comodines (comodín * para varios caracteres o ? para un solo carácter).

Advertencia
Se cargan en el navegador de Internet todos los tipos de fichero y contenido de la lista de exclusiones sin comprobar los accesos bloqueados (lista de los tipos de fichero y MIME que deben bloquearse en Accesos bloqueados) o Web Protection: se omiten las entradas de la lista de los tipos de fichero y MIME que deben bloquearse en todas las entradas de la lista de exclusiones. No se analiza la presencia de virus y malware.

Tipos MIME: ejemplos de tipos de medios

- `texto` = para ficheros de texto.
- `imagen` = para ficheros de gráficos.
- `vídeo` = para ficheros de vídeo.
- `audio` = para ficheros de sonido.
- `aplicación` = para ficheros que están asociados a un programa determinado.

Ejemplos: tipo de fichero y MIME omitidos

- `audio/` = se excluyen del análisis de Web Protection todos los archivos de los tipos de medios de audio.
- `vídeo/quicktime` = se excluyen del análisis de Web Protection todos los archivos de vídeo del subtipo Quicktime (*.qt, *.mov).
- `.pdf` = se excluyen del análisis de Web Protection todos los archivos Adobe-PDF.

Añadir

Con este botón puede adoptar el tipo MIME o de fichero introducido en el campo de entrada en la ventana.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

URL omitidas de Web Protection

Se excluyen del análisis de Web Protection todas las URL de esta lista.

Campo de entrada

En este campo puede introducir las URL (direcciones de Internet) que deben excluirse del análisis de Web Protection, p. ej., **www.nombrededominio.com**. Puede introducir de forma parcial la URL, para ello debe identificar el nivel del dominio con puntos de inicio o final: .nombrededominio.de para todas las páginas y los subdominios del dominio. Escriba una página web con el dominio de nivel superior preferido (.com o .net) con un punto final: **nombrededominio.**. Si escribe una secuencia de caracteres sin el punto de inicio o final, dicha secuencia se interpreta como un dominio de nivel superior, p. ej., **net** para todos los dominios NET (www.dominio.net).

Nota
Cuando indique las direcciones URL, también puede usar el carácter comodín * para tantos caracteres como desee. Utilice también los puntos de inicio o final, junto con los comodines, para identificar los niveles del dominio:
`.nombrededominio.*`
`*.nombrededominio.com`
`.*nombre*.com` (es válido, pero no se recomienda).
Las entradas sin puntos como `*nombre*` se interpretan como partes de un dominio de nivel superior y no tienen ninguna utilidad.

Advertencia
En el navegador de Internet se cargan todas las páginas web de la lista de las URL omitidas sin comprobar el filtro Web o Web Protection: se omiten las entradas del filtro Web en todas las entradas de la lista de las URL omitidas (véase Accesos bloqueados). No se analiza la presencia de virus y malware. Por tanto, excluya del análisis de Web Protection únicamente las URL de confianza.

Añadir

Este botón permite incluir en la ventana de visualización la URL (dirección de Internet) introducida en el campo de introducción.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Ejemplos: URL omitidas

- `www.avira.com` -O- `www.avira.com/*`
  = se excluyen del análisis de Web Protection todas las URL con el dominio 'www.avira.com': www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,..
  Se excluyen del análisis de Web Protection todas las URL con el dominio www.avira.de.
- `avira.com` -O- `*.avira.com`
  = se excluyen del análisis de Web Protection todas las URL con el dominio de nivel secundario o principal 'avira.com'. La entrada se refiere a todos los subdominios existentes de '.avira.com': www.avira.com, forum.avira.com,...
- `avira.` -O- `*.avira.*`
  = se excluyen del análisis de Web Protection todas las URL con el dominio de nivel secundario 'avira'. La entrada se refiere a todos los dominios de nivel principal o los subdominios existentes de '.avira.': www.avira.com, www.avira.de, forum.avira.com,...

- `.*dominio*.*`
  = se excluyen del análisis de Web Protection todas las URL que contienen un dominio de nivel secundario con la cadena de caracteres 'dominio': www.dominio.com, www.dominio-nuevo.de, www.ejemplo-dominio1.de, ...
- `net` -O- `*.net.*`
  = se excluyen del análisis de Web Protection todas las URL con el dominio de nivel principal 'net': www.nombre1.net, www.nombre2.net,...

Advertencia
Sea lo más preciso posible cuando indique las URL que quiere excluir del análisis de Web Protection. Evite introducir los dominios de nivel principal completos o partes del nombre de un nombre de dominio de nivel secundario, dado que existe el peligro de que se excluyan del análisis de Web Protection páginas de Internet, que difunden malware y programas no deseados debido a entradas globales en las excepciones. Se recomienda que introduzca al menos el dominio de nivel secundario y el dominio de nivel superior completos: nombrededominio.com.

Heurística

Esta sección de configuración trata sobre la configuración de la heurística del motor de análisis.

Los productos de Avira integran heurísticas muy potentes con las que se puede detectar de forma proactiva el malware desconocido, es decir, antes de que se cree una firma de virus especial contra el parásito y se envíe una actualización de la protección frente a los virus. Los virus se detectan gracias a un análisis y un examen exhaustivos del código afectado de acuerdo con las funciones habituales del malware. Si el código analizado cumple estas características, se considera sospechoso. Sin embargo, esto no significa necesariamente que el código sea malware; también se pueden producir falsas alarmas. El usuario es responsable de decidir qué debe hacerse con el código afectado, p. ej., basándose en sus conocimientos de si la fuente que contiene el código afectado es de confianza.

Heurística de macrovirus

Su producto de Avira integra una heurística de macrovirus muy potente. Si esta opción está activada, durante una posible reparación se borran todas las macros del documento afectado o bien se muestra una notificación acerca de los documentos sospechosos, es decir, se muestra una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Advanced Heuristic Analysis and Detection (AHeAD)

Activar AHeAD

Su producto de Avira incorpora en la tecnología AHeAD de Avira una heurística muy potente que puede detectar también el malware desconocido (nuevo). Si esta opción

está activada, aquí puede ajustar hasta qué punto es "precisa" esta heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si esta opción está activada, se detecta en menor medida el malware desconocido, pero se reduce el riesgo de posibles falsos positivos.

Nivel de detección medio

Si esta opción está activada, se garantiza una protección equilibrada con pocos falsos positivos. Este ajuste está activado de forma estándar si ha seleccionado que se aplique esta heurística.

Nivel de detección alto

Si esta opción está activada, el malware desconocido se detecta en mayor medida, pero se debe contar con falsos positivos.

8.7.2 Informe

Web Protection cuenta con una completa función de registro que puede proporcionar al usuario o al administrador información exacta acerca del tipo y la forma de una detección.

Protocolización

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Si esta opción está activada, Web Protection no crea ningún informe.
Renuncie a realizar el registro solo en casos excepcionales, por ejemplo, solo si realiza pruebas con muchos virus o programas no deseados.

Predeterminado

Si esta opción está activada, Web Protection registra información importante (detecciones, advertencias y errores) en el fichero de informe, obviando información importante para ganar en claridad. Este ajuste está activado de forma estándar.

Extendido

Si esta opción está activada, Web Protection registra también información secundaria en el fichero de informe.

Completo

Si esta opción está activada, Web Protection registra toda la información (también el tamaño y el tipo del archivo, la fecha, etc.) en el fichero de informe.

Limitar fichero de informe

Limitar tamaño a n MB

Si esta opción está activada, el fichero de informe se limita a un tamaño determinado; valores posibles: 1 a 100 MB. Cuando se limita el fichero de informe, se reserva un espacio aproximado de 50 kilobytes, con el fin de limitar la carga del equipo. Si el archivo de registro supera el tamaño indicado en 50 kilobytes, se borran automáticamente las entradas grandes antiguas hasta que el tamaño indicado se ha reducido en menos del 20 %.

Escribir configuración en fichero de informe

Si esta opción está activada, la configuración empleada del análisis en tiempo real se registra en el fichero de informe.

Nota
Si no se indica ninguna limitación para el fichero de informe, se eliminan automáticamente las entradas más antiguas si el fichero de informe ha alcanzado un tamaño de 100 MB. Se borran las entradas necesarias hasta que el fichero de informe ha alcanzado un tamaño de 80 MB.

8.8 Mail Protection

La sección Mail Protection de la configuración sirve para configurar Mail Protection.

8.8.1 Análisis

Mail Protection se usa para analizar los correos electrónicos entrantes en cuanto a la presencia de virus, malware y . Mail Protection también puede analizar los correos electrónicos salientes en cuanto a la presencia de virus y malware. Los correos electrónicos salientes enviados por un robot de software desconocido para propagar correo no solicitado desde su equipo pueden bloquearse con Mail Protection.

Activar Mail Protection

Si esta opción está activada, Mail Protection supervisa el tráfico de correo electrónico. Mail Protection es un servidor proxy que comprueba el tráfico de datos entre el servidor de correo que utiliza y el programa de cliente de correo de su equipo: en la configuración predeterminada se analiza la existencia de malware en los correos electrónicos entrantes. Si la opción está desactivada, se inicia el servicio Mail Protection, pero se desactiva la monitorización por parte de Mail Protection.

Analizar emails entrantes

Si esta opción está activada, los correos electrónicos entrantes se analizan en cuanto a la presencia de virus y malware. Mail Protection es compatible con los protocolos POP3 e IMAP. Active la cuenta de entrada de correo que usa su cliente de correo para recibir correos electrónicos, con el fin de que Mail Protection la supervise.

Supervisar cuentas POP3

Si esta opción está activada, se supervisan las cuentas POP3 en los puertos indicados.

Puertos supervisados

En este campo se indica el puerto que usa el protocolo POP3 como entrada de correo. Indique varios puertos separándolos con comas.

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de POP3.

Supervisar cuentas IMAP

Si esta opción está activada, se supervisan las cuentas IMAP en los puertos indicados.

Puertos supervisados

En este campo se indica el puerto que usa el protocolo IMAP. Indique varios puertos separándolos con comas.

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de IMAP.

Analizar emails salientes (SMTP)

Si esta opción está activada, los correos electrónicos salientes se analizan en cuanto a la presencia de virus y malware. Los correos electrónicos enviados por robots de software desconocidos para propagar correo no solicitado se bloquean.

Puertos supervisados

En este campo se indica el puerto que usa el protocolo STMP como salida de correo. Indique varios puertos separándolos con comas.

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de SMTP.

Nota
Para verificar los protocolos y puertos usados, abra las propiedades de sus cuentas de correo electrónico en el programa del cliente de correo. Normalmente se usan puertos estándar.

Compatibilidad de IPv6

Si esta opción está activada, Mail Protection es compatible con la versión 6 del protocolo de Internet. (Opción no disponible para instalaciones nuevas o cambios en la instalación de Windows 8).

Acción al detectar

Esta sección de configuración contiene la configuración que indica la acción que se ejecutará cuando Mail Protection detecte un virus o programa no deseado en un correo electrónico o en los datos adjuntos.

> **Nota**
> Las acciones establecidas aquí se llevan a cabo tanto en el caso de detectar virus en correos electrónicos entrantes como al detectarlos en correos electrónicos salientes.

Interactivo

Si esta opción está activada, si se detecta un virus o un programa no deseado en un correo electrónico o en datos adjuntos, aparece un cuadro de diálogo en el que puede seleccionar cómo proceder con el correo electrónico o los datos adjuntos afectados. Esta opción está activada de forma estándar.

Mostrar barra de progreso

Si esta opción está activada, Mail Protection muestra una barra de progreso durante la descarga de los correos electrónicos. Solo se puede activar esta opción si se ha seleccionado la opción **Interactivo**.

Acciones permitidas

En esta área puede seleccionar las acciones que se muestran en el cuadro de diálogo cuando se detecta un virus o un programa no deseado. Para ello, tiene que activar las opciones correspondientes.

Mover a cuarentena

Si esta opción está activada, el correo electrónico, junto con todos los datos adjuntos, se mueve a la cuarentena. Se puede enviar posteriormente mediante el Gestor de cuarentena. El email afectado se elimina. El texto principal y los datos adjuntos, si los hay, se sustituyen por un texto predeterminado.

Eliminar email

Si esta opción está activada, se borra el correo electrónico afectado cuando se detecta un virus o un programa no deseado. El texto principal y los datos adjuntos, si los hay, se sustituyen por un texto predeterminado.

Eliminar datos adjuntos

Si esta opción está activada, se sustituyen los datos adjuntos afectados por un texto predeterminado. Si está afectado el texto principal del correo electrónico, este se borra y se sustituye también por un texto predeterminado. El email en sí se entrega.

Mover datos adjuntos a cuarentena

Si esta opción está activada, se mueven los datos adjuntos afectados a la cuarentena y se borran posteriormente (se sustituyen por un texto predeterminado). El cuerpo del

texto en sí se entrega. Los datos adjuntos se pueden enviar posteriormente mediante el Gestor de cuarentena.

Omitir

Si esta opción está activada, se envía un correo electrónico afectado a pesar de que se detecta un virus o un programa no deseado.

Predeterminado

Con ayuda de este botón, puede seleccionar la acción que debe estar activada por defecto en el cuadro de diálogo cuando se detecta un virus. Marque la acción debe estar activada por defecto y haga clic en el botón "**Predeterminado"**.

Automático

Si esta opción está activada, no se notifica cuando se detecta un virus o un programa no deseado. Mail Protection reacciona en función de la configuración que ha realizado en esta sección.

Emails afectados

Se ejecuta como acción principal la opción seleccionada en "*Emails afectados*" si Mail Protection detecta un virus o un programa no deseado en un correo electrónico. Si se ha seleccionado la opción "**Omitir"**, es posible seleccionar en "*Datos adjuntos afectados***"** qué debe hacerse con los datos adjuntos si se produce una detección.

Eliminar

Si esta opción está activada, se borra automáticamente el correo electrónico afectado cuando se detecta un virus o un programa no deseado. El texto principal del correo (cuerpo) se sustituye por el texto predeterminado introducido. Lo mismo se aplica a todos los adjuntos incluidos; estos también se reemplazan con un texto predeterminado.

Omitir

Si esta opción está activada, se envía el correo electrónico afectado a pesar de que se detecta un virus o un programa no deseado. En cualquier caso, puede decidir qué hacer con los datos adjuntos afectados.

Mover a cuarentena

Si esta opción está activada, se envía a la cuarentena el correo electrónico afectado, incluidos los datos adjuntos, cuando se detecta un virus o un programa no deseado. En caso necesario, puede restaurarse posteriormente. Se borra el correo electrónico afectado. El texto principal del correo (cuerpo) se sustituye por el texto predeterminado introducido. Lo mismo se aplica a todos los adjuntos incluidos; estos también se reemplazan con un texto predeterminado.

Datos adjuntos afectados

Solo puede seleccionarse la acción "**Datos adjuntos afectados**" si en "*Emails afectados***"** se ha seleccionado el ajuste "**Omitir**". Con esta opción se decide qué debe hacerse si se produce una detección en los datos adjuntos.

Eliminar

Si esta opción está activada, se borran los datos adjuntos afectados cuando se detecta un virus o un programa no deseado y se sustituyen por un texto predeterminado.

Omitir

Si esta opción está activada, se ignoran y se envían los datos adjuntos afectados a pesar de que se detecta un virus o un programa no deseado.

Advertencia
Si esta opción está seleccionada, no tiene protección contra virus o programas no deseados por parte de Mail Protection. Seleccione esta opción solo si está seguro de lo que está haciendo. Desactive la vista previa del programa de correo electrónico y, en ningún caso, abra los datos adjuntos haciendo doble clic.

Mover a cuarentena

Si esta opción está activada, se mueven los datos adjuntos afectados a la cuarentena y se borran posteriormente (se sustituyen por un texto predeterminado). En caso necesario, pueden restaurarse posteriormente.

Acciones adicionales

Esta sección de configuración contiene la configuración adicional que indica la acción que se ejecutará cuando Mail Protection detecte un virus o programa no deseado en un correo electrónico o en los datos adjuntos.

Nota
Las acciones establecidas aquí se llevan a cabo únicamente en el caso de detectar virus en correos electrónicos entrantes.

Texto predeterminado para emails eliminados y movidos

El texto de este campo se inserta como mensaje en el email infectado sustituyéndolo. Puede editar este mensaje. El texto puede tener 500 caracteres como máximo.

Puede usar la siguiente combinación de teclas para aplicar formatos:

Ctrl + Intro = inserta un salto de línea.

Predeterminado

Este botón inserta un texto estándar predefinido en el campo de edición.

Texto predeterminado para datos adjuntos eliminados y movidos

El texto de este campo se inserta como mensaje en el email infectado sustituyendo los datos adjuntos. Puede editar este mensaje. El texto puede tener 500 caracteres como máximo.

Puede usar la siguiente combinación de teclas para aplicar formatos:

Ctrl + Intro = inserta un salto de línea.

Predeterminado

Este botón inserta un texto estándar predefinido en el campo de edición.

Heurística

Esta sección de configuración trata sobre la configuración de la heurística del motor de análisis.

Los productos de Avira integran heurísticas muy potentes con las que se puede detectar de forma proactiva el malware desconocido, es decir, antes de que se cree una firma de virus especial contra el parásito y se envíe una actualización de la protección frente a los virus. Los virus se detectan gracias a un análisis y un examen exhaustivos del código afectado de acuerdo con las funciones habituales del malware. Si el código analizado cumple estas características, se considera sospechoso. Sin embargo, esto no significa necesariamente que el código sea malware; también se pueden producir falsas alarmas. El usuario es responsable de decidir qué debe hacerse con el código afectado, p. ej., basándose en sus conocimientos de si la fuente que contiene el código afectado es de confianza.

Heurística de macrovirus

Su producto de Avira integra una heurística de macrovirus muy potente. Si esta opción está activada, durante una posible reparación se borran todas las macros del documento afectado o bien se muestra una notificación acerca de los documentos sospechosos, es decir, se muestra una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Advanced Heuristic Analysis and Detection (AHeAD)

Activar AHeAD

Su producto de Avira incorpora en la tecnología AHeAD de Avira una heurística muy potente que puede detectar también el malware desconocido (nuevo). Si esta opción está activada, aquí puede ajustar hasta qué punto es "precisa" esta heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si esta opción está activada, se detecta en menor medida el malware desconocido, pero se reduce el riesgo de posibles falsos positivos.

Nivel de detección medio

Si esta opción está activada, se garantiza una protección equilibrada con pocos falsos positivos. Este ajuste está activado de forma estándar si ha seleccionado que se aplique esta heurística.

