Avira Internet Security

Manual para usuarios

AVIRA

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 protegidas no se indican como tales en este manual. Esto no significa, de todas formas, que pueden usarse libremente.

Información de copyright

Para Avira Internet Security se utiliza el código de otros proveedores. Agradecemos a los titulares de los derechos de autor que hayan puesto su código a nuestra disposición.
Encontrará más información sobre los derechos de autor del programa de ayuda de Avira Internet Security en "Licencias de terceros".

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
- consulte el capítulo: Administración de licencias

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 Vista 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
- Avira SearchFree Toolbar, que es una barra de búsqueda integrada en el navegador web mediante la cual puede realizar búsquedas en la red. También cuenta con widgets para las principales funciones de Internet.
- 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)
- Módulo Protección infantil para el filtrado basado en roles de sitios web no deseados y para la limitación temporal del uso de Internet
- Avira Free Android Security es una aplicación que protege contra robos y pérdidas. Este programa ofrece funciones que permiten localizar el dispositivo móvil en caso de extravío o sustracción. Asimismo, este programa le permite bloquear las llamadas entrantes y los SMS. Avira Free Android Security protege teléfonos móviles y smartphones que utilizan el sistema operativo Android.
- Componentes Backup para la creación de copias de seguridad de sus datos (copias de seguridad de espejo)
- 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
- 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

Los requisitos del sistema son los siguientes:

- Procesador Pentium, como mínimo 1 GHz

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

> **Nota**
> La certificación de Windows 8 para Avira Internet Security está en fase de tramitación.

- 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 512 MB de memoria con Windows XP
- Mínimo de 1024 MB de memoria con Windows 7, Windows Server 2008 (32 bits o 64 bits) y Windows Server 2008 R2 (64 bits)
- Para la instalación del programa: permisos de administrador
- Para todas las instalaciones: Windows Internet Explorer 6.0 o superior
- Conexión a Internet (consulte Instalación)

Avira SearchFree Toolbar

- Sistema operativo
  - Windows XP, SP más reciente (32 bits o 64 bits) o
  - Windows 7, SP más reciente (32 bits o 64 bits)
- Navegador web
  - Windows Internet Explorer 6.0 o superior
  - Mozilla Firefox 3.0 o superior
  - Google Chrome 18.0 o superior

> **Nota**
> Desinstale las barras de búsqueda que estén instaladas antes de llevar a cabo la instalación de Avira SearchFree Toolbar. Si no procede de esta manera, no será posible instalar Avira SearchFree Toolbar.

Nota para los usuarios de Windows Vista

En Windows XP existen muchos usuarios que trabajan con permisos 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, en Windows Vista, Microsoft ha establecido el Control de cuentas de usuario (User Account Control) que ofrece mayor protección para el usuario que inicia

sesión como administrador. Así, en Windows Vista, un administrador disfruta únicamente de los privilegios de un usuario normal. Windows Vista marca claramente con un icono indicador las acciones para las que se precisan permisos 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.

En Windows Vista, el producto Avira precisa de permisos 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 permisos de administrador. Si su actual cuenta de usuario no tiene permisos de administrador, la ventana de diálogo en Windows Vista 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.

2.3 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 da en forma de un código de activación. Este código de activación es un código alfanumérico que recibirá tras la adquisición de su producto Avira. Comprende los datos concretos de su licencia, es decir, los programas para los que tiene licencia y los períodos de tiempo en que esta es válida.

Si adquirió el producto Avira por Internet, se le enviará el código de activación en un correo electrónico; si no, puede encontrarlo en el envase del producto.

Para activar la licencia de su programa, introduzca el código de activación durante la activación del producto. Esta puede efectuarse durante la instalación. No obstante, también puede activar su producto Avira tras la instalación en el administrador de licencias en **Ayuda > Gestión 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. No obstante, también puede prolongar la licencia de su producto Avira a través de la Administración de licencias bajo **Ayuda > Administración de licencias**.

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.

2.3.3 Actualización

En la administración de licencias puede iniciar la actualización de un producto de la familia de productos de Avira Desktop. En este caso, no es necesario desinstalar el antiguo producto ni instalar manualmente el nuevo. Para efectuar actualizaciones desde la administración de licencias, introduzca en el campo de entrada correspondiente el código de activación del producto al que desea actualizarse. A continuación, el nuevo producto se instalará automáticamente.

Con el fin de que su equipo disfrute de unos niveles de fiabilidad y seguridad elevados, Avira le informará de las actualizaciones pendientes. Haga clic en **Actualización** en el elemento emergente para acceder a la página de actualización específica de su producto. Puede actualizar su producto actual o adquirir un producto Avira más completo. La página resumen de los productos Avira le muestra los productos que utiliza en la actualidad y le ofrece la posibilidad de comparar estos con otros productos Avira. Para obtener más información, haga clic en el símbolo de información situado a la derecha del nombre de producto. Si desea seguir usando su producto actual, haga clic en **Actualización** para instalar inmediatamente la nueva versión con funciones mejoradas. Si desea adquirir un producto más completo, haga clic en **Comprar** en el extremo inferior de la columna de producto correspondiente y accederá a la tienda online de Avira, donde podrá realizar su pedido.

> **Nota**
> En función de su producto y su sistema operativo, puede que necesite permisos de administrador para efectuar la actualización. Inicie sesión como administrador antes de comenzar este proceso.

2.3.4 Administración de licencias

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

Administración de licencias de Avira Internet 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 Internet 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

En este capítulo obtendrá información sobre la instalación y desinstalación de su producto Avira:

- consulte el capítulo: Antes de la instalación: requisitos y preparación del equipo para la instalación
- consulte el capítulo: Instalación exprés: instalación predeterminada según la configuración predefinida
- consulte el capítulo: Instalación personalizada: instalación configurable
- consulte el capítulo: Instalación del producto de prueba
- consulte el capítulo: Asistente de configuración
- consulte el capítulo: Cambios en la instalación
- consulte el capítulo: Módulos de instalación
- consulte el capítulo: Desinstalación: ejecutar desinstalación

3.1 Tipos de instalación

Durante la instalación, puede seleccionar un tipo de instalación en el asistente de instalación:

Exprés

- Se instalan los componentes predeterminados.
- Los ficheros de programa se instalan en un directorio estándar predefinido en *C:\Archivos de programa*.
- Su producto Avira se instala con los ajustes de configuración predeterminados. No dispondrá de la posibilidad de establecer valores predefinidos en el asistente de configuración.

Definido por el usuario

- Tiene la posibilidad de seleccionar determinados componentes del programa para su instalación (consulte el capítulo Instalación y desinstalación > Módulos de instalación).
- Puede seleccionar una carpeta de destino para ubicar los ficheros 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.
- Con ayuda del asistente de configuración, puede definir ajustes de configuración personalizados para su producto Avira y llevar a cabo un breve análisis del sistema nada más concluir la instalación.

3.2 Antes de la instalación

Nota
Antes de la instalación, compruebe si su equipo cumple los requisitos del sistema. De ser así, puede instalar el producto Avira.

Inicialización antes de la instalación

✓ Cierre su programa de correo. También se recomienda cerrar todas las aplicaciones.
✓ 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.

↳ El producto Avira examinará su equipo para comprobar si existe software incompatible.

↳ Si se detecta software incompatible, se 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**.

▸ Algunos programas únicamente pueden desinstalarse manualmente. Seleccione los programas y haga clic en **Siguiente**.

↳ La desinstalación de uno o varios programas precisa reiniciar su equipo. Tras el reinicio, proseguirá el proceso de desinstalación.

Advertencia
Su equipo no estará protegido hasta que este proceso del producto Avira haya concluido.

Instalación

El programa de instalación le guía durante la misma. En la mayoría de los pasos de la instalación, basta con hacer un simple clic para seguir adelante en el proceso.

Los botones más importantes tienen asignadas las siguientes funciones:

- **Aceptar**: confirmar la operación.
- **Cancelar**: cancelar operación.
- **Siguiente**: continuar al siguiente paso.
- **Anterior**: regresar al paso anterior.