Nivel de detección alto

Si esta opción está activada, el malware desconocido se detecta en mayor medida, pero se debe contar con falsos positivos.

AntiBot

Con la función AntiBot de Mail Protection se impide el uso indebido del equipo como parte de una red de robots de software para difundir correos electrónicos no solicitados: en el caso de la propagación de correos electrónicos no solicitados a través de una red de robots, normalmente un atacante infecta numerosos equipos con un robot que, a continuación, se conecta a un servidor IRC, tiene acceso a un determinado canal y espera aquí la orden de envío de correos electrónicos no solicitados. Para distinguir entre los correos electrónicos no solicitados procedentes de un robot de software desconocido y los correos electrónicos de los usuarios del equipo, Mail Protection analiza si el servidor SMTP y el remitente de un correo electrónico saliente están guardados en las listas de servidores y remitentes permitidos. Si no lo están, se bloquea el correo electrónico saliente, es decir, no se envía. El correo electrónico bloqueado se muestra en un cuadro de diálogo.

Nota
La función AntiBot únicamente se puede usar si se ha activado el análisis de Mail Protection para los correos electrónicos salientes (consulte la opción **Analizar emails salientes** en Mail Protection > Análisis).

Servidores permitidos

Todos los servidores de esta lista tienen permiso de Mail Protection para el envío de correos electrónicos: Mail Protection **no** bloquea los correos electrónicos que se envían a estos servidores. Si la lista no contiene ningún servidor, no se analizan los correos electrónicos salientes en lo que se refiere al servidor SMTP utilizado. Si la lista contiene entradas, Mail Protection bloquea los correos electrónicos que se envían a cualquier servidor SMTP que no conste en la lista.

Campo de entrada

En este campo se indica el nombre de host o la dirección IP del servidor SMTP que utiliza para el envío de los correos electrónicos.

Nota
Encontrará la información sobre los servidores SMTP utilizados por el programa de correo para el envío de correos electrónicos en el programa de correo, en la información de las cuentas de usuario creadas.

Añadir

El botón permite añadir el servidor que consta en el campo de entrada a la lista de servidores permitidos.

Eliminar

El botón elimina la entrada marcada de la lista de servidores permitidos. El botón está inactivo si no hay ninguna entrada seleccionada.

Eliminar todos

El botón elimina todas las entradas de la lista de servidores permitidos.

Remitentes permitidos

Mail Protection permite el envío de correos electrónicos a todos los remitentes de esta lista: Mail Protection **no** bloquea los correos electrónicos que se envían desde esta dirección de correo electrónico. Si la lista no contiene ningún remitente, no se analizan los correos electrónicos salientes en lo que se refiere a la dirección de correo electrónico del remitente. Si la lista contiene entradas, Mail Protection bloquea los correos electrónicos cuyos remitentes no consten en la lista.

Campo de entrada

En este campo se indican las direcciones de remitente de correo electrónico.

Añadir

El botón permite añadir el remitente que consta en el campo de entrada a la lista de remitentes permitidos.

Eliminar

El botón elimina la entrada marcada de la lista de remitentes permitidos. El botón está inactivo si no hay ninguna entrada seleccionada.

Eliminar todos

El botón elimina todas las entradas de la lista de remitentes permitidos.

8.8.2 General

Excepciones

Direcciones de email que no se comprueban

En esta tabla se muestra la lista de las direcciones de correo electrónico excluidas del análisis por parte de Mail Protection de Avira (lista blanca).

Nota
Mail Protection utiliza la lista de excepciones exclusivamente en el caso de correos electrónicos entrantes.

Direcciones de email que no se comprueban

Campo de entrada

Aquí se introduce la dirección de correo electrónico que desea añadir a la lista de direcciones que no se analizarán. Dependiendo de su configuración, la dirección de correo no se analizarán en el futuro por Mail Protection.

Añadir

Con este botón puede añadir la dirección de correo electrónico introducida en el campo de entrada a la lista de las direcciones de correo electrónico que no se analizarán.

Eliminar

Este botón elimina una dirección de correo electrónico marcada en la lista.

Dirección de correo electrónico

Esta dirección de correo electrónico no se analizará más.

Malware

Si esta opción está activada, no se vuelve a analizar la dirección de correo electrónico para buscar malware.

Subir

Con este botón la dirección de correo electrónico marcada se desplaza una posición hacia arriba. Este botón no está activado si no hay ninguna entrada marcada o si la dirección marcada se encuentra en la primera posición de la lista.

Bajar

Con este botón la dirección de correo electrónico marcada se desplaza una posición hacia abajo. Este botón no está activado si no hay ninguna entrada marcada o si la dirección marcada se encuentran en la última posición de la lista.

Memoria caché

La memoria caché de Mail Protection contiene los datos acerca de los correos electrónicos analizados que se muestran en la estadística del Centro de control en **Mail Protection**.

Máximo número de emails guardados en la memoria caché

Este campo contiene el número máximo de correos electrónicos que Mail Protection guarda en la memoria caché. Los correos electrónicos más antiguos son los que primero se borran.

Máximo número de días que se guarda el email

Aquí se introduce el número máximo de días durante los cuales se guarda un correo electrónico. Tras este periodo, se elimina el correo electrónico de la memoria caché.

Vaciar memoria caché

Si se hace clic en este botón, se eliminan los correos electrónicos almacenados en la memoria caché.

Pie de página

En **Pie de página** puede configurar el pie de página de los correos electrónicos que se muestra en los correos que envía.

Esta función requiere la activación de la comprobación de los correos electrónicos salientes por Mail Protection (véase la opción **Analizar emails salientes (SMTP)** en **Configuración > Mail Protection > Análisis**. Puede utilizar el pie de página predefinido de Mail Protection de Avira con el que confirma que el correo electrónico enviado se ha comprobado mediante un programa antivirus. También tiene la posibilidad de introducir un texto propio, con el fin de personalizar el pie de página. Si utiliza las dos opciones de pie de página, el texto definido por el usuario antecede al pie de página de Mail Protection de Avira.

Pie de página de los emails a enviar

Anexar pie de página de Mail Protection

Si esta opción está activada, el pie de página de Mail Protection de Avira se visualiza debajo del texto del mensaje de los correos electrónicos enviados. Gracias al pie de página de Mail Protection de Avira confirma que el correo electrónico enviado se ha comprobado mediante Mail Protection de Avira en cuanto a virus y programas no deseados y que no procede de un robot de software desconocido. El pie de página de Mail Protection de Avira contiene el texto siguiente: "*Analizado por Mail Protection de Avira [versión del producto] [abreviatura y número de versión del motor de análisis] [abreviatura y número de versión del fichero de definiciones de virus]*".

Anexar este pie de página

Si esta opción está activada, se visualiza en los correos electrónicos enviados el texto que indica en el campo de entrada.

Campo de entrada

En este campo de entrada puede introducir un texto que se visualiza como pie de página en los correos electrónicos enviados.

8.8.3 Informe

Mail Protection cuenta con una completa función de registro que puede proporcionar al usuario o al administrador información exacta acerca del tipo y la forma de una detección.

Protocolización

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Si esta opción está activada, Mail Protection no crea ningún informe.
Renuncie a realizar el registro solo en casos excepcionales, por ejemplo, solo si realiza pruebas con muchos virus o programas no deseados.

Predeterminado

Si esta opción está activada, Mail Protection registra información importante (detecciones, advertencias y errores) en el fichero de informe, obviando información importante para ganar en claridad. Este ajuste está activado de forma estándar.

Extendido

Si esta opción está activada, Mail Protection registra también información secundaria en el fichero de informe.

Completo

Si esta opción está activada, Mail Protection registra toda la información en el fichero de informe.

Limitar fichero de informe

Limitar tamaño a n MB

Si esta opción está activada, el fichero de informe se limita a un tamaño determinado; valores posibles: 1 a 100 MB. Cuando se limita el fichero de informe, se reserva un espacio aproximado de 50 kilobytes, con el fin de limitar la carga del equipo. Si el archivo de registro supera el tamaño indicado en 50 kilobytes, se borran automáticamente las entradas grandes antiguas hasta que el tamaño indicado se haya reducido en menos de 50 kilobytes.

Guardar fichero de informe antes de reducir

Si esta opción está activada, se guarda el fichero de informe antes de reducirlo. Consulte la ubicación del archivo en Configuración > General > Directorios > Directorio de informes.

Escribir configuración en fichero de informe

Si esta opción está activada, la configuración empleada de Mail Protection se registra en el fichero de informe.

Nota
Si no ha indicado ninguna limitación del fichero de informe, se crea de forma automática un nuevo fichero de informe cuando este haya alcanzado un tamaño de 100 MB. Se crea una copia de seguridad del antiguo fichero de informe. Se conservan hasta tres copias de seguridad de los ficheros de informe antiguos. Se conservan hasta tres copias de seguridad de los ficheros de informe antiguos. Las copias de seguridad más antiguas son las que primero se borran.

8.9 General

8.9.1 Categorías de riesgos

Selección de categorías de riesgos avanzadas

Su producto de Avira lo protege frente a virus informáticos. Asimismo, tiene la posibilidad de ejecutar un análisis de acuerdo con las siguientes categorías de riesgos.

- Adware
- Adware/spyware
- Aplicaciones
- Software control backdoor
- Ficheros con extensión oculta
- Programas de marcación telefónica con coste
- Suplantación de identidad (phishing)
- Programas que dañan la esfera privada
- Programas broma
- Juegos
- Software engañoso
- Utilidades de compresión poco habituales

Si se hace clic en la casilla correspondiente, se activa (con marca de verificación) o desactiva (sin marca de verificación) el tipo seleccionado.

Activar todas

Si esta opción está activada, se activan todos los tipos.

Valores predeterminados

Este botón restablece los valores estándar predefinidos.

Nota
Si se desactiva un tipo, no se siguen indicando los ficheros que se reconocen como pertenecientes al mismo. Tampoco se realiza ningún registro en el fichero de informe.

8.9.2 Protección avanzada

Protección avanzada

ProActiv

Activar ProActiv

Si esta opción está activada, se supervisan los programas de su equipo para detectar acciones sospechosas. Si se produce un comportamiento típico de malware, aparecerá un mensaje. Entonces puede bloquear el programa o seguir ejecutándolo pulsando "**Omitir**". Quedan excluidos de la supervisión los programas clasificados como fiables, los programas fiables y firmados incluidos de forma estándar en el filtro de aplicaciones permitidas y todos los programas que ha añadido al filtro de aplicaciones permitidas.

Con el uso de ProActiv se está protegiendo de nuevas y desconocidas amenazas para las que aun no existen definiciones de virus ni heurísticas. La tecnología ProActiv está integrada en Real-Time Protection y observa y analiza las acciones ejecutadas por los programas. Se analiza si el comportamiento de los programas presenta patrones de actividad típicos de malware: tipo de acción y secuencias de acciones. Si un programa muestra un comportamiento típico de malware, se trata y notifica como una detección de virus : tiene la posibilidad de bloquear la ejecución del programa o ignorar el mensaje y continuar ejecutando el programa. Puede clasificar el programa como digno de confianza y añadirlo así al filtro de aplicaciones de los programas permitidos. También puede añadir el programa a través del comando **Bloquear siempre** al filtro de aplicaciones de los programas que deben bloquearse.

Para detectar un comportamiento sospechoso, el componente ProActiv utiliza juegos de reglas desarrollados por el Avira Malware Research Center. Los juegos de reglas los proporcionan las bases de datos de Avira. Para recopilar información en las bases de datos de Avira, ProActiv envía información sobre programas sospechosos notificados. Durante la instalación de Avira, tiene la posibilidad de desactivar la transmisión de datos a las bases de datos de Avira.

Nota
La tecnología ProActiv todavía no está disponible para sistemas de 64 Bit.

Protection Cloud

Activar Protection Cloud

Se envían a Avira Cloud todas las huellas de los ficheros sospechosos para la detección en línea dinámica. Los ficheros de aplicación se indican de inmediato como limpios, infectados o desconocidos.

El sistema Protection Cloud sirve como punto de nodo central para detectar los ataques cibernéticos a la comunidad de Avira. Se comparan los ficheros a los que accede su PC con los archivos de muestra que hay guardados en el sistema de nube. Gracias a que la tarea principal se desarrolla en la nube, el programa de protección local consume menos recursos.

En cada **análisis rápido del sistema** se crea una lista de las ubicaciones de guardado de ficheros. En esta lista se incluyen, por ejemplo, procesos en curso y programas de inicio y de servicio. De cada archivo se crea una suma de comprobación digital ("huella") que se envía al sistema Protection Cloud y se clasifica como "limpio" o "malware". Los ficheros de programas desconocidos se cargan para el análisis en el sistema Protection Cloud.

Confirmar manualmente si se han enviado ficheros sospechosos a Avira

Puede comprobar la lista de los ficheros sospechosos que se deben cargar en Protection Cloud y seleccionar qué archivos quiere cargar.

Análisis de archivos en tiempo real

Si esta opción está activada, los ficheros de programas desconocidos se cargan en el sistema Protection Cloud para el análisis tan pronto como se accede a ellos.

Mostrar progreso de las cargas en Avira Protection Cloud

Una ventana muestra la siguiente información sobre los ficheros cargados en forma de una barra de progreso:

- Ubicación del fichero
- Nombre del fichero
- Estado (cargando / analizando)
- Resultado (limpio / infectado)

En *Aplicaciones a bloquear* puede incorporar aplicaciones que considera nocivas y que desea que Avira ProActiv bloquee de forma estándar. Las aplicaciones incorporadas no pueden ejecutarse en su equipo. Además, puede añadir programas al filtro de las aplicaciones que se deben bloquear a través del mensaje de Real-Time Protection acerca de un comportamiento sospechoso de un programa, utilizando la opción **Bloquear siempre este programa**.

Aplicaciones a bloquear

Aplicación

La lista contiene todas las aplicaciones que ha clasificado como nocivas y añadido a través de la configuración o los mensajes del componente ProActiv. Avira ProActiv bloquea las aplicaciones de la lista, por lo que no pueden ejecutarse en su equipo. Al iniciarse un programa bloqueado, aparece un mensaje del sistema operativo. Avira ProActiv identifica las aplicaciones que se deben bloquear a partir de la ruta y el nombre de fichero indicados y se bloquean independientemente de su contenido.

Campo de entrada

Indique en este campo la aplicación que desea bloquear. Para la identificación de la aplicación, es necesario indicar la ruta completa y el nombre del fichero junto con su extensión. La indicación de la ruta debe incluir la unidad que contiene la aplicación o comenzar con una variable de entorno.

Mediante este botón se abre una ventana en la que puede seleccionar la aplicación que se debe bloquear.

Añadir

Mediante el botón "**Añadir"** es posible añadir la aplicación que consta en el campo de entrada en la lista de aplicaciones que se deben bloquear.

Nota
No se pueden añadir aplicaciones necesarias para la funcionalidad del sistema operativo.

Eliminar

Mediante el botón "**Eliminar"** puede borrar la aplicación marcada de la lista de aplicaciones que se deben bloquear.

En *Aplicaciones a excluir* se enumeran las aplicaciones excluidas de la supervisión por el componente ProActiv: programas que se han clasificado como fiables y están en la lista de forma estándar, todas las aplicaciones que ha clasificado como fiables y añadido al filtro de aplicación: en la configuración puede añadir aplicaciones a la lista de las aplicaciones permitidas. Asimismo, tiene la posibilidad de añadir aplicaciones a través de los mensajes de Real-Time Protection acerca de un comportamiento del programa sospechoso, activando en el mensaje de Real-Time Protection la opción **Programa de confianza**.

Aplicaciones a excluir

Aplicación

La lista contiene aplicaciones excluidas de la supervisión por el componente ProActiv. Con la configuración predeterminada tras la instalación, la lista contiene aplicaciones

firmadas de fabricantes de confianza. Tiene la posibilidad de incorporar aplicaciones que considera de confianza a través de la configuración o los mensajes de Real-Time Protection. El componente ProActiv identifica las aplicaciones por la ruta, el nombre de fichero y el contenido. La comprobación del contenido es útil, ya que puede añadirse un código dañino a un programa con posterioridad, por ejemplo, a través de actualizaciones. Puede determinar a través del **tipo** indicado si desea realizar un análisis del contenido: si el tipo es "*Contenido*", las aplicaciones indicadas con ruta y nombre de fichero se comprueban en cuanto a las modificaciones de su contenido, antes de que se excluyan de la supervisión por parte del componente ProActiv. Si el contenido del archivo ha variado, el componente ProActiv vuelve a supervisar la aplicación. Si se trata del tipo "*Ruta*", no se analiza el contenido antes de excluir la aplicación de la supervisión por Real-Time Protection. Para cambiar el tipo de exclusión, haga clic en el tipo indicado.

Advertencia
Utilice el tipo "*Ruta*" solo en casos excepcionales. A través de una actualización se puede añadir código dañino a una aplicación. La aplicación antes inofensiva se convierte en malware.

Nota
Algunas aplicaciones de confianza, como p. ej., todos los componentes de aplicación de su producto de Avira, están excluidas de forma estándar de la supervisión por el componente ProActiv, pero no figuran en la lista.

Campo de entrada

Indique en este campo las aplicaciones que desea excluir de la supervisión por el componente ProActiv. Para la identificación de la aplicación, es necesario indicar la ruta completa y el nombre del fichero junto con su extensión. La indicación de la ruta debe incluir la unidad que contiene la aplicación o comenzar con una variable de entorno.

Si se pulsa este botón, se abre una ventana en la que puede seleccionar la aplicación que se debe omitir.

Añadir

Mediante el botón "**Añadir**" puede incorporar la aplicación que consta en el campo de entrada en la lista de aplicaciones omitidas.

Eliminar

Mediante el botón "**Eliminar**" puede borrar la aplicación marcada de la lista de aplicaciones omitidas.

8.9.3 Contraseña

Puede proteger su producto de Avira en diferentes áreas mediante una contraseña. Si se ha definido una contraseña, esta se le solicita cada vez que quiera acceder a esta área protegida.

Contraseña

Introducir contraseña

Introduzca aquí la contraseña que desee. Como medida de seguridad, los caracteres que introduce en este campo se sustituyen por asteriscos (*). Puede introducir un máximo de 20 caracteres. Una vez que se ha introducido la contraseña, el programa impide el acceso al introducir una contraseña incorrecta. Un campo vacío significa que "No hay contraseña".