▸ Establezca una conexión de Internet. La conexión de Internet es necesaria para ejecutar los siguientes pasos de la instalación:

- Descarga de los ficheros de programa actuales y del motor de análisis, así como de los ficheros de firmas de virus actuales del día mediante el programa de instalación (en instalaciones basadas en Internet)
- Activación del programa
- Si fuera necesario, ejecución de una actualización tras finalizar la instalación

▸ Debe indicar el código de activación o el fichero de licencia de su producto Avira si desea activar el programa.

Nota
Instalación basada en Internet:
Para la instalación basada en Internet, dispone de un programa de instalación que descarga los ficheros de programa actuales de los servidores web de Avira antes de ejecutar la instalación. Este procedimiento garantiza que su producto Avira se instale con un fichero de firmas de virus actual del día.

Instalación con un paquete de instalación:
El paquete de instalación contiene el programa de instalación y todos los ficheros de programa necesarios. Sin embargo, al instalar con un paquete de instalación no se puede seleccionar el idioma de su producto Avira. Se recomienda ejecutar una actualización al acabar la instalación para actualizar el fichero de firmas de virus.

Nota
Para activar el producto, su producto Avira se comunica a través del protocolo HTTP y el puerto 80 (comunicación Web), así como a través del protocolo de cifrado SSL y el puerto 443 con los servidores de Avira. Si usa un cortafuegos, asegúrese de que este no bloquee las conexiones necesarias y los datos entrantes o salientes.

3.3 Instalación exprés

Instalación del producto Avira:

Inicie el programa de instalación haciendo doble clic en el archivo de instalación que ha descargado de Internet o inserte el CD del programa.

Instalación desde Internet

↳ Se muestra la pantalla **Bienvenido**.

▸ Haga clic en **Siguiente** para continuar con la instalación.

↳ Se muestra el cuadro de diálogo **Selección de idioma**.

- Seleccione el idioma que desea utilizar para la instalación del producto Avira y haga clic en **Siguiente** para confirmar la selección del idioma.
  - ↪ Se abre el cuadro de diálogo **Descargar**. Todos los archivos necesarios para la instalación se descargan de los servidores web de Avira. La ventana **Descargar** se cierra una vez concluida la descarga.

Instalación con un paquete de instalación

- ↪ Se abre la ventana **Preparando la instalación**.
- ↪ Se extrae el archivo de instalación. Se inicia la rutina de instalación.
- ↪ Se visualizará el cuadro de diálogo **Elegir el tipo de instalación**.

Nota
De forma predeterminada se utiliza la instalación exprés. Se instalan todos los componentes estándar, que no podrá configurar. En caso de que prefiera una instalación personalizada, consulte el capítulo Instalación y desinstalación > Instalación personalizada.

- La casilla **Deseo mejorar mi protección con Avira Proactiv y Protection Cloud** (Configuración > General > Protección avanzada) está seleccionada de forma predeterminada. Desactive esta casilla si no desea formar parte de la Comunidad Avira.
  - ↪ Si confirma la participación en la Comunidad Avira, Avira enviará datos sobre programas sospechosos que se detecten 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 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 correspondiente.
  - ↪ Se abre el **Asistente para licencias** que le ayuda a activar el producto.
  - ↪ Aquí tiene la oportunidad de configurar un servidor proxy.
- Si lo desea, haga clic en **Configuración de proxy** para ejecutar las configuraciones deseadas y confirme las configuraciones realizadas haciendo clic en **OK**.
- Si ya dispone de un código de activación, seleccione **Activar producto** e introduzca el código.

  -O BIEN-
- Si no dispone de ningún código de activación, haga clic en el enlace **compre una clave de activación ahora**.
  - ↪ Será redireccionado al sitio web de Avira.

Como alterativa, puede hacer clic en el enlace **Ya tengo un fichero de licencia**.

↳ Se visualizará el cuadro de diálogo **Abrir archivo**.

- Seleccione el archivo de licencia, con la extensión *.KEY*, y haga clic en **Abrir**.

  ↳ El código de activación se copiará al asistente para licencias.

- En caso de que desee probar el producto, consulte la información a partir del capítulo Instalación del producto de prueba.
- Haga clic en **Siguiente**.

  ↳ El progreso de la instalación se muestra mediante una barra verde.

- Haga clic en **Siguiente**.

  ↳ Se visualizará el cuadro de diálogo **Únase a los millones de usuarios de Avira que ya disfrutan de Avira SearchFree**.

- En caso de que no desee instalar Avira SearchFree Toolbar, desactive tanto la casilla de verificación del **Contrato de licencia** de Avira SearchFree Toolbar y Avira SearchFree Updater, como la casilla de verificación de **Avira SearchFree (search.avira.com)** con la que se determinará como página de inicio de su navegador.

Nota
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.

- Haga clic en **Siguiente**.

  ↳ El progreso de la instalación de la Avira SearchFree Toolbar se muestra mediante una barra verde.

  ↳ El icono de bandeja de Avira se ubica en la barra de tareas.

  ↳ El módulo **Updater** busca posibles actualizaciones para proteger su equipo de forma óptima.

  ↳ La ventana de estado **Luke Filewalker** se abre para el primer análisis directo del escáner, informa sobre el estado del análisis y muestra los resultados.

- Si después del análisis del sistema se le solicita un reinicio del sistema, llévelo a cabo para que su sistema esté totalmente protegido.

Tras concluir correctamente la instalación, se recomienda comprobar en el área **Estado** del Centro de control si el programa de protección está actualizado.

- Si su producto Avira muestra que su equipo no está totalmente protegido, haga clic en **Solucionar problema**.

  ↳ Se abrirá el cuadro de diálogo **Restaurar protección**.

- Maximice la seguridad de su sistema, activando las opciones especificadas.

- A continuación, realice en caso necesario un análisis completo del sistema.

3.4 Instalación personalizada

Instalación del producto Avira:

Inicie el programa de instalación haciendo doble clic en el archivo de instalación que ha descargado de Internet o inserte el CD del programa.

Instalación desde Internet

→ Se muestra la pantalla **Bienvenido**.

- Haga clic en **Siguiente** para continuar con la instalación.
  → Se muestra el cuadro de diálogo **Selección de idioma**.
- Seleccione el idioma que desea utilizar para la instalación del producto Avira y haga clic en **Siguiente** para confirmar la selección del idioma.
  → Se abre el cuadro de diálogo **Descargar**. Todos los archivos necesarios para la instalación se descargan de los servidores web de Avira. La ventana **Descargar** se cierra una vez concluida la descarga.

Instalación con un paquete de instalación

→ Se abre la ventana **Preparando la instalación**.

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

→ Se visualizará el cuadro de diálogo **Elegir el tipo de instalación**.

Nota
De forma predeterminada se utiliza la instalación exprés. Se instalan todos los componentes estándar, que no podrá configurar. Si desea ejecutar una instalación exprés, consulte el capítulo: Instalación y desinstalación > Instalación exprés.

- Seleccione **Personalizada** como el tipo de instalación deseado.
- La opción **Deseo mejorar mi protección con Avira ProActiv y Protection Cloud** está predeterminada. Si no desea participar en la Comunidad Avira, desmarque esta casilla.
  → Si confirma la participación en la Comunidad Avira, Avira enviará datos sobre programas sospechosos que se detecten 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 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 correspondiente.
- Haga clic en **Siguiente**.
  - ↪ Se abre la ventana **Seleccionar directorio de destino**.
  - ↪ El directorio predeterminado es *C:\Programme\Avira\AntiVir Desktop*
- Haga clic en **Siguiente** para proseguir con la instalación.

  -O BIEN-

  Seleccione otro directorio de destino con **Examinar** y confirme pulsando **Siguiente**.
  - ↪ Aparece el cuadro de diálogo **Instalar componentes**.
- Active o desactive los componentes deseados y confirme con **Siguiente**.
- Si ha seleccionado el componente **Protection Cloud** 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**.
- Haga clic en **Siguiente**.
- En el siguiente cuadro de diálogo puede establecer si debe crearse un acceso directo en el escritorio o un grupo de programas en el menú Inicio.
- Haga clic en **Siguiente**.
  - ↪ Se abre el **Asistente para licencias**.

Dispone de las siguientes opciones para activar el programa:

- Introducción de un código de activación.
  - ↪ Su producto Avira se activa con su licencia introduciendo su código de activación.
- Si no dispone de ningún código de activación, haga clic en el enlace **compre una clave de activación ahora**.
  - ↪ Será redireccionado al sitio web de Avira.
- Selección de la opción **Probar el producto**
  - ↪ Si selecciona **Probar el producto**, se genera durante la activación una licencia de prueba que activará el programa. Puede probar el producto Avira con todas las funciones durante un tiempo determinado (consulte Instalación del producto de prueba).

Nota
Con la opción **Ya tengo un fichero de licencia** puede leer un fichero de licencia válido. El fichero de licencia se genera durante el proceso de activación del producto con un código de activación válido y se guarda en el directorio de

su producto Avira. Use esta opción si ya ha ejecutado una activación del producto y desea volver a instalar su producto Avira.

Nota
En algunas versiones para la venta de productos Avira ya se incluye un código de activación con el producto. Por lo tanto, no es necesario introducir un código de activación. Si es necesario, el código de activación guardado se muestra en el asistente para licencias.

Nota
Para activar el programa, se establece conexión con los servidores de Avira. En **Configuración de proxy** puede configurar la conexión a Internet a través de un servidor proxy.

- Seleccione un proceso de activación y confirme con **Siguiente**.
- Si ya dispone de un fichero de licencia válido, salte al apartado "Selección de la opción *Ya tengo un fichero de licencia*".

Activación del producto

↳ Se abre un cuadro de diálogo en el que puede indicar sus datos personales.

- Escriba sus datos y pulse **Siguiente**.

↳ Los datos se transmiten a los servidores de Avira y se verifican. Su producto Avira se activa con su licencia.

↳ En el cuadro de diálogo siguiente, se muestran los datos de la licencia.

- Haga clic en **Siguiente**.
- Salte el siguiente apartado "Selección de la opción *Ya tengo un fichero de licencia*".

Selección de la opción "Ya tengo un fichero de licencia"

↳ Se abre un cuadro de diálogo para leer el fichero de licencia.

- Seleccione un fichero de licencia (extensión *.KEY*) con sus datos de licencia para el programa y haga clic en **Abrir**.

↳ En el cuadro de diálogo siguiente, se muestran los datos de la licencia.

- Haga clic en **Siguiente**.

Continuación tras finalizar la activación o carga del fichero de licencia

↳ Se visualizará el cuadro de diálogo **Únase a los millones de usuarios de Avira que ya disfrutan de Avira SearchFree**.

- Si no desea instalar Avira SearchFree Toolbar, desmarque la casilla del **Contrato de licencia** de Avira SearchFree Toolbar y Avira SearchFree Updater y la casilla que define **Avira SearchFree (search.avira.com)** como página de inicio del navegador.

Nota 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.

- Haga clic en **Siguiente**.
  - ↪ El progreso de la instalación de la Avira SearchFree Toolbar se muestra mediante una barra verde.
  - ↪ Se cierra el **Asistente de instalación** y se abre el **Asistente de configuración**.

3.5 Instalación del producto de prueba

Instalación del producto Avira:

Inicie el programa de instalación haciendo doble clic en el archivo de instalación que ha descargado de Internet o inserte el CD del programa.

Instalación desde Internet

- ↪ Se muestra la pantalla **Bienvenido**.

- Haga clic en **Siguiente** para continuar con la instalación.
  - ↪ Se muestra el cuadro de diálogo **Selección de idioma**.
- Seleccione el idioma que desea utilizar para la instalación del producto Avira y haga clic en **Siguiente** para confirmar la selección del idioma.
  - ↪ Se abre el cuadro de diálogo **Descargar**. Todos los archivos necesarios para la instalación se descargan de los servidores web de Avira. La ventana **Descargar** se cierra una vez concluida la descarga.

Instalación con un paquete de instalación

- ↪ Se abre la ventana **Preparando la instalación**.
- ↪ Se extrae el archivo de instalación. Se inicia la rutina de instalación.
- ↪ Se visualizará el cuadro de diálogo **Elegir el tipo de instalación**.

Nota
De forma predeterminada se utiliza la instalación exprés. Se instalan todos los componentes estándar, que no podrá configurar. Si desea ejecutar una instalación personalizada, consulte el capítulo : Instalación y desinstalación > Instalación personalizada.

- La casilla **Deseo mejorar mi protección con Avira Proactiv y Protection Cloud** (Configuración > General > Protección avanzada) está seleccionada de forma predeterminada. Si no desea participar en la Comunidad Avira, desmarque esta casilla.
  - ↪ Si confirma la participación en la Comunidad Avira, Avira enviará datos sobre programas sospechosos que se detecten 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 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 correspondiente.
- Haga clic en **Siguiente**.
  - ↪ Se abre el **Asistente para licencias** que le ayuda a activar el producto.
  - ↪ Aquí tiene la oportunidad de configurar un **servidor proxy**.
- Haga clic en **Configuración de proxy** para realizar la configuración y confirme los ajustes con **Aceptar**.
- Seleccione la opción **Probar el producto** en el asistente para licencias y haga clic en **Siguiente**.
- Inserte los datos en los campos obligatorios del **Registro**. Decida si desea suscribirse al **Boletín de noticias de Avira** y haga clic en **Siguiente**.
  - ↪ El progreso de la instalación se muestra mediante una barra verde.
  - ↪ Se muestra el cuadro de diálogo **Únase a los millones de usuarios de Avira que ya usan Avira SearchFree Toolbar**.
- Si no desea instalar Avira SearchFree Toolbar, desmarque la casilla del **Contrato de licencia** de Avira SearchFree Toolbar y Avira SearchFree Updater y la casilla que define **Avira SearchFree (search.avira.com)** como página de inicio del navegador.

Nota
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.

- Haga clic en **Siguiente**.
  - ↪ El progreso de la instalación de la Avira SearchFree Toolbar se muestra mediante una barra verde.
- Se le pedirá que reinicie el sistema para activar el producto Avira. Haga clic en **Sí** para reiniciar el ordenador inmediatamente.
  - ↪ El icono de bandeja de Avira se ubica en la barra de tareas.
  - ↪ La licencia de evaluación es válida durante 31 días.

3.6 Asistente de configuración

En caso de una instalación personalizada, al final se abre el asistente de configuración. En el asistente de configuración puede establecer los parámetros importantes de su producto Avira.

- En la ventana de bienvenida del asistente de configuración, haga clic en **Siguiente** para iniciar la configuración del programa.
  - ↪ El cuadro de diálogo **Configurar AHeAD** permite elegir un nivel de detección para la tecnología AHeAD. El nivel de detección seleccionado se aplica en la configuración de la tecnología AHeAD de Scanner (análisis directo) y de Real-Time Protection (análisis en tiempo real).
- Seleccione un nivel de detección y continúe con la configuración pulsando **Siguiente**.
  - ↪ En el siguiente cuadro de diálogo, **Seleccionar categorías de riesgos avanzadas**, puede adaptar las funciones de protección de su producto Avira seleccionando categorías de riesgos.
- Si fuera necesario, active más categorías de riesgos y prosiga con la configuración pulsando **Siguiente**.
  - ↪ En caso de que haya seleccionado el módulo de instalación Avira FireWall para su instalación , aparece la ventana de diálogo **Reglas predeterminadas para el acceso a la red y el uso de recursos de la red**. Puede especificar si Avira FireWall permitirá accesos externos a recursos compartidos, así como accesos a la red por parte de las aplicaciones de empresas de confianza.
- Active las opciones pertinentes y prosiga con la configuración pulsando **Siguiente**.
  - ↪ En caso de que haya seleccionado el módulo de instalación Avira Real-Time Protection para su instalación, aparece la ventana de diálogo **Modo de inicio de Real-Time Protection**. Podrá definir el momento de inicio de Real-Time Protection. Real-Time Protection se iniciará con el modo de inicio indicado cada vez que se reinicie el equipo.