Confirmación

Introduzca de nuevo la contraseña introducida antes para confirmarla. Como medida de seguridad, los caracteres que introduce en este campo se sustituyen por asteriscos (*).

Nota
Se distingue entre mayúsculas y minúsculas.

Áreas protegidas con contraseña

Su producto Avira puede proteger distintas áreas con una contraseña. Si se hace clic en la casilla correspondiente, puede desactivarse y activarse la solicitud de contraseña para las diferentes áreas.

Área protegida con contraseña	Función
Centro de control	Si esta opción está activada, es necesaria la contraseña definida para iniciar el Centro de control.
Activar/desactivar Real-Time Protection	Si esta opción está activada, es precisa la contraseña definida para activar o desactivar Real-Time Protection de Avira.

Activar/desactivar Mail Protection	Si esta opción está activada, es precisa la contraseña definida para activar o desactivar Mail Protection.
Activar/desactivar FireWall	Si esta opción está activada, es precisa la contraseña definida para activar o desactivar FireWall.
Activar/desactivar Web Protection	Si esta opción está activada, es precisa la contraseña definida para activar o desactivar Web Protection.
Cuarentena	Si esta opción está activada,
Restaurar los objetos afectados	Si esta opción está activada, es necesaria la contraseña definida para restaurar un objeto.
Volver a analizar objetos afectados	Si esta opción está activada, es necesaria la contraseña definida para volver a comprobar un objeto.
Propiedades de los objetos afectados	Si esta opción está activada, es necesaria la contraseña definida para mostrar las propiedades de un objeto.
Eliminar los objetos afectados	Si esta opción está activada, es necesaria la contraseña definida para borrar un objeto.
Enviar un email a Avira	Si esta opción está activada, es necesaria la contraseña definida para enviar al Centro de investigación de malware de Avira un objeto y comprobarlo.
Copiar los objetos afectados	Si esta opción está activada, es necesaria la contraseña definida para copiar los objetos afectados.

Añadir y modificar tareas	Si esta opción está activada, es necesaria la contraseña definida para añadir y modificar tareas en el planificador.
Descargar CD de rescate de Internet	Si esta opción está activada, es necesaria la contraseña definida para iniciar la descarga del CD de rescate de Avira.
Configuración	Si esta opción está activada, solo es posible la configuración del programa tras introducir la contraseña definida.
Instalación/desinstalación	Si esta opción está activada, es necesaria la contraseña definida para instalar o desinstalar el programa.

8.9.4 Seguridad

Ejecución automática

Bloquear función de ejecución automática

Si esta opción está activada, se bloquea la función de Windows Ejecución automática en todas las unidades asociadas, como lápices USB, unidades de CD y DVD y unidades de red. Con la función de Windows Ejecución automática se leen de inmediato los archivos en soportes de datos o unidades de red al insertarlos o asociarlos, de modo que los archivos se inician y reproducen automáticamente. Sin embargo, esta funcionalidad conlleva un elevado riesgo en la seguridad, ya que el inicio automático de ficheros permite la instalación de malware y programas no deseados. La función Ejecución automática es especialmente importante para los lápices USB, ya que los datos de un lápiz pueden modificarse constantemente.

Excluir CD y DVD

Si esta opción está activada, se permite la función de Windows Ejecución automática en las unidades de CD y DVD.

Advertencia
Desactive la función Ejecución automática para las unidades de CD y DVD únicamente si está seguro de que solo utiliza soportes de datos de confianza.

Protección del sistema

Proteger el fichero host de Windows de cualquier cambio

Si esta opción está activada, el fichero host de Windows está protegido contra escritura. Ya no es posible manipular el fichero. Por ejemplo, ningún malware podrá redirigirlo a páginas web no deseadas. Esta opción está activada de forma estándar.

Protección del producto

Nota
Las opciones de protección del producto no están disponibles si no se ha instalado Real-Time Protection durante una instalación personalizada.

Proteger los procesos contra finalización no deseada

Si esta opción está activada, todos los procesos del programa quedan protegidos contra una finalización no deseada a causa de virus y malware o bien contra la finalización 'incontrolada' por parte de un usuario, p. ej., a través del Administrador de tareas. Esta opción está activada de forma estándar.

Protección extendida de procesos

Si esta opción está activada, todos los procesos del programa quedan protegidos contra la finalización no deseada mediante métodos extendidos. La protección extendida de procesos requiere significativamente más recursos del equipo que la protección simple de procesos. Esta opción está activada de forma estándar. Para desactivar la opción, se debe reiniciar el equipo.

Nota
La protección de procesos no está disponible en Windows XP 64 Bit .

Advertencia
Si está activada la protección de procesos, pueden producirse problemas de interacción con otros productos de software. En estos casos, desactive la protección de procesos.

Proteger los ficheros y las entradas del registro contra manipulaciones

Si esta opción está activada, todas las entradas en el registro del programa, así como todos los ficheros del programa (ficheros binarios y de configuración), quedan protegidos contra manipulaciones. La protección contra manipulaciones consta de la protección contra acceso de escritura, eliminación y parcialmente de lectura a las entradas del registro o a los ficheros de programa por parte de los usuarios o programas de terceros. Para activar la opción, se debe reiniciar el equipo.

Advertencia
Tenga en cuenta que, con la opción desactivada, puede resultar imposible la reparación de ordenadores infectados con determinados tipos de malware.

Nota
Si esta opción está activada, la modificación de la configuración, y también la modificación de tareas de análisis o actualización, solo es posible por medio de la interfaz de usuario.

Nota
La protección de ficheros y entradas del registro no está disponible en Windows XP 64 Bit .

8.9.5 WMI

Compatibilidad con Instrumental de administración de Windows (WMI)

Instrumental de administración de Windows (Windows Management Instrumentation) es una tecnología fundamental de administración de Windows que, mediante lenguajes de script y de programación, permite el acceso de lectura, escritura, local y remoto a la configuración de los equipos con Windows. Su producto de Avira es compatible con WMI y ofrece datos (información de estado, datos estadísticos, informes, tareas programadas, etc.), así como los eventos y métodos (detener e iniciar procesos), en una interfaz. Por medio de WMI, tiene la posibilidad de consultar datos operativos del programa y controlar el programa. Puede solicitar referencias de la interfaz WMI al fabricante. Tras firmar un acuerdo de confidencialidad, recibirá la referencia en formato PDF.

Activar compatibilidad con WMI

Si esta opción está activada, gracias a WMI tiene la posibilidad de consultar datos operativos del programa y controlar el programa.

Permitir activar/desactivar servicios

Si esta opción está activada, gracias a WMI tiene la posibilidad de activar y desactivar datos operativos del programa y controlar el programa.

8.9.6 Eventos

Limitar tamaño de base de datos de eventos

Limitar el tamaño a un máximo de n entrada(s)

Si esta opción está activada, el número máximo de entradas en la base de datos de eventos se puede limitar hasta un tamaño concreto; los valores permitidos se

encuentran entre 100 y 10 000 registros. Si se supera el número de registros introducidos, se borran las entradas más antiguas.

Eliminar todos los eventos de hace más de n día(s)

Si esta opción está activada, se borran de la base de datos de eventos los eventos transcurridos un cierto número de días; los valores permitidos se encuentran entre 1 y 90 días. Esta opción está activada de forma estándar con un valor de 30 días.

Sin limitación

Si esta opción está activada, no se limita el tamaño de la base de datos de eventos. No obstante, en la interfaz de programa en **Eventos** se muestra un máximo de 20 000 registros.

8.9.7 Informes

Limitar informes

Limitar a un máximo de n unidad(es)

Si esta opción está activada, el número máximo de informes se puede limitar hasta un número concreto; los valores permitidos se encuentran entre 1 y 300 registros. Si se supera el número introducido, se borran los informes más antiguos.

Eliminar los informes anteriores a n día(s)

Si esta opción está activada, se borran automáticamente los informes transcurrido un cierto número de días; los valores permitidos se encuentran entre 1 y 90 días. Esta opción está activada de forma estándar con un valor de 30 días.

Sin limitación

Si esta opción está activada, no se limita el número de informes.

8.9.8 Directorios

Ruta temporal

Usar configuración del sistema

Si esta opción está activada, se utiliza la configuración del sistema para manejar los ficheros temporales.

Nota
La ubicación en la que el sistema guarda los archivos temporales se encuentra (por ejemplo, en Windows XP) en: **Inicio > Configuración > Panel de control > Sistema >** pestaña "**Opciones avanzadas**" > botón "**Variables de entorno**". Las variables temporales (`TEMP`, `TMP`) son visibles, junto con sus valores

correspondientes, para el usuario conectado y las variables del sistema (`TEMP`, `TMP`).

Usar el directorio siguiente

Si esta opción está activada, se utiliza la ruta mostrada en el campo de entrada.

Campo de entrada

En este campo de entrada puede introducir la ruta en la que el programa debe guardar los ficheros temporales.

...

El botón abre una ventana en la que puede seleccionar la ruta temporal que desee.

Predeterminado

El botón restablece el directorio predefinido de la ruta temporal.

Directorio de informes

Campo de entrada

Este campo de entrada contiene la ruta absoluta al directorio de informes.

...

Si se pulsa este botón, se abre una ventana en la que puede seleccionar el directorio deseado.

Predeterminado

El botón restablece la ruta predefinida al directorio de informes.

Directorio de cuarentena

Campo de entrada

Este campo de entrada contiene la ruta al directorio de cuarentena.

...

Si se pulsa este botón, se abre una ventana en la que puede seleccionar el directorio deseado.

Predeterminado

El botón restablece la ruta predefinida al directorio de cuarentena.

8.9.9 Advertencias acústicas

Cuando Scanner o Real-Time Protection detectan virus o malware, en el modo de acción interactivo se emite un sonido de advertencia. Puede desactivar o activar el sonido de advertencia, así como seleccionar un fichero WAVE distinto para el sonido de advertencia.

Nota
El modo de acción de Scanner se ajusta en la configuración en Seguridad del PC > Scanner > Análisis > Acción al detectar. El modo de acción de Real-Time Protection se ajusta en la configuración en Seguridad del PC > Real-Time Protection > Análisis > Acción al detectar.

Sin advertencia

Si esta opción está activada, en caso de que Scanner o Real-Time Protection detecten virus, no se emite ninguna advertencia acústica.

Reproducir a través de altavoces del PC (solo en modo interactivo)

Si esta opción está activada, en caso de que Scanner o Real-Time Protection detecten virus, se emite una advertencia acústica con el sonido de advertencia predeterminado. El sonido de advertencia se reproduce a través del altavoz interno del PC.

Usar el siguiente fichero WAVE (solo en modo interactivo)

Si esta opción está activada, en caso de que Scanner o Real-Time Protection detecten virus, se emite una advertencia acústica con el fichero WAVE seleccionado. El fichero WAVE seleccionado se reproduce a través de un altavoz externo conectado.

Fichero WAVE

En este campo, puede introducir el nombre y ruta del fichero de audio deseado. El tono de advertencia predeterminado del programa se guarda como valor predefinido.

...

El botón abre una ventana en la que puede navegar hasta el fichero con la ayuda del explorador de ficheros.

Prueba

Este botón se utiliza para comprobar el fichero WAVE seleccionado.

8.9.10 Advertencias

Red

Puede enviar advertencias configurables individualmente de Scanner o Real-Time Protection a los equipos deseados de su red.

Nota
Compruebe si se ha iniciado "Servicio de alerta". Puede encontrar este servicio en (por ejemplo, en Windows XP) "**Inicio > Configurar > Panel de control > Herramientas administrativas > Servicios**".

Nota
Se envía siempre una advertencia al equipo, **no** a un usuario determinado.

Advertencia
La función **ya no es compatible** con los siguientes sistemas operativos:
- Windows Server 2008 y superior
- Windows Vista y superior.

Enviar mensaje a

La lista de esta ventana muestra los nombres de los equipos que reciben un mensaje tras una detección.

Nota
Solo se puede registrar un ordenador una vez en esta lista.

Insertar

Con este botón puede añadir otro equipo. Se abre una ventana en la que puede introducir el nombre del equipo nuevo. El nombre del equipo puede tener 15 caracteres como máximo.

Al pulsar el botón, se abre una ventana en la que puede seleccionar directamente un equipo de su entorno de red.

Eliminar

Con este botón puede borrar de la lista el registro marcado actualmente.

Real-Time Protection - Advertencias de red

Advertencias de red

Si esta opción está activada, se envían advertencias de red. Esta opción está desactivada de forma estándar.

Nota
Con el fin de poder activar esta opción, debe haber registrado al menos un destinatario en Configuración > General > Advertencias > Red.

Mensaje para enviar

En la ventana se muestra el mensaje que se envía al equipo seleccionado tras una detección. Puede editar este mensaje. El texto puede tener 500 caracteres como máximo.

Es posible utilizar las siguientes combinaciones de teclas para formatear el mensaje:

Comando de teclas	Descripción
Ctrl + Tab	Inserta una tabulación. La línea actual se desplaza algunos caracteres hacia la derecha.
Ctrl + Intro	Inserta un salto de línea.

El mensaje puede incluir además comodines para la información importante durante el análisis. Estos comodines se sustituyen con el texto real durante el proceso de envío.

Es posible utilizar los comodines siguientes:

Comodín	Descripción
%VIRUS%	Contiene el nombre del virus encontrado o el programa no deseado.
%FILE%	Contiene la ruta y el nombre del archivo afectado.
%COMPUTER%	Contiene el nombre del equipo en el que se está ejecutando Real-Time Protection.
%NAME%	Contiene el nombre del usuario que ha accedido al fichero afectado.
%ACTION%	Incluye la acción que se ha ejecutado después de la detección del virus.
%MACADDR%	Contiene la dirección MAC del equipo en el que se está ejecutando Real-Time Protection.

Predeterminado

El botón restablece el texto predeterminado predefinido de una advertencia.

Scanner - Advertencias de red

Advertencias de red

Si esta opción está activada, se envían advertencias de red. Esta opción está desactivada de forma estándar.

> **Nota**
> Con el fin de poder activar esta opción, debe haber registrado al menos un destinatario en Configuración > General > Advertencias > Red.

Mensaje para enviar

En la ventana se muestra el mensaje que se envía al equipo seleccionado tras una detección. Puede editar este mensaje. El texto puede tener 500 caracteres como máximo.

Es posible utilizar las siguientes combinaciones de teclas para formatear el mensaje:

Comando de teclas	Descripción
Ctrl + Tab	Inserta una tabulación. La línea actual se desplaza algunos caracteres hacia la derecha.
Ctrl + Intro	Inserta un salto de línea.

El mensaje puede incluir además comodines para la información importante durante el análisis. Estos comodines se sustituyen con el texto real durante el proceso de envío.

Es posible utilizar los comodines siguientes:

Comodín	Descripción
`%VIRUS%`	Contiene el nombre del virus encontrado o el programa no deseado.
`%NAME%`	Contiene el nombre del usuario conectado que está ejecutando Scanner.
`%COMPUTER%`	Contiene el nombre del equipo en el que se está ejecutando Scanner.

Predeterminado

El botón restablece el texto predeterminado predefinido de una advertencia.

Email

El producto de Avria puede enviar, ante determinados eventos, advertencias y mensajes por correo electrónico a uno o más destinatarios. Para ello, se emplea el protocolo simple de transferencia de correo (SMTP).

Los mensajes pueden estar causados por diferentes eventos. Los componentes siguientes son compatibles con el envío de correos electrónicos:

- Real-Time Protection - Notificaciones de correo electrónico
- Scanner - Notificaciones de email
- Updater - Notificaciones de email

> **Nota**
> Tenga en cuenta que ESMTP no es compatible. Además, actualmente no es posible la transmisión cifrada por TLS (Transport Layer Security) ni SSL (Secure Sockets Layer).

Mensajes de email

Servidor SMTP

Introduzca el nombre del host que va a utilizarse, ya sea su dirección IP o el nombre del host directo.
La longitud máxima posible del nombre del host es de 127 caracteres.

Por ejemplo:

`192.168.1.100` o `mail.empresadeejemplo.de`.

Puerto

Introduzca aquí el puerto que debe utilizarse.

Dirección del remitente

En este campo puede introducir la dirección o direcciones de correo electrónico del remitente. La longitud máxima de la dirección del remitente es de 127 caracteres.

Autenticación

Algunos servidores de correo electrónico esperan que un programa se autentique (registre) en el servidor antes de enviar un correo electrónico. Las advertencias por correo electrónico se pueden transmitir con la autenticación en un servidor SMTP.

Usar autenticación

Si esta opción está activada, es posible introducir un nombre de usuario y una contraseña en los campos correspondientes para el registro (autenticación).

Nombre de usuario
Introduzca aquí el nombre de usuario.
Contraseña
Introduzca aquí la contraseña correspondiente. Esta contraseña se guarda cifrada. Como medida de seguridad, los caracteres que introduce en este campo se sustituyen por asteriscos (*).

Enviar email de prueba

Si se hace clic en este botón, el programa intenta enviar un correo electrónico de prueba a la dirección del remitente para comprobar los datos introducidos.

Real-Time Protection - Notificaciones de correo electrónico

Real-Time Protection de Avira puede enviar, ante determinados eventos, advertencias por correo electrónico a uno o más destinatarios.

Advertencias por email

Si esta opción está activada, Real-Time Protection de Avira envía mensajes de correo electrónico con la información más importante cuando se produce un evento determinado. Esta opción está desactivada de forma estándar.

Notificación por email de los siguientes eventos

El análisis en tiempo real detectó un virus o programa no deseado

Si esta opción está activada, recibe un correo electrónico con el nombre del virus o programa no deseado y el fichero afectado, siempre que el análisis en tiempo real detecte alguno de ellos.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "Detección durante análisis en tiempo real". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Se ha producido un error crítico en Real-Time Protection

Si esta opción está activada, al detectar un error crítico interno, recibe un correo electrónico.

> **Nota**
> En este caso, contacte con Soporte técnico e incluya los datos indicados en el correo electrónico. El fichero especificado también debería enviarse para examinarlo.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "Error crítico en Real-Time Protection". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Destinatario

En este campo puede introducir la dirección o direcciones de correo electrónico del o de los destinatarios. Cada dirección se separa mediante una coma; como máximo se pueden introducir 260 caracteres (longitud total de la cadena de caracteres).

Scanner - Notificaciones de email

El análisis directo, es decir la búsqueda a petición, puede enviar, ante determinados eventos, advertencias y mensajes por correo electrónico a uno o más destinatarios.

Advertencias por email

Si esta opción está activada, el programa envía mensajes de correo electrónico con la información más importante cuando se produce un evento determinado. Esta opción está desactivada de forma estándar.