Nota
El modo de inicio especificado de Real-Time Protection se guarda en el registro y no puede modificarse a través de la configuración.

Nota
La selección del modo de inicio predeterminado para Real-Time Protection (inicio normal) y un inicio de sesión rápido en la cuenta de usuario tienen como consecuencia que, en determinadas circunstancias, durante el inicio del equipo los programas que se inician automáticamente al iniciar el sistema no puedan ser escaneados, ya que se han iniciado antes de que se produzca la carga completa de Real-Time Protection.

- Active la opción pertinente y prosiga con la configuración pulsando **Siguiente**.
  - ↪ En caso de que haya seleccionado el módulo de instalación de Avira Web Protection, aparece el cuadro de diálogo **Safe Browsing**. Tiene la opción de asignar a los usuarios de un equipo diversas funciones para el uso de Internet (infantil, juvenil, adulto). También puede desactivar la opción Safe Browsing.
- Configure las opciones deseadas para Safe Browsing y prosiga la configuración con **Siguiente**.
  - ↪ En el siguiente cuadro de diálogo, **Asignar contraseña**, puede proteger el acceso a la configuración con una contraseña. Ello se recomienda sobre todo en caso de que Safe Browsing esté activado.
  - ↪ En el siguiente cuadro de diálogo, **Análisis del sistema**, puede activarse o desactivarse la ejecución de un análisis rápido del sistema. El análisis rápido del sistema se ejecuta una vez concluida la configuración y antes de reiniciar el equipo. En él se analizan los programas iniciados y los ficheros más importantes del sistema en busca de virus y malware.
- Active o desactive la opción **Análisis rápido del sistema** y prosiga la configuración con **Siguiente**.
  - ↪ En el siguiente cuadro de diálogo puede concluir la configuración con **Finalizar**.
  - ↪ Se aplican los parámetros de configuración indicados y seleccionados.
  - ↪ Si ha activado la opción **Análisis rápido del sistema**, se abrirá la ventana **Luke Filewalker**. Scanner lleva a cabo un análisis rápido del sistema.
  - ↪ Si después del análisis del sistema se le solicita un reinicio del sistema, llévelo a cabo para que su sistema esté totalmente protegido.

Tras concluir correctamente la instalación, se recomienda comprobar en el área **Estado** del Centro de control si el programa de protección está actualizado.

- Si su producto Avira muestra que su equipo no está totalmente protegido, haga clic en **Solucionar problema**.
  - ↪ Se abrirá el cuadro de diálogo **Restaurar protección**.
- Maximice la seguridad de su sistema, activando las opciones especificadas.
- A continuación, realice en caso necesario un análisis completo del sistema.

3.7 Cambios en la instalación

Tiene la posibilidad de añadir o eliminar componentes del programa de la instalación actual del producto Avira (consulte el capítulo Instalación y desinstalación > Módulos de 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**.

Seleccione su producto Avira y haga clic **Cambiar**. En el cuadro de diálogo *Bienvenido*, seleccione la opción **Modificar programa**. Se le guiará a través de los cambios en la instalación.

3.8 Módulos de instalación

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

- **Avira Internet Security**
  Este módulo contiene todos los componentes necesarios para la instalación correcta de su producto Avira.
- **Real-Time Protection**
  Avira Real-Time Protection se ejecuta en segundo plano. Supervisa y repara, si fuera posible, los ficheros en operaciones como abrir, escribir y copiar en tiempo real (en acceso). Si un usuario realiza una operación con un fichero (cargar, ejecutar, copiar el fichero), el producto Avira analiza automáticamente el fichero. En el caso de la operación de fichero Cambiar nombre, Avira Real-Time Protection no realiza análisis alguno.
- **Mail Protection**
  Mail Protection es la interfaz entre su equipo y el servidor de correo del cual su programa de correo (cliente de correo) descarga los emails. Mail Protection se intercala como proxy entre el programa de correo y el servidor de correo. Todos los emails entrantes se dirigen a través de este proxy, que analiza la existencia de virus o programas no deseados en los emails y los entrega al programa de correo. Según la configuración, el programa trata los emails infectados automáticamente o pregunta al usuario antes de realizar una determinada acción. Además, Mail Protection puede protegerle de manera eficaz de los emails de spam.
- **Avira FireWall**
  El Avira FireWall controla las vías de comunicación hacia y desde su ordenador. Permite o deniega la comunicación basándose en directrices de seguridad.
- **Rootkits Protection**
  Avira Rootkits Protection analiza si ya hay software instalado en el equipo que, una vez ha irrumpido en el sistema informático, ya no puede detectarse con los métodos convencionales de detección de software malintencionado.
- **ProActiv**
  El componente ProActiv supervisa acciones de aplicaciones y avisa sobre un comportamiento sospechoso. Mediante este reconocimiento basado en el comportamiento podrá protegerse ante malware desconocido. El componente ProActiv está integrado en Avira Real-Time Protection.
- **Protection Cloud**
  El componente Protection Cloud es un módulo para el reconocimiento dinámico en línea de malware desconocido hasta ese momento.

- **Backup**
  El componente Backup permite crear backups reflejados, manuales o automáticos, de sus datos.
- **Web Protection**
  Mientras se navega por Internet, el explorador web solicita datos a un servidor web. Los datos transmitidos por el servidor web (ficheros HTML, ficheros de script y de imagen, ficheros Flash, secuencias de audio y de vídeo, etc.) pasan por regla general de la memoria caché del navegador directamente a la ejecución en el navegador web, de modo que el análisis en tiempo real, como el 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 transmisión de datos (80, 8080, 3128) y analiza los datos transmitidos para detectar la existencia de virus y programas no deseados. Según la configuración, el programa trata los ficheros infectados automáticamente o pregunta al usuario antes de realizar una determinada acción.
- **Extensión de shell**
  Extensión de shell crea la entrada *Analizar ficheros seleccionados con Avira* en el menú contextual del Explorador de Windows (botón derecho del ratón). Esta entrada permite analizar directamente determinados ficheros o directorios.

3.9 Desinstalación

Si desea desinstalar el producto Avira del equipo, puede utilizar la opción **Programas** para **Agregar o Quitar Programas** desde el Panel de control de Windows.

Modo de desinstalar su producto Avira (se describe a modo de ejemplo para Windows 7):

- En el menú **Iniciar**, abra el **Panel de control**.
- Haga doble clic en **Programas y características**.
- Seleccione de la lista su producto Avira y haga clic en **Desinstalar**.
  - ↳ Se le pregunta si confirma que desea quitar el programa.
- Confirme la operación pulsando **Sí**.
  - ↳ Se le pregunta si debe activarse de nuevo el Firewall de Windows (puesto que se va a desactivar Avira FireWall).
- Confirme la operación pulsando **Sí**.
  - ↳ Se quitan todos los componentes del programa.
- Haga clic en **Finalizar** para concluir con la desinstalación.
  - ↳ Es posible que aparezca un cuadro de diálogo recomendando el reinicio del equipo.
- Confirme la operación pulsando **Sí**.

↪ El producto Avira se habrá desinstalado. Si fuera necesario, se reiniciará el equipo, proceso en el cual se eliminarán todos los directorios, archivos y entradas de registro del programa.

Nota
Avira SearchFree Toolbar no se incluye en el programa de desinstalación, sino que debe ser desinstalada por separado siguiendo los pasos mencionados anteriormente. Para ello, debe estar activada Avira SearchFree Toolbar mediante el administrador de complementos. Tras la desinstalación, la barra de búsqueda ya no estará integrada en su explorador web.

4. Acerca de Avira Internet 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 Avira SearchFree Toolbar
- consulte el capítulo Procedimientos

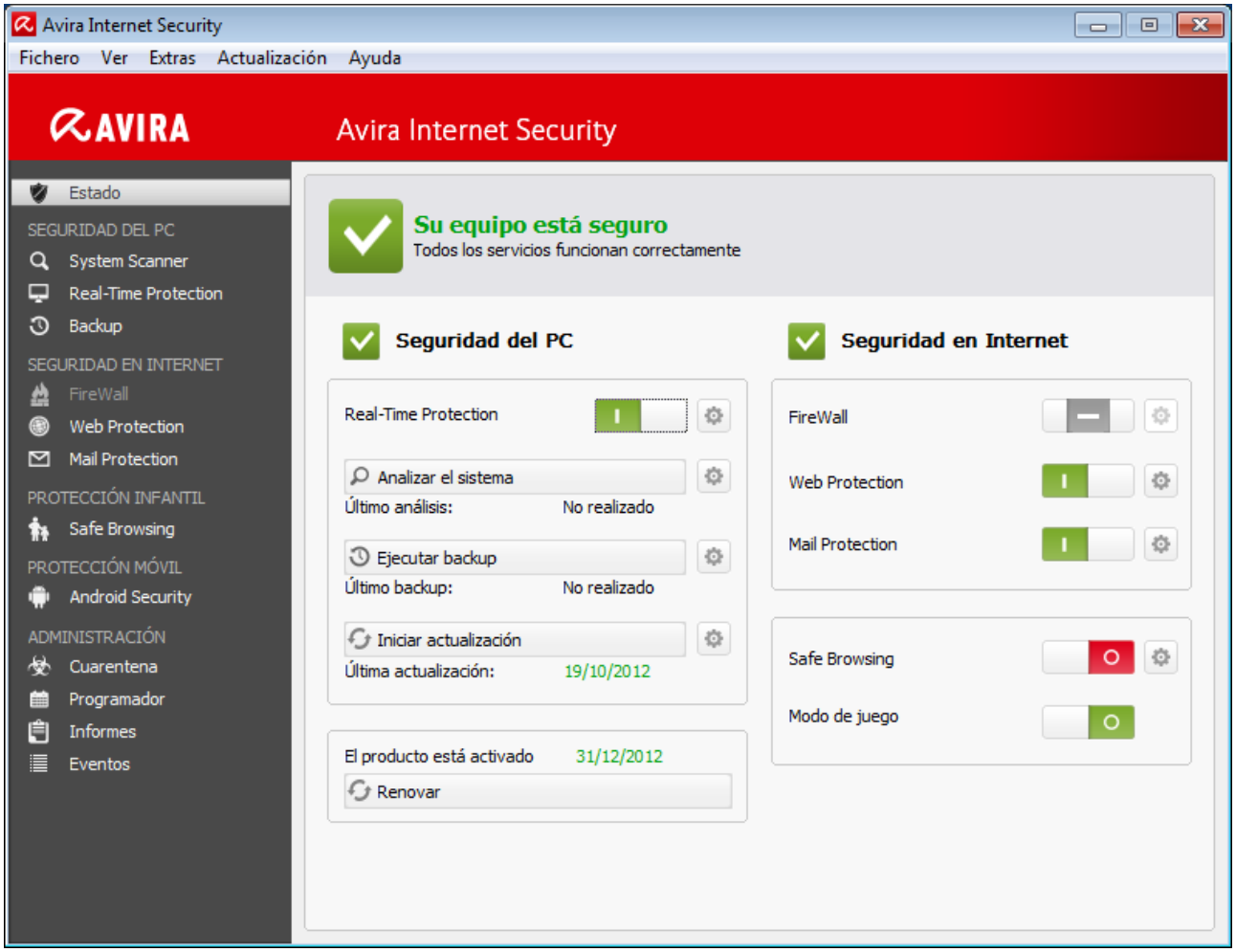
4.1 Interfaz de usuario y uso

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.
- En la sección **Backup** puede realizar copias de seguridad de sus datos de forma rápida y fácil, así como crear tareas de backup (consulte Backup).

- *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 de Avira 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 enseñar al filtro AntiSpam para que aprenda qué 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).
- *PROTECCIÓN INFANTIL*: Aquí encontrará herramientas que permiten que sus niños disfruten de una experiencia en la Red totalmente segura.
  - Safe Browsing: Es posible asignar funciones de usuario a cada usuario del equipo. Puede configurar una función de usuario, que comprende un conjunto de reglas con los siguientes criterios: URL (direcciones de Internet) prohibidas o permitidas, categorías de contenido prohibidas, duración de uso de Internet y, en su caso, períodos de uso permitidos para los días de la semana
- *PROTECCIÓN MÓVIL*: Desde la categoría Avira Free Android Security puede disponer de sus dispositivos Android en línea.
  - Con Avira Free Android Security puede administrar todos sus dispositivos que funcionan con el sistema operativo Android.
- *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 Modo de juego

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 juego. En el modo de juego se aplican todas las reglas definidas de adaptador y aplicación que ha configurado en Avira FireWall sin que se le notifiquen eventos de red.

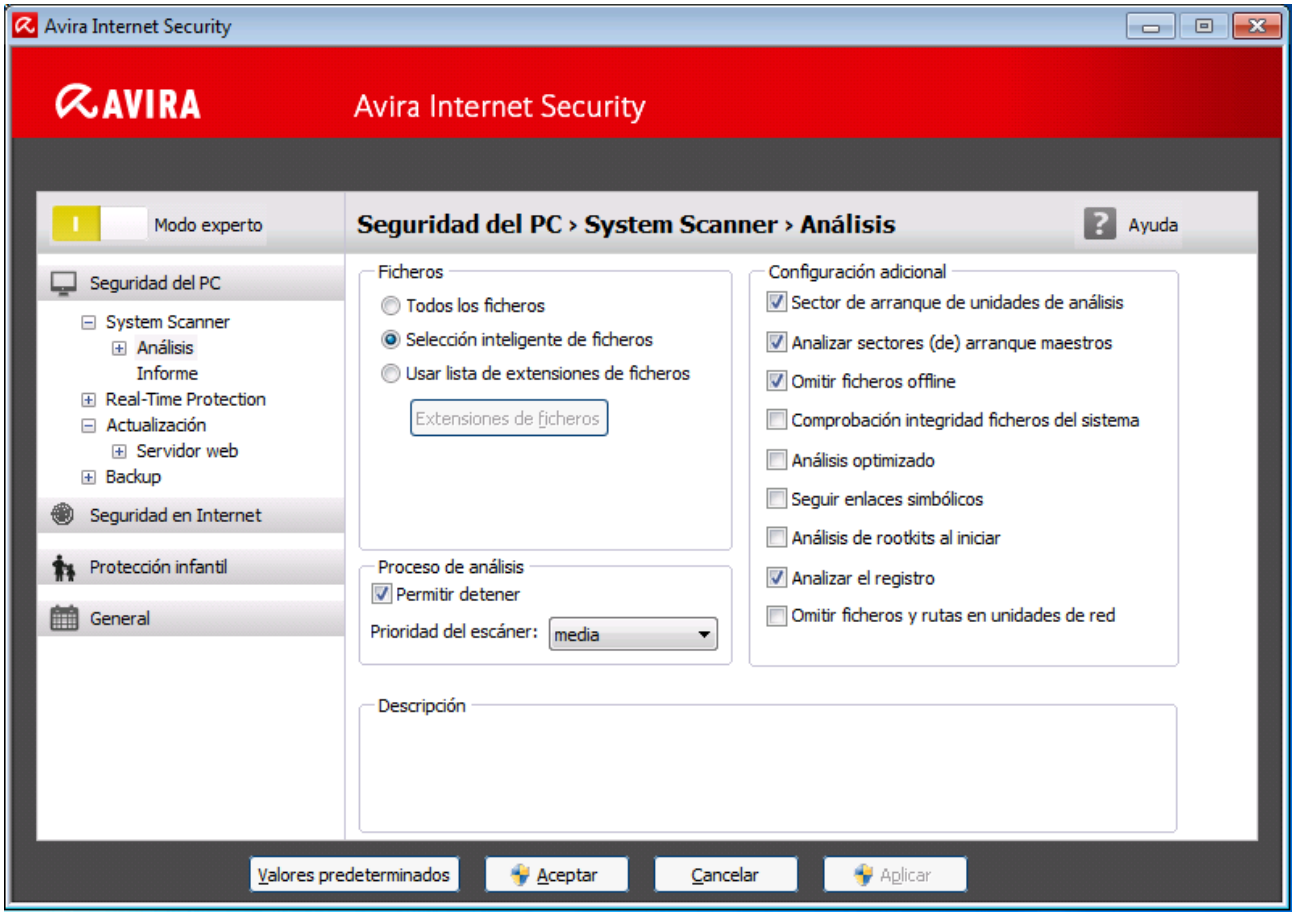
Tiene la posibilidad de activar el modo de juego con un clic sobre el botón **CONECTADO/DESCONECTADO** o de mantener el modo automático. El modo de juego está preseleccionado con **Automático** y se representa en color verde. Con esta preselección, su producto Avira cambia automáticamente al modo de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