Notificación por email de los siguientes eventos

Durante el análisis se notificó una detección

Si esta opción está activada, recibe un correo electrónico con el nombre del virus o programa no deseado y el fichero afectado, siempre que el análisis directo detecte alguno de ellos.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "Detección durante análisis". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Fin de un análisis programado

Si esta opción está activada, se envía un correo electrónico tras haber ejecutado una tarea de análisis. El correo electrónico contiene datos sobre cuándo se realizó el análisis y su duración, los directorios y ficheros analizados, así como sobre la detección de virus y las advertencias.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "Fin del análisis". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Añadir fichero de informe como adjunto

Si esta opción está activada, el fichero de informe actual del componente Scanner se adjunta al correo electrónico cuando se envían las notificaciones del componente Scanner.

Destinatario

En este campo puede introducir la dirección o direcciones de correo electrónico del o de los destinatarios. Cada dirección se separa mediante una coma. La longitud máxima de todas las direcciones (es decir, la cadena de caracteres completa) es de 260 caracteres.

Updater - Notificaciones de email

En determinados eventos, el componente Updater puede enviar mensajes por correo electrónico a uno o más destinatarios.

Advertencias por email

Si esta opción está activada, el componente Updater envía mensajes de correo electrónico con los datos más importantes cuando se produce un evento determinado. Esta opción está desactivada de forma estándar.

Notificaciones por email de los siguientes eventos

Actualización innecesaria. El programa está actualizado.

Si esta opción está activada, se envía un correo electrónico cuando Updater ha podido establecer correctamente una conexión con el servidor de descargas, pero en el servidor no hay disponible ningún fichero nuevo. Esto significa que su producto de Avira está actualizado.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "Actualización innecesaria". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Actualización finalizada con éxito. Se instalaron ficheros nuevos.

Si esta opción está activada, se envía un correo electrónico con todas las actualizaciones realizadas: se puede tratar de una actualización de un producto o una actualización del fichero de definición de virus o el motor de análisis.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "La actualización finalizó con éxito. Se instalaron ficheros nuevos". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Error de actualización

Si esta opción está activada, se envía un correo electrónico si se ha producido un error durante la actualización.

Editar

Con el botón "**Editar**" se abre la ventana "**Plantilla de email**" en la que puede configurar el mensaje sobre el evento "Error de actualización". Tiene la posibilidad de introducir el texto del asunto y el mensaje del correo electrónico. Puede utilizar variables. (Véase Plantilla de email.)

Añadir fichero de informe como adjunto

Si esta opción está activada, el fichero de informe actual del componente Updater se adjunta al correo electrónico cuando se envían las notificaciones del Updater.

Destinatario

En este campo puede introducir la dirección o direcciones de correo electrónico del o de los destinatarios. Cada dirección se separa mediante una coma. La longitud máxima de todas las direcciones (es decir, la cadena de caracteres completa) es de 260 caracteres.

Plantilla de email

En la ventana **Plantilla de email** configure las notificaciones de correo electrónico de los componentes individuales sobre los eventos activados. Puede introducir un texto con un máximo de 128 caracteres en la línea del asunto y un texto con un máximo de 1024 caracteres en el campo del texto del mensaje.

Es posible emplear las variables siguientes en el asunto y el texto del correo electrónico:

Variables válidas globalmente

Variable	Valor
Variables de entorno de Windows	El componente de las notificaciones de correo electrónico es compatible con todas las variables de entorno de Windows.
%SYSTEM_IP%	Dirección IP del equipo.

%FQDN%	Nombre completo del dominio (fully qualified domain name).
%TIMESTAMP%	Sello de hora del evento: formatos de la hora y la fecha en función de la configuración del idioma del sistema operativo.
%COMPUTERNAME%	Nombre del ordenador NetBIOS.
%USERNAME%	Nombre del usuario que accede al componente.
%PRODUCTVER%	Versión del producto.
%PRODUCTNAME%	Nombre del producto.
%MODULENAME%	Nombre del componente que envía el correo electrónico.
%MODULEVER%	Versión del componente que envía el correo electrónico.

Variables específicas del componente

Variable	Valor	Correos electrónicos de los componentes
%ENGINEVER%	Versión del motor de análisis empleado.	Real-Time Protection Scanner
%VDFVER%	Versión del archivo de definición de virus empleado.	Real-Time Protection Scanner

%SOURCE%	Nombre completo del fichero.	Real-Time Protection
%VIRUSNAME%	Nombre del virus o el programa no deseado.	Real-Time Protection
%ACTION%	Acción que se ha ejecutado después de la detección.	Real-Time Protection
%MACADDR%	Dirección MAC de la tarjeta de red registrada en primer lugar.	Real-Time Protection
%UPDFILESLIST%	Lista de los ficheros actualizados.	Updater
%UPDATETYPE%	Tipo de actualización: actualización del motor de análisis y fichero de definición de virus o actualización del producto con actualización del motor de análisis y fichero de definición de virus.	Updater
%UPDATEURL%	URL del servidor de descarga que se ha empleado para la actualización.	Updater
%UPDATE_ERROR%	Texto de los errores de la actualización.	Updater
%DIRCOUNT%	Número de los directorios analizados.	Scanner
%FILECOUNT%	Número de los ficheros analizados.	Scanner
%MALWARECOUNT%	Números de los virus o programas no deseados detectados.	Scanner
%REPAIREDCOUNT%	Número de los ficheros afectados reparados.	Scanner

%RENAMEDCOUNT%	Número de los ficheros afectados a los que se ha cambiado el nombre.	Scanner
%DELETEDCOUNT%	Número de los ficheros afectados borrados.	Scanner
%WIPECOUNT%	Número de los ficheros afectados que se han sobrescrito y eliminado.	Scanner
%MOVEDCOUNT%	Número de los ficheros afectados que se han aislado.	Scanner
%WARNINGCOUNT%	Número de las advertencias.	Scanner
%ENDTYPE%	Estado del final del análisis: Cancelado | Finalizado con éxito.	Scanner
%START_TIME%	Momento de inicio del análisis Momento de inicio de la actualización	Scanner, Updater
%END_TIME%	Final del análisis Final de la actualización	Scanner, Updater
%TIME_TAKEN%	Duración en minutos de la ejecución del análisis Duración en minutos de la ejecución de la actualización	Scanner, Updater
%LOGFILEPATH%	Ruta y nombre del fichero de informe.	Scanner, Updater

Advertencias acústicas

Cuando Scanner o Real-Time Protection detectan virus o malware, en el modo de acción interactivo se emite un sonido de advertencia. Puede desactivar o activar el sonido de advertencia, así como seleccionar un fichero WAVE distinto para el sonido de advertencia.

Nota
El modo de acción de Scanner se ajusta en la configuración en Seguridad del PC > Scanner > Análisis > Acción al detectar. El modo de acción de Real-Time

Protection se ajusta en la configuración en Seguridad del PC > Real-Time Protection > Análisis > Acción al detectar.

Sin advertencia

Si esta opción está activada, en caso de que Scanner o Real-Time Protection detecten virus, no se emite ninguna advertencia acústica.

Reproducir a través de altavoces del PC (solo en modo interactivo)

Si esta opción está activada, en caso de que Scanner o Real-Time Protection detecten virus, se emite una advertencia acústica con el sonido de advertencia predeterminado. El sonido de advertencia se reproduce a través del altavoz interno del PC.

Usar el siguiente fichero WAVE (solo en modo interactivo)

Si esta opción está activada, en caso de que Scanner o Real-Time Protection detecten virus, se emite una advertencia acústica con el fichero WAVE seleccionado. El fichero WAVE seleccionado se reproduce a través de un altavoz externo conectado.

Fichero WAVE

En este campo, puede introducir el nombre y ruta del fichero de audio deseado. El tono de advertencia predeterminado del programa se guarda como valor predefinido.

El botón abre una ventana en la que puede navegar hasta el fichero con la ayuda del explorador de ficheros.

Prueba

Este botón se utiliza para comprobar el fichero WAVE seleccionado.

Advertencias

Ante determinados eventos, su producto de Avira emite notificaciones en el escritorio, los denominados avisos emergentes, con los que se le informa acerca de riesgos y procesos incorrectos de programas, como p. ej., la ejecución de una actualización. En **Advertencias** tiene la opción de activar o desactivar las notificaciones para determinados eventos.

En las notificaciones en el escritorio es posible desactivar la notificación directamente en el aviso emergente. Puede volver a activar las notificaciones en la ventana de configuración **Advertencias**.

Actualización

Alertar, si la última actualización se produjo hace más de n días

En este campo puede introducir el número de días que pueden transcurrir como máximo desde la última actualización. Si se supera este período, en el centro de control en Estado se muestra un icono rojo que indica el estado de la actualización.

Mostrar mensaje si el fichero de firmas de virus está obsoleto

Si esta opción está activada, se muestra un mensaje de advertencia en el caso de un fichero de definición de virus antiguo. Con ayuda de la opción "Advertencia si desde la última actualización hace más de n día(s)" puede configurar el intervalo de tiempo del mensaje de advertencia.

Advertencias/mensajes relativos a las siguientes situaciones

Se utiliza la conexión de marcación

Si esta opción está activada, se advierte mediante una notificación en el escritorio cuando en su equipo un programa de marcación ha establecido una conexión de marcación mediante la red telefónica o la red ISDN. Existe el peligro de que el programa de marcación sea desconocido y no deseado y establezca una conexión sujeta a costes. (Consulte Categorías de riesgos: Programas de marcación telefónica con coste)

Los ficheros se han actualizado con éxito

Si esta opción está activada, se muestra una notificación en el escritorio cuando se ha finalizado correctamente una actualización y se han actualizado los ficheros.

Error de actualización

Si esta opción está activada, se muestra una notificación en el escritorio cuando se ha producido un error durante la actualización: no se ha podido establecer ninguna conexión con el servidor de descargas o no se han podido instalar los ficheros de actualización.

No es necesaria ninguna actualización

Si esta opción está activada, se muestra una notificación en el escritorio cuando se ha iniciado una actualización, pero no era necesaria, ya que su programa está actualizado.

9. El icono de bandeja

El icono de la bandeja situado en la bandeja del sistema de la barra de tareas muestra el estado de Real-Time Protection y del FireWall.

Icono	Descripción
	Se han activado Real-Time Protection y FireWall
	Se ha desactivado Real-Time Protection o FireWall

Entradas en el menú contextual

- **Activar Real-Time Protection**: Activa o desactiva Avira Real-Time Protection.
- **Activar Mail Protection**: Activa o desactiva Avira Mail Protection.
- **Activar Web Protection**: Activa o desactiva Avira Web Protection.
- **FireWall**:
  - **Activar FireWall**: Activa o desactiva Avira FireWall.
  - **Activar Windows Firewall**: Activa o desactiva Windows Firewall (esta función está disponible a partir de Windows 8).
  - **Bloquear todo el tráfico**: Si está activa, bloquea cualquier transferencia de datos excepto aquellas que vayan dirigidas al propio ordenador (Local Host / IP 127.0.0.1).
- **Iniciar Avira Professional Security**: Abre el Centro de control.
- **Configurar Avira Professional Security**: Abre la configuración.
- **Iniciar actualización**: Inicia una actualización.
- **Seleccionar configuración**:
  Abre un submenú que contiene los perfiles de configuración disponibles. Haga clic en una configuración para activarla. El comando de menú estará desactivado si ya se han definido las reglas para la selección automática de una configuración.
- **Ayuda**: Abre la ayuda en línea.
- **Acerca de Avira Professional Security**:
  Abre una ventana de diálogo con información relativa a su producto Avira: información de producto, versión y licencias.
- **Avira en Internet**:
  Abre el portal web de Avira en Internet. Para ello, es imprescindible disponer de un acceso activo a Internet.

10. FireWall

Avira Professional Security le permite supervisar y ajustar el tráfico de datos entrante y saliente conforme a la configuración de su equipo:

- Avira FireWall

Avira FireWall se incluye en su Avira Professional Security.

- Avira FireWall en AMC

En los sistemas administrados por Avira Management Console, Avira FireWall también está incluido en Avira Professional Security.

- FireWall de Windows

A partir de Windows 7 tiene la opción de gestionar el FireWall de Windows mediante el Centro de control y la configuración.

10.1 Avira FireWall

10.1.1 FireWall

Avira FireWall supervisa y regula el tráfico de datos entrante y saliente de su sistema informático y le protege frente a distintos ataques y amenazas procedentes de Internet: sobre la base de directrices de seguridad se permite o rechaza el tráfico de datos entrante y saliente o la escucha de puertos. Recibirá una notificación en el escritorio si Avira FireWall rechaza las actividades de la red y, por lo tanto, bloquea las conexiones de red. Dispone de las siguientes opciones para configurar Avira FireWall:

Establecer el nivel de seguridad en el Centro de control

En el Centro de control puede configurar el nivel de seguridad. Los niveles de seguridad *Bajo*, *Medio* y *Alto* contienen varias reglas de seguridad cada uno que se complementan y están basadas en filtros de paquete. Estas reglas de seguridad están guardadas como reglas de adaptador predefinidas en la configuración en FireWall > Reglas del adaptador.

Guardar acciones en la ventana Evento de red

Cuando una aplicación intenta establecer por primera vez una conexión de red o de Internet, se abre la ventana emergente *Evento de red*. En la ventana *Evento de red* el usuario puede seleccionar si la actividad de red de la aplicación se permitirá o se rechazará. Si está activada la opción **Guardar acción para esta aplicación** la acción se crea como regla de aplicación y se guarda en la configuración, en **FireWall > Reglas de aplicación**. Al guardar las acciones en la ventana *Evento de red* se obtiene un conjunto de reglas para las actividades de red de las aplicaciones.

Nota
En el caso de aplicaciones de proveedores de confianza, el acceso a la red se permite de forma estándar, a no ser que una regla del adaptador prohíba el acceso a la red. Tiene la posibilidad de quitar proveedores de la lista de proveedores de confianza.

Crear reglas de adaptador y de aplicación en la configuración

En la configuración puede modificar las reglas predefinidas del adaptador o crear nuevas reglas del adaptador. El nivel de seguridad del FireWall se establece automáticamente en el valor *Usuario* cuando se añaden o modifican reglas del adaptador.
Las reglas de aplicación permiten definir reglas de supervisión específicas de aplicaciones:
Unas sencillas reglas de aplicación permiten establecer si se permitirán o rechazarán todas las actividades de red de una aplicación de software, o si se tratarán de manera interactiva por medio de la ventana emergente *Evento de red*.
En la sección *Reglas de aplicación* de la configuración avanzada puede definir distintos filtros de paquete para una aplicación que se ejecutarán como reglas específicas de la aplicación.

10.1.2 Evento de red

En la ventana Evento de red del componente Avira FireWall puede seleccionar si se permite o rechaza el acceso a la red, el envío de datos u otras actividades de red de una aplicación de software: puede permitir o rechazar el tráfico de datos o la escucha de puertos. Es posible que el rechazo de las actividades de red conlleve la cancelación de la conexión.

La ventana Evento de red se abre en los siguientes casos de acceso a la red de las aplicaciones:

- No se creó todavía ninguna regla de aplicación para la aplicación. Es el caso cuando una aplicación establece conexión en la red por primera vez tras la instalación de Avira FireWall. Sin embargo, se excluyen las aplicaciones cuyos fabricantes se clasificaron como de confianza por lo que el acceso a la red de estas se permite automáticamente (consulte el cap. Proveedores de confianza).
- Se creó una regla de aplicación simple para la aplicación con el tipo de acción **Preguntar**.
- Se crearon reglas de aplicación específicas para la aplicación sobre la base de filtros de paquetes en la configuración avanzada, pero no se encontró ninguna regla para el evento de red que tuvo lugar. En ese caso, dispone de la posibilidad de abrir las reglas de aplicación existentes e introducir el acceso a la red como nueva regla usando para ello el botón *Avanzado*.

Evento de red

Información mostrada

Nombre de la aplicación

Nombre de la aplicación

Nombre del fichero

Nombre del fichero ejecutable

Comprobación de firma y recomendación

Resultado de la comprobación de firma y acción recomendada
Si la aplicación está firmada con el certificado de un productor de confianza, se recomienda permitir el tráfico de datos.

Información detallada

Dirección local

Dirección de origen y puerto de origen

Dirección remota

Dirección de destino y puerto de destino

Usuario

Usuario que inició sesión y con el que se ejecuta la aplicación

Id. de proceso

La identificación del proceso asignado a la aplicación

Ruta

Ruta al fichero ejecutable de la aplicación

Empresa

Empresa editora de la aplicación (información de versión)

Versión

Versión de la aplicación

Firmado por

Fabricante de la aplicación (firma)

Acciones y botones

Confiar siempre en este proveedor

Si está activada esta opción, el proveedor del software se añade a la lista de proveedores de confianza tras ejecutar la consulta *Evento de red*. El botón Rechazar se desactiva en cuanto se activa la opción.

> **Nota**
> Esta acción solo está disponible con aplicaciones firmadas.

Guardar acción para esta aplicación

Si está activada esta opción, la acción ejecutada se guarda como regla de aplicación. La regla de aplicación se puede consultar en la configuración, en FireWall > Configuración de ventanas emergentes.

Si la opción *Guardar acción para esta aplicación* está activa y existen reglas de aplicación específicas para la aplicación basadas en filtros de paquete, al pulsar los botones **Permitir** o **Rechazar** se abre la ventana de configuración avanzada de las reglas de aplicación. El tráfico de datos que ha tenido lugar se ha añadido como regla de aplicación específica automáticamente en la primera posición. En la ventana *FireWall > Reglas de aplicación* puede cambiar la posición de la regla de aplicación añadida o quitar esa regla.

Botones	Descripción
Avanzado	Se abre la ventana de configuración avanzada de las reglas de aplicación. **Nota** El botón solo está disponible si se ha activado la configuración avanzada para las reglas de aplicación (consulte Configuración > FireWall > Configuración).
Permitir	Se permite la actividad de red que se produce.
Rechazar	Se rechaza la actividad de red que se produce.
Mostrar/ocultar detalles	Se muestra u oculta la información detallada de la aplicación.

10.2 Firewall de Windows

A partir de Windows 8, Avira FireWall deja de estar incluido en Avira Professional Security. No obstante, tiene la opción de gestionar el Firewall de Windows mediante el Centro de control y la configuración. Para ello, dispone de las siguientes opciones para configurar el Firewall de Windows:

Activar el FireWall de Windows en el Centro de control

Puede activar o desactivar el FireWall de Windows haciendo clic en el botón **CONECTADO/DESCONECTADO** de la opción *FireWall* en **Estado > Seguridad en Internet**.