- Haga clic en el botón situado a la izquierda junto a **DESCONECTADO** para activar el modo de juego.
  - ↪ El modo de juego 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 juego mensajes de sobremesa y advertencias sobre accesos a la red y peligros eventuales claramente visibles.

4.1.3 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. Para seleccionar cada una de las fichas de configuración,

debe estar activado el **modo experto** de la configuración. En ese caso, aparecerá un cuadro de diálogo que solicita activar el **modo experto**.

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.

Nota
Solo en el modo experto se muestran todas las secciones de configuración. Active el **Modo experto** para ver todas las secciones de configuración. Puede asignar una contraseña al **Modo experto** y, al activarlo, tendrá que indicarla.

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.

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
  - 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
- **Backup**:
  - Configuración del componente Backup (copia de seguridad incremental, análisis de virus durante la copia de seguridad)
  - Excepciones: configuración de los ficheros de los que se va a hacer una copia de seguridad.
  - Configuración de la función de informe
- **Actualización**: Configuración de los ajustes de la actualización
- **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 la base de datos de aprendizaje AntiSpam, vaciar base de datos de aprendizaje
  - Configuración de un pie de página en correos electrónicos enviados
  - Configuración de la función de informe
- **Protección infantil**:
  - Safe Browsing: función de protección para los niños con filtro basado en funciones y limitación de horario basada en funciones del acceso a Internet.
- **General**:
  - 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
  - Configuración de las advertencias acústicas tras la detección de malware

4.1.4 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.
  - **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 Internet Security**: Abre el Centro de control.
- **Configurar Avira Internet Security**: Abre la configuración.
- **Mis mensajes**: Abre una ventana emergente con los mensajes más recientes relacionados con su producto Avira.
- **Mi configuración de comunicación**: Abre el Centro de suscripción para mensajes de producto.
- **Iniciar actualización**: Inicia una actualización.
- **Ayuda**: Abre la ayuda en línea.
- **Acerca de Avira Internet 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 Avira SearchFree Toolbar

Avira SearchFree Toolbar contiene dos componentes principales: Avira SearchFree y la ya conocida Toolbar.

La nueva Avira SearchFree Toolbar se instala como un complemento (add-on). Al iniciar por primera vez el navegador (Internet Explorer y Firefox), se le preguntará si desea que el programa Avira SearchFree Toolbar modifique su navegador. Debe aceptar si quiere instalar correctamente Avira SearchFree Toolbar.

Avira SearchFree es el nuevo motor de búsqueda de Avira. Está formado por el logotipo de Avira, que conduce al sitio web de Avira al hacer clic sobre él, y por canales web, de imagen y de vídeo. Permite que los usuarios de Avira lleven a cabo búsquedas exhaustivas y seguras.

La barra de herramientas se integra en su navegador web y contiene un campo de búsqueda, un logotipo de Avira que permite enlazar directamente con el sitio web de Avira, dos indicadores de estado, tres widgets y el menú **Opciones**.

- Barra de búsqueda
  Use la barra de búsqueda para rastrear Internet rápidamente y sin coste alguno con ayuda del motor de búsqueda Avira SearchFree.
- Indicador de estado
  Los indicadores de estado ofrecen información sobre el estado de Web Protection y sobre el grado de actualización de su producto Avira, por lo que le ayudan a identificar las acciones que, eventualmente, deben llevarse a cabo para proteger su equipo.
- Widgets
  Avira le permite acceder directamente a las funciones más importantes de Internet, como las relacionadas con los mensajes de Facebook o el correo electrónico. También puede definir la seguridad de su sistema mediante el widget de Seguridad del navegador (únicamente en Firefox e Internet Explorer).
- Opciones
  Gracias a este menú, puede acceder a las opciones de Toolbar, cancelar el proceso de búsqueda, consultar información y la ayuda de la barra de herramientas, y desinstalar Avira SearchFree Toolbar directamente desde el navegador web (únicamente en Firefox e Internet Explorer).

4.2.1 Uso

Barra de búsqueda

Mediante la barra de búsqueda puede llevar a cabo búsquedas en Internet basándose en la palabra o las palabras desee.

Introduzca el término en el campo de búsqueda y después pulse la tecla **Enter** o haga clic en **Buscar**. El motor de búsqueda Avira SearchFree llevará a cabo la búsqueda y, a continuación, mostrará las coincidencias en la ventana del navegador.

Para averiguar cómo configurar a su gusto Avira SearchFree en los navegadores Internet Explorer, Firefox y Google Chrome, consulte **Opciones.**

Indicador de estado

Web Protection

Para determinar el estado de seguridad de su equipo, puede usar los iconos y los mensajes siguientes:

Icono	Indicador de estado	Descripción
	*Web Protection*	Al pasar el puntero del ratón por encima del símbolo, aparecerá el siguiente mensaje: *Avira Web Protection está activado. Su navegación por Internet está protegida.* Esto significa que no es necesario realizar ninguna otra acción.
	*Web Protection*	Al pasar el puntero del ratón por encima del símbolo, aparecerá el siguiente mensaje: *Avira Web Protection está apagado. Haga clic para saber cómo encenderlo.* ↪ Se le redireccionará a un artículo de nuestra base de datos de conocimientos.

	*Sin Web Protection*	Al pasar el puntero del ratón por encima del símbolo, aparecerá el siguiente mensaje: • *No tiene instalado Avira Web Protection. Haga clic para saber cómo proteger su navegación por Internet.* Esto significa que, o bien se ha desinstalado el antivirus de Avira, o bien no se ha instalado correctamente. • *Web Protection se incluye de forma gratuita con Avira Anti-Virus. Haga clic para saber cómo instalarlo.* Esto significa que, o bien se ha desinstalado Avira Web Protection, o bien no se ha instalado correctamente. ↪ En ambos casos, se le redireccionará al sitio web de Avira, donde podrá descargar el correspondiente producto.
	*Error*	Al pasar el puntero del ratón por encima del símbolo, aparecerá el siguiente mensaje: *Avira informó de un error.* ▸ Haga clic en el símbolo de color gris o en el texto para abrir la página de soporte técnico de Avira.

Widgets

Avira SearchFree Toolbar cuenta con 3 widgets para las principales funciones de Internet: Facebook, correo electrónico y Seguridad del navegador.

Facebook

Esta función le permite recibir directamente los mensajes de Facebook para tener siempre la información más reciente.

Email

Al hacer clic en el símbolo del correo electrónico, se muestra una lista desplegable en la que puede escoger entre los proveedores más utilizados.