Comprobar el estado del FireWall de Windows en el Centro de control

Puede comprobar el estado del FireWall de Windows en la sección **SEGURIDAD EN INTERNET > FireWall** y restaurar la configuración recomendada haciendo clic en el botón **Solucionar problema**.

11. Actualizaciones

11.1 Actualizaciones

La validez de un antivirus depende de su grado de actualización, sobre todo en lo que se refiere al archivo de firmas de virus y al motor de análisis. Para poder llevar a cabo las actualizaciones, el producto Avira lleva integrado el componente Updater. Este módulo garantiza que su producto Avira funcione en todo momento con la información más reciente y que esté en disposición de detectar los virus que surgen a diario. El Updater actualiza los siguientes componentes:

- Archivo de firmas de virus:

  El archivo de firmas de virus contiene los patrones de reconocimiento de software malicioso, que consulta su producto Avira durante la búsqueda de virus y malware, así como durante la reparación de los objetos afectados.

- Motor de análisis:

  El motor de análisis contiene los métodos que aplica su producto Avira para buscar virus y malware.

- Archivos de programa (actualización del producto):

  Los paquetes de actualización del producto proporcionan nuevas funciones a cada uno de los componentes del programa.

Durante la ejecución de una actualización, se comprueba la actualidad del archivo de firmas de virus, del motor de análisis y de los ficheros del programa y, en caso necesario, se actualizan. Es posible que deba reiniciar el ordenador después de ejecutar una actualización del producto. Si tan sólo se actualiza el archivo de firmas de virus y el motor de análisis, no es necesario reiniciar el ordenador.

Si fuera necesario reiniciar el ordenador tras una actualización del producto, usted podrá decidir si desea continuar con la actualización o si desea que el ordenador se lo vuelva a recordar más tarde. Si, a pesar de todo, desea continuar con la actualización, podrá decidir cuándo debe reiniciarse el equipo.

Si desea ejecutar la actualización del producto en otro momento, el archivo de firmas de virus y el motor de análisis serán actualizados de todos modos, pero no los ficheros del programa.

Nota
La actualización del producto no concluirá hasta que se haya efectuado un reinicio del equipo.

Nota
Por razones de seguridad, el Updater comprueba si el archivo *hosts* de

Windows de su ordenador ha sido modificado, en concreto si la URL de actualización ha sido manipulada, por ejemplo, por malware, y redirecciona el Updater a páginas de descarga no deseadas. Si el archivo de host de Windows ha sido manipulado, se indicará en el archivo de informe del Updater.

La actualización se ejecuta automáticamente en el siguiente intervalo de tiempo: 60 minutos. La actualización automática se puede modificar o desactivar a través de los ajustes de configuración en (Configuración > Actualización).

En el **Programador** del Centro de control se pueden definir más tareas de actualización, que el Updater ejecutará en los intervalos establecidos. También tiene la opción de iniciar una actualización manualmente:

- En el Centro de control: En el menú **Actualización**, en la sección **Estado**
- A través del menú contextual del icono de bandeja

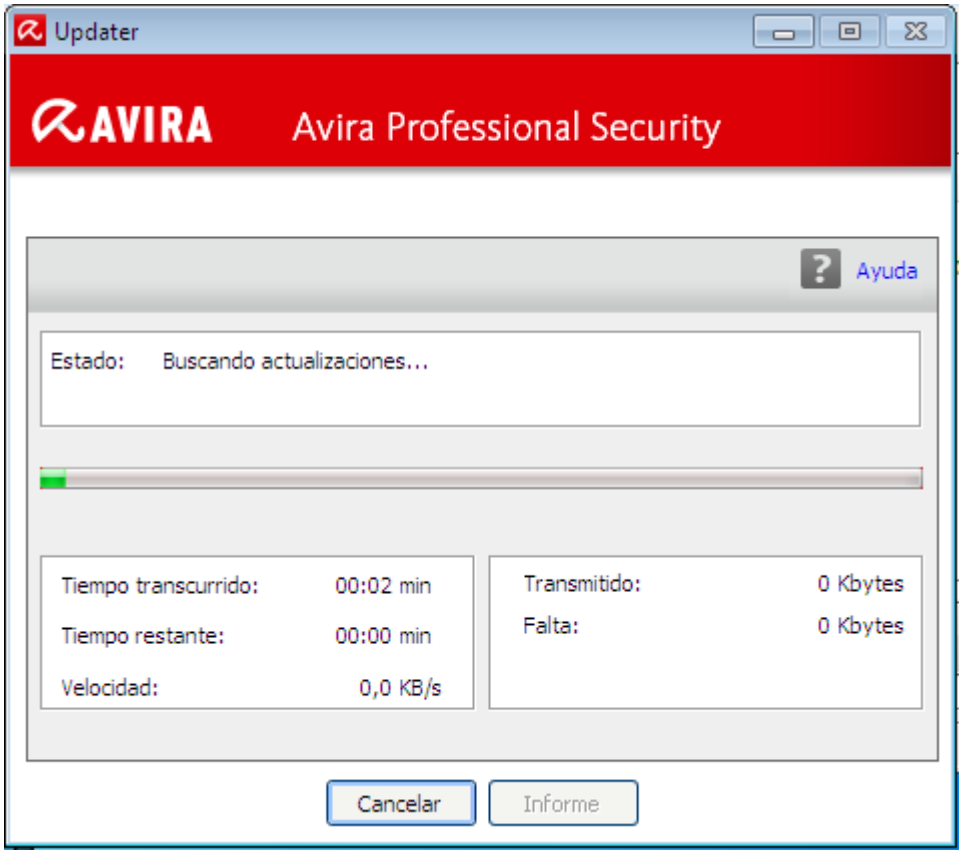
Las actualizaciones se pueden obtener en Internet a través de un servidor web del fabricante o a través de un servidor de ficheros o servidor web de la Intranet, el cual descarga los archivos de actualización de Internet y los pone a disposición del resto de equipos de la red. Esto resulta muy práctico si se desean actualizar productos Avira en varios equipos conectados a una red. Si se utiliza un servidor de descarga en la Intranet, es posible garantizar la validez de los productos Avira instalados en los equipos que deben ser protegidos y, a la vez, hacer un uso eficiente de los recursos. Para instalar en la Intranet un servidor de descarga que funcione adecuadamente, necesita contar con un servidor que ofrezca la estructura de actualización de su producto Avira.

Nota
Se puede utilizar el administrador de actualizaciones de Avira (servidor de archivos o servidor web en Windows) a modo de servidor de archivos o servidor web en la Intranet. El administrador de actualizaciones de Avira espejea el servidor de descargas de los productos Avira y está disponible en el sitio web de Avira:
http://www.avira.es

Si utiliza un servidor web, la descarga se produce mediante protocolo HTTP. Si se utiliza un servidor de archivos, se accede a los archivos de actualización a través de la red. La conexión al servidor web o al servidor de archivos se puede configurar en Configuración > Actualización. En la configuración estándar, se utiliza la conexión a Internet existente como conexión a los servidores web de Avira.

11.2 Updater

Al iniciar una actualización, se abre la ventana de Updater.



Nota
En las tareas de actualización que figuran en el Programador, puede configurar el **Modo de visualización** de la ventana de actualización. Puede elegir entre el modo de visualización **Invisible**, **Minimizado** o **Maximizado**.

Nota
Si utiliza un programa en modo de pantalla completa (p. ej., con juegos) y Updater está en el modo de visualización maximizado o minimizado, Updater cambiará momentáneamente al escritorio. Para evitar esto, tiene la opción de iniciar Updater en el modo de visualización invisible. De esta forma, durante una actualización ya no será informado mediante una ventana de actualización.

Estado: Muestra el comportamiento actual de Updater.

Tiempo transcurrido: Tiempo que ha transcurrido desde que se inició el proceso de descarga.

Tiempo restante: Tiempo que resta para finalizar el proceso de descarga.

Velocidad: Velocidad de descarga de los archivos.

Transmitido: Ficheros ya descargados

Falta: Bytes restantes.

Botones y enlaces

Botón/Enlace	Descripción
	Por medio de este botón o enlace se abre esta página de la ayuda en pantalla.
Reducir	La ventana de Updater se muestra en tamaño pequeño.
Aumentar	La ventana de Updater se muestra en el tamaño original.
Cancelar	Se interrumpe el proceso de actualización. Se cierra Updater.
Finalizar	Ha concluido el proceso de actualización. Se cierra la ventana.
Informe	Se muestra el archivo con el informe de la actualización.

12. Solución de problemas, sugerencias

En este capítulo encontrará indicaciones importantes para la solución de problemas y una serie de recomendaciones que le ayudarán a aprovechar al máximo su producto Avira.

- consulte el capítulo Ayuda en caso de problemas
- consulte el capítulo Comandos de teclado
- consulte el capítulo Centro de seguridad de Windows (para Windows XP) or Centro de actividades de Windows (a partir de Windows 7)

12.1 Ayuda en caso de problemas

Aquí encontrará información sobre las causas y soluciones de potenciales problemas.

- Aparece el mensaje de error *No puede abrirse el fichero de licencia.*.
- Al intentar iniciar una actualización, aparece el mensaje de error *Error de establecimiento de conexión al descargar el fichero...*.
- No es posible mover ni eliminar los virus y el malware.
- El icono de bandeja muestra el estado desactivado.
- El equipo se ralentiza visiblemente cuando se lleva a cabo una copia de seguridad (backup).
- Tan pronto como mi cortafuegos (firewall) está activo, registra los módulos Avira Real-Time Protection y Avira Mail Protection nada más estos se activan
- Avira Mail Protection no funciona.
- No existe ninguna conexión de red disponible en las máquinas virtuales cuando Avira FireWall está instalado en el sistema operativo huésped y se ha definido el nivel de seguridad de Avira FireWall como *Medio* o *Alto*.
- La conexión de red privada virtual (Virtual Private Network, VPN) se bloquea cuando el nivel de seguridad de Avira FireWall se ha definido como *Medio* o *Alto*.
- Mail Protection ha bloqueado un correo electrónico enviado a través de la conexión TLS.
- El chat en Web no funciona: no se muestran los mensajes de chat.

Aparece el mensaje de error *No puede abrirse el fichero de licencia.*.

Causa: El fichero está encriptado.

- Para activar la licencia, no debe abrir el fichero, sino guardarlo en el directorio del programa. Consulte también Administración de licencias.

Al intentar iniciar una actualización, aparece el mensaje de error *Error de establecimiento de conexión al descargar el fichero....*

Causa: Su conexión a Internet no está activa. Por consiguiente, no es posible establecer una conexión con el servidor web de Internet.

- Compruebe si funcionan otros servicios de Internet, como WWW o el correo electrónico. Si no funcionan, restablezca la conexión a Internet.

Causa: El servidor proxy no está accesible.

- Compruebe si se ha cambiado el nombre de usuario para el servidor proxy y, en su caso, reajuste su configuración.

Causa: El fichero *update.exe* no ha podido atravesar su cortafuegos.

- Asegúrese de que el fichero *update.exe* pueda atravesar su cortafuegos.

En caso contrario:

- Compruebe la configuración en Seguridad del PC > Actualización.

No es posible mover ni eliminar los virus y el malware.

Causa: Windows ha cargado el fichero y este se encuentra en estado activo.

- Actualice su producto Avira.
- Si utiliza el sistema operativo Windows XP, desactive la herramienta de restauración del sistema.
- Inicie el equipo en el modo seguro.
- Abra la configuración de su producto Avira .
- Seleccione **Scanner > Análisis**, active en el campo *Ficheros* la opción **Todos los ficheros** y confirme la operación con **Aceptar**.
- Inicie una búsqueda por todas las unidades locales.
- Inicie el equipo en el modo normal.
- Realice una búsqueda en el modo normal.
- Si no se han encontrado más virus o malware, active la herramienta de restauración del sistema, si es que está disponible y se desea utilizar.

El icono de bandeja muestra el estado desactivado.

Causa: Se ha desactivado Avira Real-Time Protection.

- Haga clic en el Centro de control en la opción **Estado** y active en el área *Seguridad del PC* **Real-Time Protection**.

- O BIEN-

- Haga clic con el botón derecho del ratón en el icono de bandeja. Se abrirá el menú contextual. Haga clic en **Activar Real-Time Protection**.

Causa: Avira Real-Time Protection está siendo bloqueado por un cortafuegos.

- Defina en la configuración de su cortafuegos un desbloqueo para Avira Real-Time Protection. Avira Real-Time Protection funciona exclusivamente con la dirección 127.0.0.1 (localhost). No se establece ninguna conexión con Internet. Lo mismo ocurre con Avira Mail Protection.

En caso contrario:

- Compruebe el tipo de inicio del servicio Avira Real-Time Protection. Si fuera necesario, active el servicio: seleccione en la barra de inicio **Inicio > Configuración > Panel de control**. Abra la ventana de configuración **Servicios** haciendo doble clic (en Windows XP encontrará la applet de servicios en la subcarpeta *Administración*). Busque la entrada *Avira Real-Time Protection*. El tipo de inicio debe ser `Automático` y el estado `Iniciado`. Dado el caso, inicie el servicio manualmente marcando la fila correspondiente y el botón **Iniciar**. Si aparece un mensaje de error, compruebe el visor de eventos.

El equipo se ralentiza visiblemente cuando se lleva a cabo una copia de seguridad (backup).

Causa: Durante el proceso de creación de copia de seguridad, Avira Real-Time Protection analiza todos los archivos que intervienen en este proceso.

- Seleccione en la configuración **Real-Time Protection > Análisis > Excepciones** e introduzca el nombre del proceso del software de backup.

Tan pronto como mi cortafuegos (firewall) está activo, registra los módulos Avira Real-Time Protection y Avira Mail Protection.

Causa: La comunicación de Avira Real-Time Protection y Avira Mail Protection se produce a través del protocolo de Internet TCP/IP. Un cortafuegos supervisa todas las conexiones a través de este protocolo.

- Defina un desbloqueo para Avira Real-Time Protection y Avira Mail Protection. Avira Real-Time Protection funciona exclusivamente con la dirección 127.0.0.1 (localhost). No se establece ninguna conexión con Internet. Lo mismo ocurre con Avira Mail Protection.

Avira Mail Protection no funciona.

✓ En el caso de que surjan problemas con Avira Mail Protection, compruebe si este módulo funciona correctamente verificando los siguientes puntos.

Puntos de verificación

✓ Compruebe si su cliente de correo electrónico se conecta con el servidor a través de Kerberos, APOP o RPA. En la actualidad, no se admiten estos métodos de

autenticación.

- ✓ Compruebe si su cliente de correo electrónico se conecta con el servidor a través de SSL (denominado frecuentemente como TLS, Transport Layer Security). Avira Mail Protection no admite SSL y, en consecuencia, cierra las conexiones SSL encriptadas. Si desea utilizar conexiones SSL encriptadas sin la protección de Avira Mail Protection, deberá utilizar un puerto que no esté vigilado por este módulo. Los puertos bajo la supervisión de Mail Protection pueden configurarse en **Mail Protection > Análisis**.
- ✓ ¿El servicio Avira Mail Protection está activo? Si fuera necesario, active este servicio: seleccione en la barra de inicio **Inicio > Configuración > Panel de control**. Abra la ventana de configuración **Servicios** haciendo doble clic (en Windows XP encontrará la applet de servicios en la subcarpeta *Administración*). Busque la entrada *Avira Mail Protection*. El tipo de inicio debe ser `Automático` y el estado `Iniciado`. Dado el caso, inicie el servicio manualmente marcando la fila correspondiente y el botón **Iniciar**. Si aparece un mensaje de error, compruebe el *visor de eventos*. Si este procedimiento no tiene éxito, llegado el caso debería desinstalar por completo el producto Avira desde **Inicio > Configuración > Panel de control > Programas**, reiniciar el equipo y, finalmente, volver a instalar su producto Avira.

General

- Hoy por hoy, las conexiones POP3 encriptadas a través de SSL (Secure Sockets Layer) (denominadas frecuentemente también como TLS [Transport Layer Security]) no pueden protegerse y se ignoran.
- En la actualidad, la autenticación para el servidor de correo electrónico solo se admite mediante contraseña. No existe compatibilidad con "Kerberos" y "RPA".
- Su producto Avira no busca virus ni programas no deseados en los correos electrónicos que se envían.

> **Nota**
> Le recomendamos llevar a cabo actualizaciones de Windows regularmente para evitar posibles lagunas de seguridad.

No existe ninguna conexión de red disponible en las máquinas virtuales cuando Avira FireWall está instalado en el sistema operativo huésped y se ha definido el nivel de seguridad de Avira FireWall como *Medio* o *Alto*.

Si Avira FireWall está instalado en un equipo en el que también se utiliza una máquina virtual (por ejemplo, VMWare, Virtual PC y otras), se bloquearán todas las conexiones de red de la máquina virtual, siempre que el nivel de seguridad de Avira FireWall se haya definido como *Medio* o *Alto*. Si el nivel de seguridad es *Bajo*, FireWall no impedirá las conexiones.

Causa: La máquina virtual emula un adaptador de red mediante software. En esta emulación, los paquetes de datos del sistema invitado se encapsulan en paquetes

especiales (denominados paquetes UDP) y se enrutan de vuelta al sistema huésped a través de la puerta de enlace externa. Avira FireWall, si tiene definido un nivel de seguridad *Medio* o superior, bloquea estos paquetes entrantes.

Para evitar este comportamiento, proceda de la siguiente manera:

- Seleccione en el Centro de control la categoría *SEGURIDAD EN INTERNET* **> FireWall**.
- Haga clic en el vínculo **Configuración**.
- Aparecerá la ventana de diálogo *Configuración*. En ese momento se encontrará en la sección de configuración *Reglas de aplicación*.
- Seleccione la sección de configuración **Reglas del adaptador**.
- Haga clic en **Añadir**.
- Seleccione en *Regla entrante* **UDP**.
- En el área *Nombre de la regla* introduzca un **nombre**.
- Haga clic en **Aceptar**.
- Compruebe si la regla tiene mayor prioridad que la regla **Denegar todos los paquetes IP**.

Advertencia
Esta regla entraña riesgos potenciales, ya que, por definición, permite todos los paquetes UDP. Después de utilizar su máquina virtual, regrese al nivel de seguridad anterior.

La conexión de red privada virtual (Virtual Private Network, VPN) se bloquea cuando el nivel de seguridad de Avira FireWall se ha definido como *Medio* o *Alto*.

Causa: Como norma general no se admiten los paquetes que no coinciden con las reglas predeterminadas. Los paquetes enviados a través del software VPN son filtrados por estas reglas, dado que, debido a su tipo (paquetes GRE), no pertenecen a ninguna otra categoría.

- En **Reglas del adaptador** de la configuración de Avira FireWall añada la regla **Permitir conexiones VPN**, para admitir todos los paquetes asociados a VPN.

Mail Protection ha bloqueado un correo electrónico enviado a través de la conexión TLS.

Causa: Actualmente, Mail Protection no admite Transport Layer Security (TLS: protocolo de cifrado para transferencias de datos en Internet). Dispone de las siguientes opciones para enviar estos correos electrónicos:

- Utilice otro puerto distinto al 25, que es el que utiliza SMTP. De esta forma, evitará la supervisión de Mail Protection.

- Renuncie a la conexión encriptada TLS y desactive el soporte TLS de su cliente de correo electrónico.
- Desactive temporalmente la vigilancia de correos electrónicos salientes por parte de Mail Protection en la configuración en **Mail Protection > Análisis**.

El chat en Web no funciona: no se muestran los mensajes de chat.

Esta circunstancia puede darse en chats basados en el protocolo HTTP con codificación de transferencia fragmentada.

Causa: Web Protection analiza exhaustivamente los datos enviados para comprobar si tienen virus o programas no deseados antes de que se carguen en el navegador web. En una transferencia de datos con codificación de transferencia fragmentada, Web Protection no puede determinar la longitud de los mensajes, es decir, la cantidad de datos.

- En la configuración, marque como excepción la dirección URL del chat en Web (vea la configuración: Web Protection > Búsqueda > Excepciones).

12.2 Comandos de teclado

Los comandos de teclado, denominados también "accesos directos", permiten navegar con rapidez por el programa, abrir los distintos módulos e iniciar determinadas operaciones.

A continuación, le ofrecemos un resumen de los comandos de teclado disponibles. Podrá encontrar indicaciones más detalladas sobre su funcionamiento y disponibilidad en el correspondiente capítulo de la ayuda.

12.2.1 En los cuadros de diálogo

Comando de teclas	Descripción
Ctrl + Tab **Ctrl + AvPág**	Navegación en el Centro de control Cambiar a la siguiente sección.
Ctrl + Mayús + Tab **Ctrl + AvPág**	Navegación en el Centro de control Cambiar a la sección anterior.

←↑→↓	Navegación en las secciones de configuración Seleccione primero con el ratón una sección de configuración. Cambiar entre las opciones de un cuadro de lista desplegable marcado o entre las diversas opciones de un grupo de opciones.
Tabulador	Cambiar a la siguiente opción o al siguiente grupo de opciones.
Mayús + Tab	Cambiar a la opción anterior o al grupo de opciones anterior.
Espacio	Si la opción activa es una casilla de verificación, esta se activa o se desactiva.
Alt + letra subrayada	Escoger opción o ejecutar operación.
Alt + ↓ **F4**	Abrir cuadro de lista desplegable seleccionado.
Esc	Cerrar el campo de lista desplegable seleccionado. Cancelar el comando y cerrar cuadro de diálogo.
Intro	Ejecutar operación de la opción activa o del botón.

12.2.2 En la ayuda

Comando de teclas	Descripción
Alt + Espacio	Mostrar menú del sistema.
Alt + Tab	Cambiar entre la ayuda y otras ventanas abiertas.
Alt + F4	Cerrar la ayuda.
Mayús + F10	Mostrar menús contextuales de la ayuda.

Ctrl + Tab	Cambiar a la siguiente sección en la ventana de navegación.
Ctrl + Mayús + Tab	Cambiar a la sección anterior en la ventana de navegación.
RePág	Cambiar al tema situado arriba del tema actual en la tabla de contenidos, en el índice o en la lista de resultados de búsqueda.
AvPág	Cambiar al tema situado debajo del tema actual en la tabla de contenidos, en el índice o en la lista de resultados de búsqueda.
RePág **AvPág**	Navegar por un tema.

12.2.3 En el Centro de control

General

Comando de teclas	Descripción
F1	Mostrar ayuda
Alt + F4	Cerrar el Centro de control
F5	Actualizar la vista
F8	Abrir la configuración
F9	Iniciar actualización

Sección **Scanner**

Comando de teclas	Descripción
F2	Renombrar perfil seleccionado
F3	Iniciar búsqueda con el perfil seleccionado
F4	Crear vínculo en el escritorio para el perfil seleccionado
Insert	Crear perfil nuevo
Supr	Eliminar perfil seleccionado

Sección **FireWall**

Comando de teclas	Descripción
Entrar	Propiedades

Sección **Cuarentena**

Comando de teclas	Descripción
F2	Volver a comprobar objeto
F3	Restablecer objeto
F4	Enviar objeto
F6	Restablecer objeto en...
Entrar	Propiedades
Insert	Añadir fichero

Supr	Eliminar objeto

Sección **Programador**

Comando de teclas	Descripción
F2	Modificar tarea
Entrar	Propiedades
Insert	Insertar nueva tarea
Supr	Eliminar tarea

Sección **Informes**

Comando de teclas	Descripción
F3	Mostrar fichero de informe
F4	Imprimir fichero de informes
Entrar	Mostrar informe
Supr	Eliminar informe o informes

Sección **Eventos**

Comando de teclas	Descripción
F3	Exportar evento o eventos
Entrar	Mostrar evento

Supr	Eliminar evento o eventos

12.3 Solución de problemas, sugerencias > Centro de seguridad de Windows

- desde Windows XP Service Pack 2 -

12.3.1 General

El Centro de seguridad de Windows comprueba el estado de un equipo desde el punto de vista de la seguridad.

Si en alguno de estos importantes aspectos se detecta un problema (p. ej., un antivirus desactualizado), el Centro de seguridad envía un mensaje de advertencia y formula recomendaciones para proteger mejor su ordenador.

12.3.2 El Centro de seguridad de Windows y su producto Avira

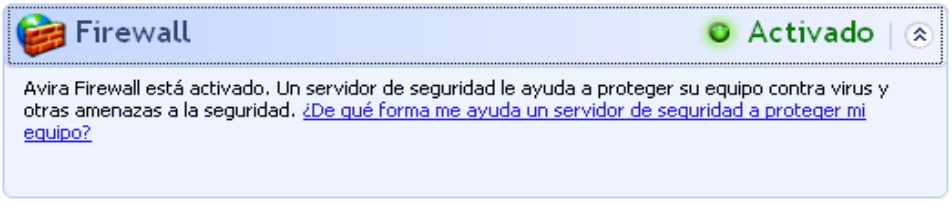
FireWall

Es posible que en el Centro de seguridad encuentre la siguiente información relativa al firewall:

- Firewall ACTIVO/Firewall activado
- Firewall INACTIVO/Firewall desactivado

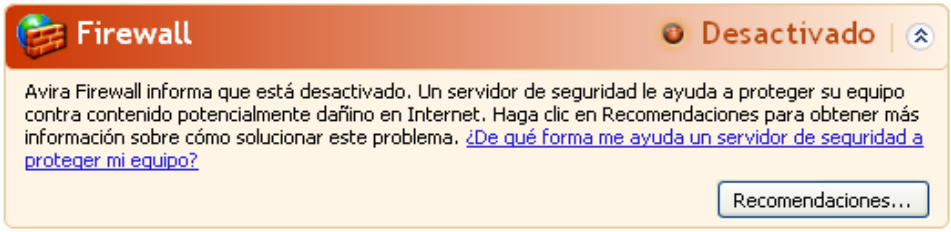
Firewall ACTIVO/Firewall activado

Tras instalar su producto Avira y desconectar el Firewall de Windows, recibirá el siguiente mensaje:



Firewall INACTIVO/Firewall desactivado

Si desactiva Avira FireWall, recibirá la siguiente notificación:



Nota
Puede activar o desactivar Avira FireWall a través del Estado en el Centro de control.

Advertencia
Si desactiva el Avira FireWall, su equipo dejará de estar protegido ante accesos no autorizados a través de la red o de Internet.

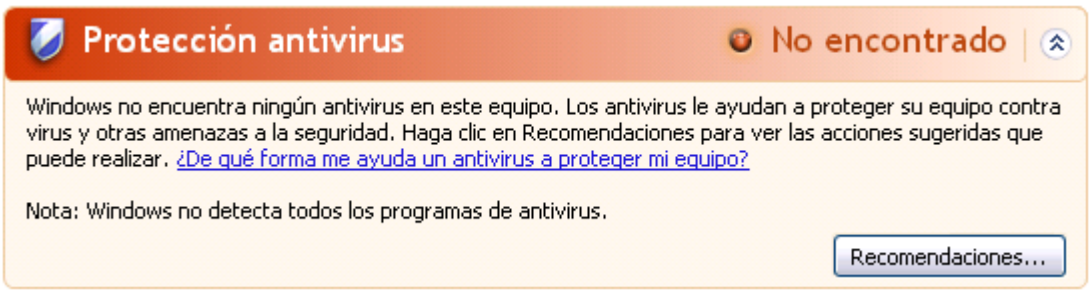
Software de protección/Protección contra software malicioso

Puede recibir los siguientes avisos del Centro de seguridad de Windows relativos a la protección antivirus:

- Protección Antivirus NO ENCONTRADA
- Protección Antivirus NO ACTUAL
- Protección Antivirus ACTIVA
- Protección Antivirus INACTIVA
- Protección Antivirus NO MONITORIZADA

Protección Antivirus NO ENCONTRADA

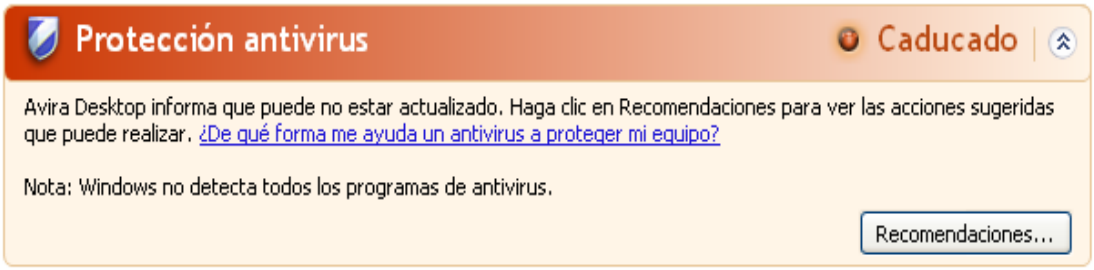
Este mensaje del Centro de seguridad de Windows aparece si no se ha encontrado ningún antivirus en el equipo.



Nota
Instale su producto Avira en el equipo para protegerlo de virus y otros programas no deseados.

Protección Antivirus NO ACTUAL

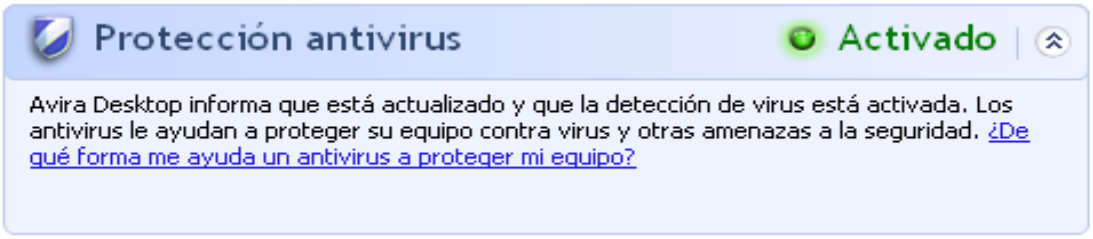
Si tiene instalado Windows XP Service Pack 2 y posteriormente instala su producto Avira, o bien si instala Windows XP Service Pack 2 en un sistema en el que ya esté instalado su producto Avira, recibirá el siguiente mensaje:



Nota
Para que el Centro de seguridad de Windows reconozca su producto Avira como actualizado, es imprescindible que lleve a cabo una actualización tras la instalación. Su sistema se actualizará si ejecuta una actualización.

Protección Antivirus ACTIVA

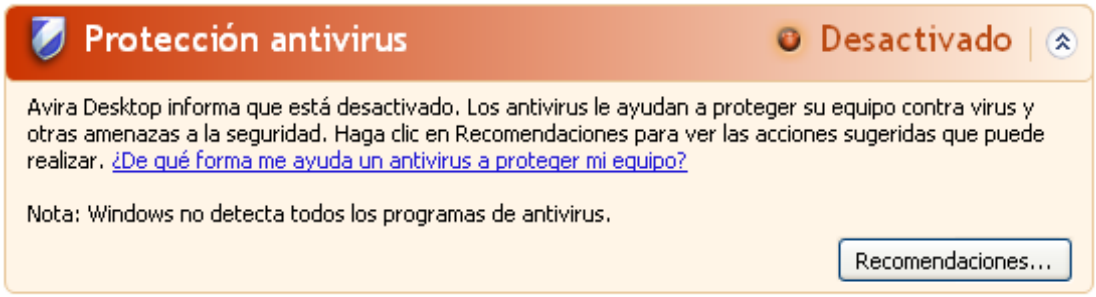
Tras instalar su producto Avira y actualizarlo a continuación, recibirá el siguiente mensaje:



Su producto Avira está actualizado y Avira Real-Time Protection está activo.

Protección Antivirus INACTIVA

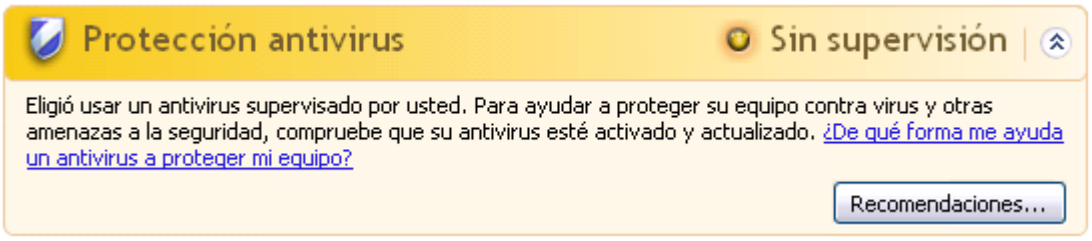
Recibirá el siguiente mensaje si desactiva Avira Real-Time Protection o si interrumpe el servicio Avira Real-Time Protection.



Nota
Puede activar o desactivar Avira Real-Time Protection en la sección Estado del **Centro de control**. Además, puede ver fácilmente si Avira Real-Time Protection está activo comprobando que el paraguas rojo de su barra de tareas esté abierto.

Protección Antivirus NO MONITORIZADA

Si recibe el siguiente mensaje del Centro de seguridad de Windows, significa que ha decidido monitorizar su software antivirus por sí mismo.



Nota
Su producto Avira es compatible con el Centro de seguridad de Windows. Puede activar esta opción siempre que lo desee con el botón **Recomendaciones...**.

Nota
Aún en el caso de que haya instalado Windows XP Service Pack 2, necesita una solución antivirus adicional. Aunque Windows monitoriza su software antivirus, no posee funciones antivirus propias de ningún tipo. En consecuencia, sin una solución antivirus adicional, no estaría protegido contra virus y otros tipos de malware.

12.4 Centro de actividades de Windows

- Windows 7 y Windows 8 -

12.4.1 General

> **Nota:**
> A partir de Windows 7, el **Centro de seguridad de Windows** será llamado **Centro de actividades de Windows**. En este apartado del programa podrá encontrar el estado de todas las opciones de seguridad.

El Centro de actividades de Windows comprueba el estado de un equipo desde el punto de vista de la seguridad. Se puede acceder directamente al Centro de actividades haciendo clic en la pequeña bandera que aparece en su barra de tareas o a través de **Panel de control > Centro de actividades**.

Si se detecta un problema en alguno de estos importantes aspectos (p. ej., un antivirus no actualizado), el Centro de actividades envía un mensaje de advertencia y ofrece recomendaciones para proteger mejor su equipo. Esto significa que, si todo funciona correctamente, no recibirá ninguna notificación del Centro de actividades. No obstante, se puede consultar el estado de seguridad del equipo en el **Centro de actividades**, en la sección **Seguridad**.
También tiene la opción de administrar y seleccionar los programas que ha instalado (p. ej. *Mostrar los programas contra spyware que hay en el equipo*).

Los mensajes de advertencia se pueden desactivar en **Centro de actividades > Modificar configuración** (p. ej. *Desactivar los mensajes de protección contra spyware y malware similar*).

12.4.2 El Centro de actividades de Windows y su producto Avira

Firewall de red

Es posible que en el Centro de actividades encuentre la siguiente información relativa al firewall:

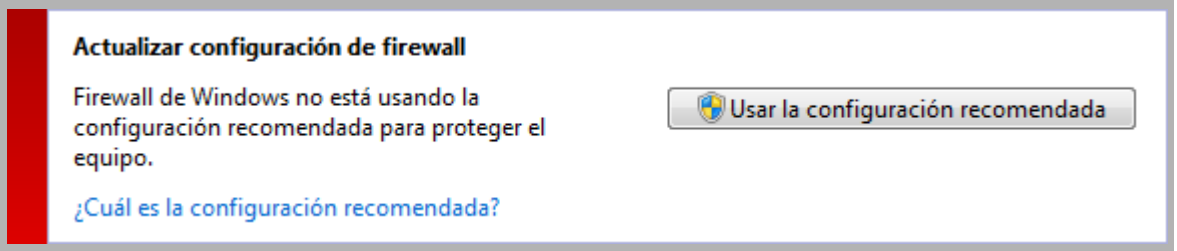
- Avira FireWall indica que está activado
- Firewall de Windows y Avira FireWall están ambos desactivados
- Windows Firewall está desactivado o configurado de manera incorrecta

Avira FireWall indica que está activado

Tras instalar su producto Avira y desactivar el Firewall de Windows, recibirá el siguiente mensaje en **Centro de actividades > Seguridad > Firewall de red**: *Avira FireWall indica que está activado*. Esto significa que Avira FireWall es la solución de cortafuegos

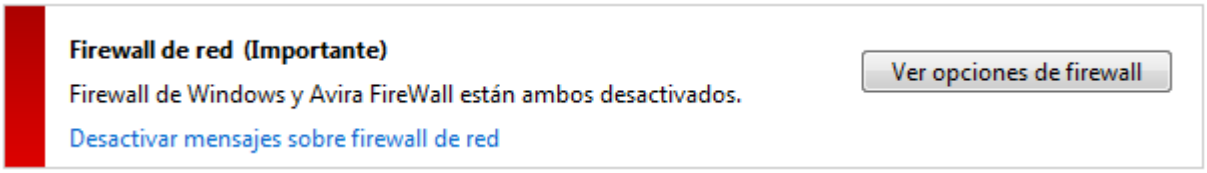
seleccionada (es importante distinguir entre el Firewall de Windows y el FireWall de Avira).