Seguridad del navegador

Avira ha creado este widget para que todas las opciones de seguridad de Internet sean fácilmente accesibles. En la actualidad, solo está disponible para Firefox e Internet Explorer. Se ofrecen diversas opciones que, según el navegador, reciben nombres diferentes:

- *Bloqueador de elementos emergentes*

Si se activa esta opción, durante la navegación por Internet se bloquearán las ventanas emergentes.

- *Bloqueador de cookies*

Si se activa esta opción, durante la navegación no se almacenarán las cookies.

- *Modo privado (Firefox) / Navegación privada (Internet Explorer)*

Si se activa esta opción, no se dejarán rastros durante la navegación. Esta opción no está disponible en Internet Explorer 7 y 8.

- *Borrar crónica más reciente (Firefox)/Borrar historial de exploración (Internet Explorer)*

Con esta opción puede borrar todas las actividades realizadas hasta el momento en Internet.

Website Safety Advisor

Website Safety Advisor determina el nivel de seguridad mientras navega por Internet. De esta forma, puede valorar si el riesgo que entraña para su seguridad la navegación por un determinado sitio web es bajo o alto.
Este widget le ofrece asimismo información adicional sobre el sitio web, como por ejemplo quién es el propietario del dominio, o por qué un sitio web se ha incluido en un determinado nivel de seguridad.
Existen tres niveles de seguridad: seguro, bajo riesgo y alto riesgo.

Los niveles de seguridad se muestran en la barra de herramientas y en los resultados de la búsqueda en forma de un icono de bandeja de Avira con distintos símbolos:

Icono	Indicador de estado	Descripción
	*Seguro*	Marca de verificación en color verde para sitios web seguros.
	*Bajo riesgo*	Signo de exclamación en color amarillo para sitios web que entrañan un riesgo bajo.

	*Alto riesgo*	Signo de STOP en color rojo para sitios web que entrañan un riesgo alto para su seguridad.
	*Fracasado*	Signo de interrogación en color gris para sitios web cuyo riesgo no se ha podido establecer.
	*Verificación*	Se muestra este signo mientras se evalúa el estado de seguridad.

Browser Tracking Blocker

Con Browser Tracking Blocker puede detener los seguimientos que recopilan información sobre usted mientras navega en Internet.
Este widget le permite decidir qué seguimientos desea bloquear y cuáles quiere autorizar.

Las empresas se dividen en tres categorías:

- Redes sociales
- Redes
- Otras empresas

4.2.2 Opciones

Avira SearchFree Toolbar es compatible con los navegadores web Internet Explorer, Firefox y Google Chrome, los cuales pueden configurarse según se desee:

- Opciones de configuración de Internet Explorer
- Opciones de configuración de Firefox
- Opciones de configuración de Chrome

Internet Explorer

En el menú **Opciones** de Internet Explorer existen las siguientes opciones de configuración para Avira SearchFree Toolbar:

Opciones de Toolbar

Buscar

Seleccionar motor Avira

En el menú **Seleccionar motor Avira** puede escoger el motor de análisis que se utilizará para llevar a cabo la búsqueda. Existen disponibles motores de análisis de EE. UU., Brasil, Alemania, España, Europa, Francia, Italia, Países Bajos, Rusia y Reino Unido.

Iniciar búsquedas en

En el menú de la opción **Iniciar búsquedas en** puede elegir dónde se mostrará el resultado de la búsqueda, bien en la **Ventana actual**, en una **Nueva ventana** o en una **Nueva pestaña**.

Mostrar búsquedas recientes

Si la opción **Mostrar búsquedas recientes** está activa, puede mostrar las palabras clave introducidas hasta el momento en el cuadro de entrada de texto de la barra de búsqueda.

Autoborrar historial de búsquedas al salir del navegador

Active la opción **Autoborrar historial de búsquedas al salir del navegador** si no quiere guardar las búsquedas en curso y desea que estas se cancelen al cerrar el navegador web.

Otras opciones

Seleccionar idioma Toolbar

En la opción **Seleccionar idioma Toolbar** puede escoger el idioma en que se mostrará Avira SearchFree Toolbar. Están disponibles los siguientes idiomas: inglés, alemán, español, francés, italiano, portugués y neerlandés.

Nota
El idioma predeterminado de Avira SearchFree Toolbar es el mismo que el de su programa, siempre y cuando esté disponible. Si la barra de herramientas no pudiera mostrarse en su idioma, la opción predeterminada será inglés.

Mostrar las etiquetas de texto del botón

Desactive la opción **Mostrar las etiquetas de texto del botón** si quiere ocultar el texto que aparece junto a los iconos de Avira SearchFree Toolbar.

Borrar historial

Active la opción **Borrar historial** si no quiere guardar las búsquedas en curso y desea que estas se cancelen inmediatamente.

Ayuda

Haga clic en **Ayuda** para acceder a la página web con las preguntas más frecuentes (P+F) acerca de la barra de herramientas.

Desinstalar

También puede desinstalar Avira SearchFree Toolbar directamente desde Internet Explorer: Desinstalar a través del navegador web.

Acerca de

Haga clic en **Acerca de** para averiguar qué versión de Avira SearchFree Toolbar está instalada.

Firefox

En el menú **Opciones** de Firefox existen las siguientes opciones de configuración para Avira SearchFree Toolbar:

Opciones de Toolbar

Buscar

Seleccionar motor Avira

En el menú **Seleccionar motor Avira** puede escoger el motor de análisis que se utilizará para llevar a cabo la búsqueda. Existen disponibles motores de análisis de EE. UU., Brasil, Alemania, España, Europa, Francia, Italia, Países Bajos, Rusia y Reino Unido.

Mostrar búsquedas recientes

Si la opción **Mostrar búsquedas recientes** está activa, puede mostrar las palabras clave introducidas hasta el momento haciendo clic en la flecha de la barra de búsqueda. Escoja una de las palabras clave para que se muestren nuevamente los resultados de la búsqueda correspondiente.

Autoborrar historial de búsquedas al salir del navegador

Active la opción **Autoborrar historial de búsquedas al salir del navegador** si no quiere guardar las búsquedas en curso y desea que estas se cancelen al cerrar el navegador web.

Mostrar los resultados de búsqueda de Ask al introducir palabras clave o URL inválidas en la barra de direcciones del explorador

Si esta opción está activa, cada vez que se introduzca una palabra clave o una dirección URL no válida en el campo de dirección del navegador Web, se iniciará una búsqueda y posteriormente se mostrarán los resultados correspondientes.

Otras opciones

Seleccionar idioma Toolbar

En la opción **Seleccionar idioma Toolbar** puede escoger el idioma en que se mostrará Avira SearchFree Toolbar. Están disponibles los siguientes idiomas: inglés, alemán, español, francés, italiano, portugués y neerlandés.

Nota
El idioma predeterminado de Avira SearchFree Toolbar es el mismo que el de

su programa, siempre y cuando esté disponible. Si la barra de herramientas no pudiera mostrarse en su idioma, la opción predeterminada será inglés.

Mostrar las etiquetas de texto del botón

Desactive la opción **Mostrar las etiquetas de texto del botón** si quiere ocultar el texto que aparece junto a los iconos de Avira SearchFree Toolbar.

Borrar historial

Active la opción **Borrar historial** si no quiere guardar las búsquedas en curso y desea que estas se cancelen inmediatamente.

Ayuda

Haga clic en **Ayuda** para acceder a la página web con las preguntas más frecuentes (P+F) acerca de la barra de herramientas.

Desinstalar

También puede desinstalar Avira SearchFree Toolbar directamente desde Internet Explorer: Desinstalar a través del navegador web.

Acerca de

Haga clic en **Acerca de** para averiguar qué versión de Avira SearchFree Toolbar está instalada.

Chrome

En el navegador web Google Chrome puede encontrar todas las opciones de configuración debajo del paraguas rojo de Avira. Existen las siguientes opciones para Avira SearchFree Toolbar:

Ayuda

Haga clic en **Ayuda** para acceder a la página web con las preguntas más frecuentes (P+F) acerca de la barra de herramientas.