Advertencia
Cuando se habla del **Firewall de Windows no** se está haciendo referencia a su **Avira FireWall**. Por ello, no debería preocuparse en el caso de que recibiera los siguientes mensajes: *Actualizar la configuración del Firewall* o ***Firewall de Windows no está usando la configuración recomendada para proteger el equipo.*** **Su producto Avira funciona correctamente y su equipo está seguro**. Windows sólo le informa de que los programas de Windows están desactivados.



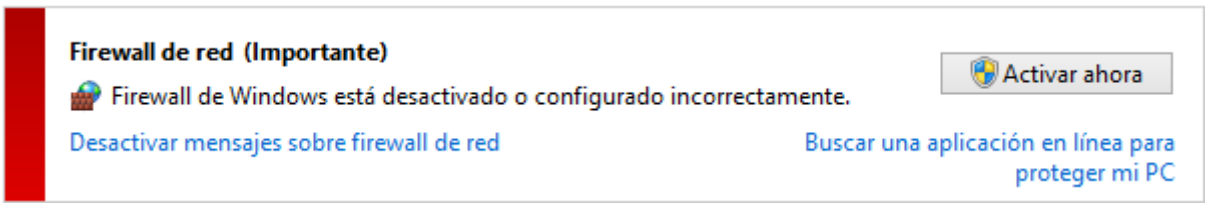
Firewall de Windows y Avira FireWall están ambos desactivados

Si desactiva Avira FireWall, recibirá la siguiente notificación:



Advertencia
Si desactiva el **Avira FireWall**, su equipo dejará de estar protegido ante accesos no autorizados a través de la red o de Internet.

Firewall de Windows está desactivado o configurado de manera incorrecta



Esto significa que no está activado ni **Firewall de Windows** ni **Avira FireWall**. Este mensaje se recibe en dos situaciones diferentes:

- **Avira FireWall**

Avira FireWall está desactivado o configurado de manera incorrecta. Avira FireWall debería ser reconocido automáticamente por el Centro de actividades. Debe reiniciar el equipo. Si el problema persiste, instale nuevamente el producto Avira.

- **FireWall de Windows**

A partir de Windows 7, Avira Professional Security tiene la opción de gestionar el Firewall de Windows mediante el Centro de control y la configuración.

Protección antivirus

El Centro de actividades de Windows le ofrece las siguientes indicaciones relativas a la protección antivirus:

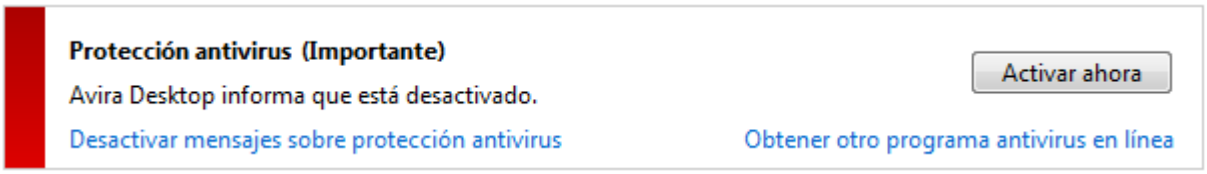
- Avira Desktop indica que está actualizado y que la detección de virus está activada
- Avira Desktop está desactivado
- Avira Desktop no actualizado
- Windows no encontró ningún software antivirus en este equipo
- Avira Desktop dejó de proteger el equipo

Avira Desktop informa que está actualizado y que la detección de virus está activada

Tras instalar su producto Avira y actualizarlo a continuación, en principio no debería recibir mensajes del Centro de actividades de Windows. No obstante, en **Centro de actividades > Seguridad** , podrá encontrar la siguiente indicación: *"Avira Desktop" indica que está actualizado y que la detección de virus está activada*. Esto significa que ahora su producto Avira está actualizado y que Real-Time Protection está activo.

Avira Desktop está desactivado

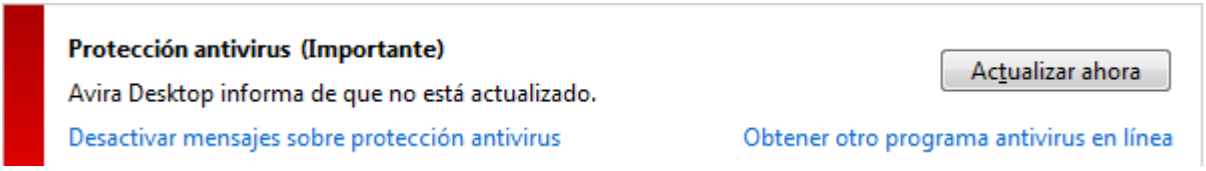
Recibirá el siguiente mensaje si desactiva Avira Real-Time Protection o si interrumpe el servicio Real-Time Protection.



Nota
Puede activar o desactivar **Avira Real-Time Protection** en la sección **Estado** del **Centro de control de Avira**. Además, puede ver fácilmente si **Avira Real-Time Protection** está activo comprobando que el paraguas rojo de su barra de tareas esté abierto. También se puede activar cada uno de los componentes de Avira haciendo clic en la tecla *Activar ahora* del Centro de actividades. Si recibiera un mensaje de confirmación, haga clic en *Permitir* y Real-Time Protection se activará.

Avira Desktop no actualizado

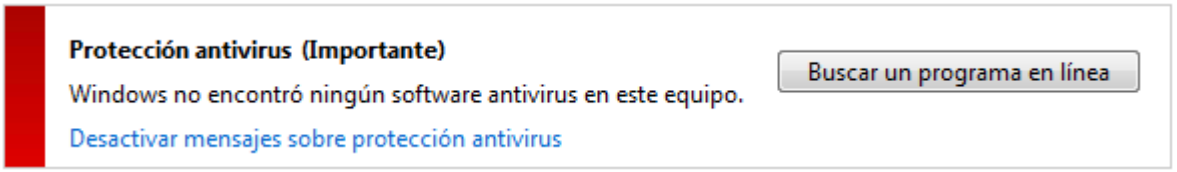
Recibirá el siguiente mensaje si acaba de instalar Avira y si por cualquier motivo el archivo de firmas de virus, el motor de análisis o los ficheros del programa de su producto Avira no se actualizaran automáticamente (p. ej., si actualiza una versión antigua de un sistema operativo de Windows, en el que ya se encuentra instalado su producto Avira, con una versión más moderna):



Nota
Para que el Centro de actividades de Windows reconozca su producto Avira como actualizado, es imprescindible que lleve a cabo una actualización tras la instalación. Su sistema se actualizará si ejecuta una actualización.

Windows no encontró ningún software antivirus en este equipo

Este mensaje del Centro de actividades de Windows aparece si el Centro de actividades de Windows no ha encontrado ningún antivirus en el equipo.

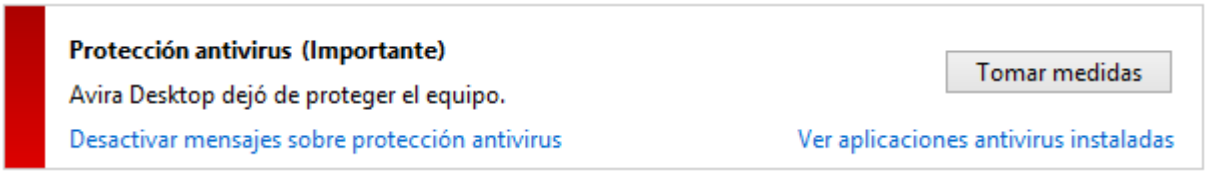


Nota
Tenga en cuenta que esta opción no se encuentra disponible en Windows 8. A partir de este sistema operativo, Windows Defender lleva a cabo la función de protección antivirus preestablecida de Microsoft.

Nota
Instale su producto Avira en el equipo para protegerlo de virus y otros programas no deseados.

Avira Desktop dejó de proteger el equipo

Esta indicación del Centro de actividades de Windows aparece si la licencia de su producto Avira ha caducado.
Si hace clic en el botón **Tomar medidas**, accederá a la página web de Avira, donde podrá adquirir una nueva licencia.



Nota
Tenga en cuenta que esta opción sólo se encuentra disponible para Windows 8.

Protección contra spyware y software no deseado

El Centro de actividades de Windows le enviará los siguientes avisos relativos a la protección contra spyware y software no deseado:

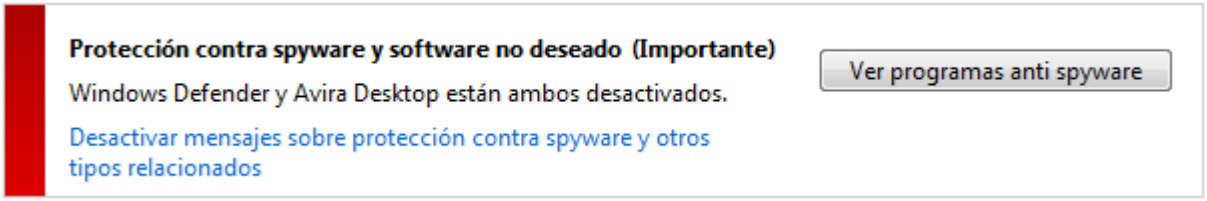
- Avira Desktop indica que está activado
- Tanto Windows Defender como Avira Desktop indican que están desactivados
- Avira Desktop no actualizado
- Windows Defender no está actualizado
- Windows Defender está desactivado

Avira Desktop indica que está activado

Tras instalar su producto Avira y actualizarlo a continuación, en principio no debería recibir mensajes del Centro de actividades de Windows. No obstante, en **Centro de actividades > Seguridad**, podrá encontrar la siguiente notificación: *"Avira Desktop" indica que está activado*. Esto significa que su producto Avira está actualizado y que Real-Time Protection está activo.

Tanto Windows Defender como Avira Desktop indican que están desactivados

Recibirá el siguiente mensaje si desactiva Avira Real-Time Protection o si interrumpe el servicio Avira Real-Time Protection.

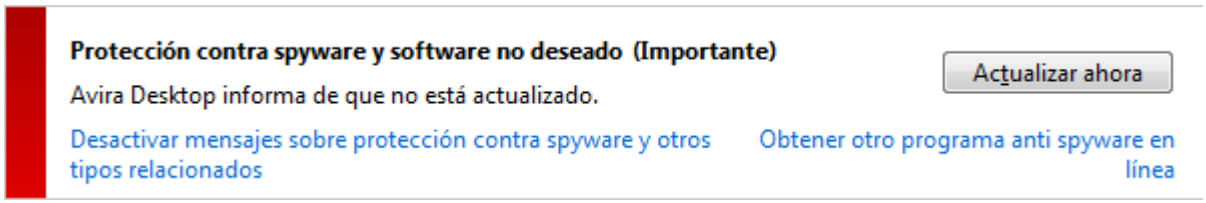


Nota
Puede activar o desactivar **Avira Real-Time Protection** en la sección **Estado** del **Centro de control de Avira**. Además, puede ver fácilmente si **Avira Real-Time Protection** está activo comprobando que el paraguas rojo de su barra de

tareas esté abierto. También se puede activar cada uno de los componentes de Avira haciendo clic en la tecla *Activar ahora* del Centro de actividades. Si recibiera un mensaje de confirmación, haga clic en *Permitir* y Real-Time Protection se activará.

Avira Desktop no actualizado

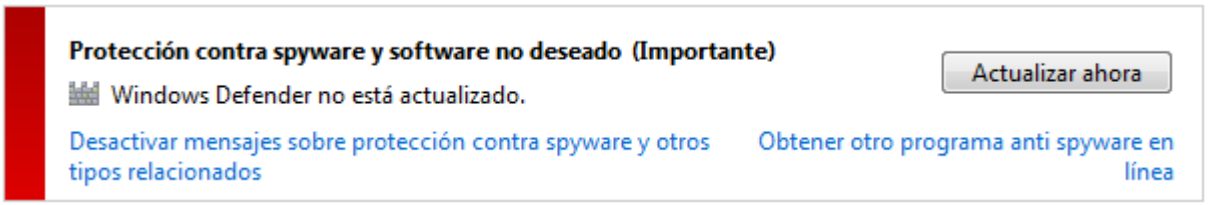
Recibirá el siguiente mensaje si acaba de instalar Avira o si por cualquier motivo el archivo de firmas de virus, el motor de análisis o los ficheros del programa de su producto Avira no se actualizaran automáticamente (p. ej., si actualiza una versión antigua de un sistema operativo de Windows, en el que ya se encuentra instalado su producto Avira, con una versión más moderna):



Nota
Para que el Centro de actividades de Windows reconozca su producto Avira como actualizado, es imprescindible que lleve a cabo una actualización tras la instalación. Su sistema se actualizará si ejecuta una actualización.

Windows Defender no está actualizado

El siguiente mensaje puede aparecer si Windows Defender está activado. Esto podría significar que su producto Avira no se ha instalado correctamente. Compruebe esta posibilidad.

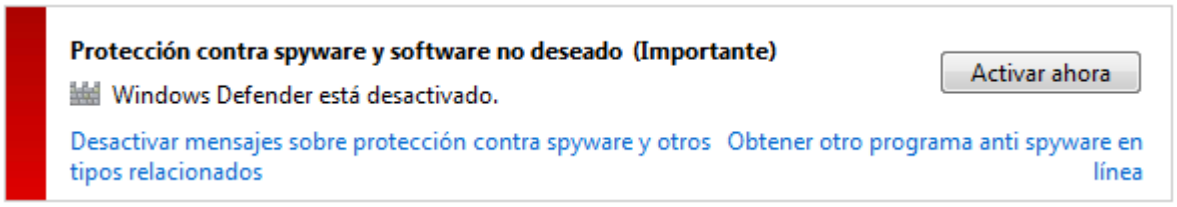


Nota
Windows Defender es la solución antivirus y contra spyware predefinida de Windows.

Windows Defender está desactivado

Recibirá del Centro de actividades de Windows el mensaje *Windows Defender está desactivado* si no se encuentra ningún otro software contra spyware en su equipo.

Windows Defender es uno de los software de Microsoft que están integrados de manera estándar en el sistema operativo y que se utiliza para la detección de spyware. Si ha instalado otro antivirus en el equipo, esta aplicación se habrá desactivado.
Si el producto Avira se ha instalado correctamente, no debería recibir este mensaje, ya que el Centro de actividades reconoce Avira automáticamente. Compruebe que Avira funcione correctamente.



13. Virus y más

Avira Professional Security no solo es capaz de detectar virus y malware, sino que también puede protegerle de otros peligros. En este En este capítulo encontrará un resumen de los distintos tipos de virus y malware, así como de otros riesgos. Se describe tanto su origen y comportamiento, como las desagradables sorpresas a las que se expone quien ha de sufrirlos.

Temas relacionados:

- Categorías de riesgos
- Virus y otros malware

13.1 Categorías de riesgos

Adware

Se denomina Adware al software que, además de ofrecer sus funciones principales, muestra al usuario anuncios en banners o elementos emergentes (popups). Normalmente, estas inserciones de publicidad no pueden desactivarse y casi siempre son visibles. En este tipo de software, los datos de conexión permiten extraer muchas conclusiones acerca de su uso. Por razones de protección de datos, estos programas son problemáticos.

Su producto Avira es capaz de detectar Adware. Si en la configuración, en Categorías de riesgos, se activa la opción **Adware**, cada vez que su producto Avira detecte este tipo de software, aparecerá el correspondiente mensaje de advertencia.

Adware/spyware

Se trata de software que muestra anuncios publicitarios o de programas que envían datos personales del usuario a terceros, con frecuencia sin su conocimiento ni consentimiento, y que, por ello, probablemente no son deseados.

Su producto Avira es capaz de detectar Adware/Spyware. Si en la configuración, en Categorías de riesgos, se activa la opción **Adware/Spyware** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia.

Aplicación

Bajo la denominación de "aplicación", se incluyen aquellos programas cuyo uso puede estar asociado a algún tipo de riesgo o cuyo origen sea sospechoso.
Su producto Avira es capaz de detectar la categoría "aplicación" (APPL). Si en la configuración, en Categorías de riesgos, se activa la opción **Aplicación** con una marca de

verificación, cada vez que su producto Avira reconozca un comportamiento de este tipo, recibirá la correspondiente advertencia.

Software control backdoor

Para robar datos o manipular el equipo, se introducen programas servidores por la puerta trasera (backdoor) sin que el usuario sea consciente de ello. Un tercero puede controlar este programa mediante un software de control de puerta trasera (cliente) a través de Internet o de una red.
Su producto Avira es capaz de detectar el software de control de puerta trasera. Si en la configuración, en Categorías de riesgos, se activa la opción **Software de control de puerta trasera** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia.

Ficheros con extensión oculta

Se trata de archivos ejecutables que ocultan de manera sospechosa las extensiones reales de sus archivos. Esta forma de ocultamiento se utiliza con mucha frecuencia en malware.
Su producto Avira es capaz de detectar archivos con extensión oculta. Si en la configuración, en Categorías de riesgos, se activa la opción **Archivos con extensiones ocultas** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia.

Programa de marcación con coste

Existen determinados servicios que se ofertan en Internet que exigen un pago. En Alemania, el cálculo de este coste se lleva a cabo a través de programas de marcación telefónica con números 0190/0900 (en Austria y Suiza, con números 09x0; en Alemania se cambiará a medio plazo al sistema 09x0). Instalados en el equipo, estos programas (en inglés, dialers) garantizan el establecimiento de una conexión a través del correspondiente número de tarificación adicional, cuyas tarifas abarcan una gama muy amplia.

La comercialización de contenidos en línea a través del teléfono es una práctica legal que puede ser beneficiosa para el usuario. Por esa razón, los programas serios de marcación con coste en ningún momento hacen sospechar que no estén siendo usados por el cliente de manera consciente y cuidadosa. Únicamente se instalan en el equipo del usuario cuando este ha dado su consentimiento, el cual debe ser el resultado de un requerimiento reconocible como tal y absolutamente claro e inconfundible. El establecimiento de la conexión mediante los programas de marcación serios se muestra de manera inequívoca. Además, los programas de marcación serios informan de manera exacta y transparente sobre el importe total de los gastos generados.

Lamentablemente, existen programas de marcación que se instalan en equipos de manera disimulada, sospechosa o directamente con intención fraudulenta. Por ejemplo: modifican la conexión de transmisión de datos estándar del usuario de Internet al proveedor de servicios de Internet (ISP), y en cada conexión llaman a un número de teléfono 0190/0900 con coste asociado que, con frecuencia, aplica tarifas

extraordinariamente elevadas. Ocurre a veces que el usuario afectado no se da cuenta hasta que le llega la siguiente factura de teléfono de que un programa de marcación no deseado que llama a números 0190/0900 y que se ha instalado en su equipo ha seleccionado un número de tarificación adicional en todas y cada una de sus conexiones a Internet, lo que implica tarifas mucho mayores.

Como norma general, para protegerse de estos programas no deseados de marcación con coste (números 0190/0900) le recomendamos que se dirija a su proveedor de telefonía y le solicite restringir las llamadas a estos números.

Su producto Avira detecta de manera predeterminada los programas de marcación con coste que conozca.

Si en la configuración, en Categorías de riesgos, se activa la opción **Programa de marcación con coste** con una marca de verificación, cuando se detecte este tipo de programas se recibirá la correspondiente advertencia. A continuación, podrá eliminar el posible programa de marcación no deseado a números 0190/0900. No obstante, si el programa encontrado sí fuera deseado, puede definirlo como archivo de excepción, de modo que en el futuro no volverá a inspeccionarse.

Suplantación de identidad (Phishing)

La suplantación de identidad (phishing, también conocida como "brand spoofing") constituye una forma sofisticada de robo de datos dirigido a clientes actuales o potenciales de proveedores de servicios de Internet, bancos, servicios de banca en línea y la administración pública.
Al facilitar el correo electrónico en Internet, rellenar formularios en línea, acceder a grupos de noticias o sitios web, puede ocurrir que sus datos sean sustraídos por los denominados "Internet crawling spiders" (rastreadores de Internet) y utilizados sin su consentimiento para cometer un fraude o cualquier otro acto delictivo.

Su producto Avira es capaz de detectar el phishing. Si en la configuración, en Categorías de riesgos, se activa la opción **Suplantación de identidad (phishing)** con una marca de verificación, cada vez que su producto Avira reconozca un comportamiento de este tipo, recibirá la correspondiente advertencia.

Programas que dañan la esfera privada

Se trata de software que tiene la capacidad de mermar la seguridad de su sistema, provocar la ejecución de programas no deseados, dañar su esfera privada o espiar su comportamiento y que, por ello, posiblemente no es deseado.

Su producto Avira es capaz de detectar programas que dañan la esfera privada. Si en la configuración, en Categorías de riesgos, se activa la opción **Programas que dañan la esfera privada** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia.

Programas broma

Los programas de broma tan solo tienen el objetivo de asustar o simplemente poner un toque de humor, pero no son dañinos ni se multiplican. La mayoría de las veces, cuando el programa de broma se activa, el ordenador empieza a reproducir una melodía o muestra alguna imagen llamativa sobre la pantalla. Algunos ejemplos de programas de broma son la lavadora en la unidad de disco (DRAIN.COM) y el comepantallas (BUGSRES.COM).

Sin embargo, hay que tener cuidado: los síntomas de programas de broma también pueden tener su origen en virus o troyanos. En el mejor de los casos, el usuario se lleva un buen susto, aunque podría ocurrir que, movidos por el pánico, nos infringiéramos daños a nosotros mismos.

Mediante la ampliación de sus rutinas de identificación y búsqueda, el producto Avira es capaz de detectar programas de broma y, si fuera necesario, los eliminaría como programas no deseados. Si en la configuración, en Categorías de riesgos, se activa la opción **Programas broma** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia.

Juegos

A todo el mundo le gustan los juegos, pero eso no significa que se deba jugar en el entorno de trabajo (a excepción, quizá, de la hora del almuerzo). Sin embargo, muchos empleados dedican parte de su tiempo de trabajo en la empresa a disparar a zombis o jugar al póker. A través de Internet se puede descargar un número enorme de juegos. Los juegos a través del correo electrónico gozan de una popularidad cada vez mayor, desde una simple partida de ajedrez, hasta auténticas maniobras navales (con lanzamientos de torpedo incluidos). Existen numerosas variantes de todo tipo, en las que los participantes se van mandando alternativamente las respectivas jugadas por correo electrónico.

Los estudios indican que el tiempo de trabajo dedicado a jugar al ordenador ha alcanzado ya desde hace tiempo magnitudes económicamente relevantes. Por ello, resulta lógico que cada vez más empresas se estén planteando mantener los juegos alejados de los equipos de trabajo.

Su producto Avira es capaz de detectar juegos de ordenador. Si en la configuración, en Categorías de riesgos, se activa la opción **Juegos** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia. En ese caso, puede terminar el juego definitivamente simplemente borrándolo.

Software engañoso

Conocidos también como "scareware" (programas de susto) o "rogueware" (programas de bribones), se trata de software engañoso que hace creer que se está sufriendo la infección de virus u otro riesgo similar, lo que hace pensar al usuario que está tratando con un antivirus profesional. El scareware se instala para crear inseguridad al usuario o para asustarlo. Si la víctima cae en la trampa y se cree amenazado, con frecuencia se le

ofrece eliminar el falso riesgo a cambio de una cierta cantidad de dinero. En otros casos, la víctima, creyendo ser el objetivo de un ataque, lleva a cabo una serie de acciones que a la postre posibilitarán un ataque real.

Si en la configuración, en Categorías de riesgos, se activa la opción **Software engañoso** con una marca de verificación, cuando se detecte este tipo de programas se recibirá la correspondiente advertencia.

Utilidades de compresión poco habituales

Se trata de archivos que han sido comprimidos con un compresor poco habitual y que, por ello, pueden ser clasificados como sospechosos.

Su producto Avira es capaz de detectar utilidades de compresión poco habituales. Si en la configuración, en Categorías de riesgos, se activa la opción **Utilidades de compresión poco habituales** con una marca de verificación, cada vez que su producto Avira encuentre este tipo de programas, recibirá la correspondiente advertencia.

13.2 Virus y otros malware

Adware

Se denomina "adware" al software que, además de ofrecer al usuario su funcionalidad característica, muestra banners y ventanas emergentes (popups) de publicidad. Normalmente, estas inserciones publicitarias no pueden desactivarse y casi siempre son visibles. Los datos de conexión ya permiten extraer múltiples conclusiones sobre los hábitos de uso del usuario, de modo que, por razones de protección de datos, estos programas son problemáticos.

Puertas traseras

El software de puerta trasera (backdoor) puede sortear las medidas de control de acceso de un equipo y lograr introducirse en el mismo.

El programa del atacante se ejecuta de manera oculta y permite obtener derechos prácticamente ilimitados. Gracias al software de puerta trasera, es posible espiar los datos personales del usuario. No obstante, estos programas se utilizan sobre todo para instalar otros virus o gusanos en el sistema afectado.

Virus de arranque

El sector de arranque (o el sector de arranque maestro) de los discos duros es uno de los objetivos preferidos de los virus de arranque. Estos borran datos de relevancia para la secuencia de inicio del sistema. Una de las consecuencias más desagradables es que el sistema operativo no puede cargarse.

Red de robots (bot-net)

El concepto "red de robots" hace referencia a una red de ordenadores en Internet controlada de manera remota y compuesta por robots intercomunicados. El control remoto se lleva a cabo mediante virus o troyanos que infectan el PC y que, posteriormente, permanecen inactivos a la espera de instrucciones, sin causar daños en el equipo infectado. Estas redes pueden utilizarse para distribuir spam, realizar ataques distribuidos de denegación de servicio (DDoS) y otras acciones. Todo ello, sin que los usuarios de los equipos afectados puedan percatarse de nada.La virtud de las redes de robots consiste en que sus redes pueden abarcar potencialmente a miles de ordenadores, obteniendo un ancho de banda total que supera ampliamente la capacidad de la mayoría de los accesos a Internet convencionales.

Vulnerabilidad de seguridad (exploit)

Las vulnerabilidades de seguridad son programas o scripts que aprovechan las debilidades o errores de funcionamiento de un sistema operativo o una aplicación informática. Una forma de estas vulnerabilidades son los ataques que tienen su origen en Internet y que, gracias a paquetes de datos manipulados, sacan partido a las lagunas de seguridad del software de red. A través de estos agujeros de seguridad pueden infiltrarse programas que permitan obtener una mayor capacidad de acceso.

Hoaxes (del inglés "hoax": broma, trastada, diablura)

Desde hace unos años, los usuarios de Internet y de otro tipo de redes no dejan de recibir advertencias sobre virus que, al parecer, se propagan a través del correo electrónico. Estas advertencias van acompañadas de peticiones para reenviar los correos electrónicos al mayor número posible de amigos o usuarios con el fin de prevenirlos de este peligro.

Honeypot

Un honeypot (literalmente, bote de miel) es un servicio (programa o servidor) instalado en una red. Este servicio tiene la función de vigilar la red y registrar los ataques que esta experimente. Su existencia es desconocida para el usuario, quien, por esa razón, no puede intervenir de ningún modo. Cuando aparezca un atacante buscando lagunas de seguridad en una red y empiece a utilizar los servicios que le presta el honeypot, será registrado y se disparará una alarma.

Virus de macros

Los virus de macros son pequeños programas escritos en el lenguaje de macros de una aplicación (p. ej., WordBasic en WinWord 6.0) que, normalmente, se propagan únicamente a través de los documentos de dicha aplicación. Por ello se denominan también virus de documentos. Están diseñados para activarse cuando se inicia la aplicación correspondiente y se ejecuta la macro infectada. A diferencia de los virus

convencionales, los virus de macros no infectan archivos ejecutables, sino documentos de la aplicación huésped.

Pharming

El pharming implica la manipulación del archivo huésped de los navegadores web con objeto de redireccionar determinadas consultas hacia falsas páginas Web. Se trata de una evolución de la clásica suplantación de identidad (phishing). Los estafadores que hacen uso del pharming mantienen un gran número de "granjas" de servidores que alojan los falsos sitios web. El pharming se ha convertido en la categoría general de distintas clases de ataques de DNS. Mediante la manipulación de un archivo huésped, y gracias a la ayuda de un troyano o un virus, se puede manipular selectivamente el sistema. El resultado es que dicho sistema tan solo podrá conectar con falsos sitios web, aún en el caso de que se escriba correctamente la dirección Web.

Suplantación de identidad (phishing)

En español, "phishing" podría traducirse como la pesca de datos personales de un usuario de Internet. El atacante envía a su víctima cartas aparentemente oficiales, por ejemplo, en forma de correos electrónicos, que inducen al usuario a revelar información confidencial, sobre todo nombres de usuario, contraseñas y pines para el acceso a la banca en línea. Tras sustraer estos datos, el atacante puede suplantar la identidad de su víctima y llevar a cabo transacciones en su nombre.No hace falta decir que los bancos y las aseguradoras jamás solicitan números de tarjeta de crédito, pines u otros datos personales por correo electrónico, teléfono o SMS.

Virus polimórficos

Los verdaderos maestros del camuflaje y el disfraz son los virus polimórficos. Este software es capaz de modificar su propio código de programación, por lo que es especialmente difícil de detectar.

Virus de programas

Un virus de programa es un software que, una vez activado, se introduce de diversas formas y de manera automática en otro programa y lo infecta. A diferencia de lo que ocurre con las bombas lógicas y los troyanos, los virus se multiplican a sí mismos. Y a diferencia de los gusanos, este virus necesita un programa a modo de huésped en el que pueda introducir su código virulento. No obstante, el flujo de programa del huésped no se modifica.

Rootkits

Los rootkits son grupos de herramientas de software que se instalan en un sistema tras introducirse en este y que tienen el objetivo de disfrazar los inicios de sesión del intruso,

ocultar procesos y grabar datos. En definitiva: se vuelven completamente invisibles. Estas herramientas intentan actualizar programas espía previamente existentes e instalar nuevamente spyware que había sido eliminado.

Virus de script y gusanos

Estos virus son muy sencillos de programar y capaces de propagarse en pocas horas por todo el mundo a través del correo electrónico, siempre y cuando se disponga de la tecnología adecuada.

Utilizan lenguajes de script, como Javascript, VBScript, etc., para introducirse en otros scripts nuevos o para propagarse cuando se activan las funciones del sistema operativo. Con frecuencia, esto ocurre a través del correo electrónico o mediante el intercambio de archivos (documentos).

Se denomina "gusano" a un programa que se multiplica a sí mismo, pero que no infecta a ningún huésped. Por lo tanto, los gusanos no pueden formar parte de otros flujos de programa. Muchas veces, la única forma de poder infiltrar un programa dañino en un sistema con fuertes medidas de seguridad es hacer uso de gusanos.

Spyware

Los spyware son programas espía que envían datos personales del usuario al fabricante de estos programas o a terceros sin el conocimiento o el consentimiento del afectado. En la mayoría de los casos, el spyware se utiliza para obtener información sobre los hábitos de navegación en Internet y, de esta forma, poder mostrar banners y ventanas emergentes (popups) de publicidad de una manera selectiva.

Troyanos

En los últimos tiempos, es muy habitual encontrarse con troyanos. Este es el nombre que reciben aquellos programas que simulan llevar a cabo una determinada función, pero que, tras comenzar su ejecución, se quitan la piel de cordero y empiezan a realizar una función diferente, la mayoría de las veces de carácter destructivo. Los troyanos no pueden reproducirse, lo que los distingue de los virus y gusanos. Casi todos ellos llevan nombres llamativos (SEX.EXE o STARTME.EXE) con el fin de inducir al usuario a iniciar su ejecución. Inmediatamente después de empezar a ejecutarse, se activan y llevan a cabo acciones perniciosas, como por ejemplo el formateo del disco duro. El "dropper" (cuentagotas, gotero) es una clase especial de troyano capaz de implantar virus en un sistema informático.

Software engañoso

Conocidos también como "scareware" (programas de susto) o "rogueware" (programas de bribones), se trata de un software engañoso que hace creer que se está sufriendo una infección de virus u otro riesgo similar, lo que hace pensar al usuario que está tratando

con un antivirus profesional. El scareware se instala para crear inseguridad al usuario o para asustarlo. Si la víctima cae en la trampa y se cree amenazado, con frecuencia se le ofrece eliminar el falso riesgo a cambio de una cierta cantidad de dinero. En otros casos, la víctima, creyendo ser el objetivo de un ataque, lleva a cabo una serie de acciones que a la postre posibilitarán un ataque real.

Zombi

Un equipo zombi es un ordenador infectado por malware que permite a los hackers utilizar dicho equipo de manera remota para cometer actos delictivos. Tras recibir la correspondiente orden, el PC afectado puede llevar a cabo acciones diversas, como ataques de denegación del servicio (DoS) o envíos de spam y correos electrónicos de suplantación de identidad.

14. Información y servicio

Este capítulo contiene información relacionada con la información y los servicios de Avira.

- Dirección de contacto
- Soporte técnico
- Archivo sospechoso
- Notificar falsa alarma
- Sus comentarios para aumentar la seguridad

14.1 Dirección de contacto

Con mucho gusto atenderemos cualquier consulta o sugerencia en relación a los productos Avira. Para conocer nuestras direcciones de contacto, consulte Centro de control en **Ayuda > Acerca de Avira Professional Security**.

14.2 Soporte técnico

El soporte técnico de Avira está siempre a su lado para resolver sus dudas y solventar cualquier problema técnico.

Puede obtener toda la información necesaria sobre nuestro completo servicio de asistencia en nuestro sitio web:

http://www.avira.es/professional-support

Para poder ayudarle de manera rápida y eficaz, debe facilitarnos los siguientes datos:

- **Datos de licencia**. Puede encontrar estos datos en la pantalla principal del programa en la opción de menú **Ayuda > Acerca de Avira Professional Security > Información de licencia**. Consulte Información de licencia.
- **Información de versión**. Podrá encontrar esta información en la pantalla principal del programa en la opción de menú **Ayuda > Acerca de Avira Professional Security > Información de versión**. Consulte Información de versión.
- **Versión de Sistema operativo** y Service Packs eventualmente instalados.
- **Paquetes de software instalados**, p. ej., antivirus de otros fabricantes.
- **Mensajes detallados** del programa o del archivo de informes.

14.3 Archivo sospechoso

Puede enviarnos los archivos y virus que nuestros productos no hayan podido detectar o eliminar. Para ello, le ofrecemos varias vías de contacto.

- Identifique el archivo en el administrador de cuarentena de Centro de control en la consola de seguridad del servidor Avira y seleccione la opción **Enviar fichero** en el menú contextual o utilice el botón correspondiente.
- Envíe el archivo seleccionado comprimido (WinZIP, PKZip, Arj, etc.) como adjunto de un correo electrónico a la siguiente dirección:
  virus-professional@avira.es
  Dado que algunas puertas de enlace de correo electrónico trabajan con antivirus, debe enviar el archivo con una contraseña (no olvide facilitárnosla).

- Otra opción es enviarnos el archivo sospechoso a través de nuestro sitio Web:
  http://www.avira.es/sample-upload

14.4 Notificar falsa alarma

Si cree que Avira Professional Security informa de una detección en un archivo que es muy probable que esté "limpio", envíe el archivo en cuestión comprimido (WinZIP, PKZip, Arj, etc.) como elemento adjunto a un correo electrónico a la siguiente dirección:

virus-professional@avira.es

Dado que algunas puertas de enlace de correo electrónico trabajan con antivirus, debe enviar el archivo con una contraseña (no olvide facilitárnosla).

14.5 Sus comentarios para aumentar la seguridad

En Avira, la seguridad de nuestros clientes es nuestra máxima prioridad. Por ello, en Avira no nos limitamos únicamente a someter todas nuestras soluciones a las más estrictas pruebas de calidad y seguridad llevadas a cabo por nuestro equipo de expertos antes de lanzar el producto al mercado. Para nosotros, es igualmente importante tomarnos muy en serio cualquier posible laguna de seguridad que pueda surgir y aprender a eliminarlas.

Si cree haber encontrado una laguna de seguridad en nuestro producto, envíenos un correo electrónico a la siguiente dirección:

vulnerabilities-professional@avira.es

Avira

Versión 4° trimestre de 2013.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Alemania | Teléfono: +49 7542-500 0
www.avira.es