Indicaciones acerca de la desinstalación

Aquí puede encontrar vínculos a las indicaciones acerca de la desinstalación de Avira SearchFree Toolbar.

Acerca de

Haga clic en **Acerca de** para averiguar qué versión de Avira SearchFree Toolbar está instalada.

Mostrar y ocultar Avira SearchFree Toolbar

Esta opción de menú permite mostrar u ocultar Avira SearchFree Toolbar, que se encuentra en la parte superior de la ventana.

4.2.3 Desinstalación

Modo de desinstalar su Avira SearchFree Toolbar (se describe a modo de ejemplo para Windows 7):

- En el menú **Iniciar**, abra el **Panel de control**.
- Haga doble clic en **Programas y características**.
- Seleccione de la lista la entrada **Avira SearchFree Toolbar plus Web Protection** y haga clic en **Desinstalar**.
  - ↪ Se le preguntará si realmente quiere desinstalar este producto.
- Confirme la operación pulsando **Sí**.
  - ↪ Se desinstalará Avira SearchFree Toolbar plus Web Protection. Si fuera necesario, se reiniciará el equipo, proceso en el cual se eliminarán todos los directorios, archivos y entradas de registro Avira SearchFree Toolbar plus Web Protection.

Desinstalación desde el navegador web

También puede desinstalar Avira SearchFree Toolbar directamente desde el navegador en **Firefox e Internet Explorer**:

- Abra el menú **Opciones** situado a la derecha de la barra de búsqueda.
- Haga clic en **Desinstalar**.
  - ↪ Si aún permanece abierto el navegador, se le pedirá que lo cierre.
- Cierre el navegador web y haga clic en **Aceptar**.
  - ↪ Se desinstalará Avira SearchFree Toolbar plus Web Protection. Si fuera necesario, se reiniciará el equipo, proceso en el cual se eliminarán todos los directorios, archivos y entradas de registro Avira SearchFree Toolbar plus Web Protection.

Nota Recuerde que para desinstalar Avira SearchFree Toolbar, esta debe estar activa en el administrador de complementos.

Desinstalación como complemento

Dado que la versión más reciente de Avira SearchFree Toolbar está instalada como complemento, también es posible administrar esta utilidad con diversos administradores de complementos.

Firefox

Haga clic en **Herramientas > Complementos > Extensiones**. Desde aquí puede administrar el complemento de Avira, es decir, puede activarlo, desactivarlo o desinstalarlo.

Internet Explorer

Haga clic en **Administrar complementos > Barras de herramientas y extensiones**. Desde aquí puede administrar el complemento de Avira, es decir, puede activarlo, desactivarlo o desinstalarlo.

Google Chrome

Puede administrar el complemento de Avira desde **Opciones > Extensiones** . Desde aquí puede activar la barra de herramientas, desactivarla o desinstalarla.

4.3 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.

4.3.1 Activar la 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 > Gestión de licencias**

Nota
En 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.

4.3.2 Activar producto

Dispone de las siguientes opciones para activar su producto Avira:

- Activación con una licencia completa válida

  Para activar el programa con una licencia completa necesita un código de activación válido que contenga los datos de la licencia que ha adquirido. Habrá recibido el código de activación por email o este consta en el embalaje del producto.
- Activación con una licencia de evaluación

  Su producto Avira se activa con una licencia de evaluación generada automáticamente con la que puede probar su producto Avira durante un tiempo limitado con el volumen completo de funciones.

Nota
Para activar el producto o para solicitar una licencia de prueba, necesita tener una conexión a Internet activa.
Si no se puede establecer conexión con los servidores de Avira, compruebe la configuración del cortafuegos que se esté utilizando: Durante la activación del producto se usan conexiones a través del protocolo HTTP y el puerto 80 (comunicación web), así como a través del protocolo de cifrado SSL y el puerto 443. Asegúrese de que su cortafuegos no esté bloqueando los datos entrantes y salientes. Compruebe primero si puede acceder a páginas web con el explorador web.

A continuación, le mostramos cómo activar su producto Avira:

Si todavía no ha instalado su producto Avira:

- Instale su producto Avira.

↳ Durante la instalación se le pide que seleccione una opción de activación

- **Activar producto** = Activación con una licencia completa válida
- **Probar producto** = Activación con una licencia de evaluación

▶ Para la activación con licencia completa, indique el código de activación.

▶ Confirme la selección del procedimiento de activación con **Siguiente**.

▶ Si fuera necesario, indique sus datos personales y confírmelos con **Siguiente**.

↳ En el cuadro de diálogo siguiente, se muestran los datos de la licencia. Se ha activado su producto Avira.

▶ Continúe con la instalación.

Si ya ha instalado su producto Avira:

▶ En el Centro de control, seleccione la opción de menú **Ayuda > Gestión de licencias**.

↳ Se abre el asistente para licencias en el que puede seleccionar una opción de activación. Los siguientes pasos de la activación de producto son idénticos al proceso descrito anteriormente.

4.3.3 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: 2 horas.

- 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

4.3.4 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: 2 horas.

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

4.3.5 Análisis directo: 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.

- En Windows Vista:

  En 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 Windows Vista 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 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)

4.3.6 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.

4.3.7 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.

4.3.8 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

4.3.9 Análisis directo: 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 Windows Vista: ).
  - ↪ Aparece la ventana **Luke Filewalker** y se inicia el análisis directo.
  - ↪ Una vez transcurrido el proceso de análisis, se muestran los resultados.

4.3.10 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.

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.

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.

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.**.

4.3.11 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
Cada vez se puede cargar un solo fichero.

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).

4.3.12 Cuarentena: Restaurar los ficheros de cuarentena

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

- **En Windows XP y 2000**:

   Este icono permite restaurar los ficheros en su directorio original.

   Este icono permite restaurar los ficheros en el directorio que elija.

- **En Windows Vista**:

  En 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:  , 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.

4.3.13 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).

4.3.14 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 ?).

4.3.15 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.

4.3.16 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:

- Backup
- Web Protection
- Real-Time Protection
- Mail Protection
- FireWall
- Servicio de ayuda
- Programador
- Safe Browsing
- Scanner
- Updater

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.

4.3.17 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 de email seleccionada ya no se analizará en el futuro en busca de spam.

  - ↪ 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 o spam.

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.

4.3.18 Mail Protection: Enseñar al módulo AntiSpam

El módulo AntiSpam contiene una base de datos de aprendizaje. En esta base de datos de aprendizaje se incorporan sus criterios de clasificación personalizados. Conforme pasa el tiempo, los filtros, algoritmos y criterios de evaluación de spam internos se adaptan a sus criterios personales.

Así se clasifican los emails para la base de datos de aprendizaje:

- Seleccione en el Centro de control la sección *SEGURIDAD EN INTERNET* **> Mail Protection**.
  - ↪ En la lista verá los emails entrantes.
- Seleccione el email que va a clasificar.

- Haga clic en el icono correspondiente para identificar el email como *spam*  o como email deseado (*'legítimo'*)  .
  - ↪ El email se incorpora a la base de datos de aprendizaje y se usará la próxima vez para detectar spam.

Nota
Puede eliminar la base de datos de aprendizaje en la configuración, en **Mail Protection > General > AntiSpam**.

Nota
Por supuesto, la exclusión de determinadas direcciones de email del análisis de malware se refiere únicamente a los emails entrantes. Asimismo, las funciones de aprendizaje AntiSpam y las excepciones AntiSpam también se refieren exclusivamente a emails entrantes. Para desconectar el análisis de los emails salientes, desactive esta opción en la configuración, en Mail Protection > Análisis.

4.3.19 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.

4.3.20 Backup: Crear backups manualmente

Con la herramienta de backup del Centro de control puede crear rápida y fácilmente una copia de seguridad de sus datos personales. Con Avira Backup se crean lo que se denomina backups en espejo que permiten hacer una copia de seguridad y preservar la versión más actual de sus datos al tiempo que se ahorran recursos. Al hacer copias de seguridad con Avira Backup, puede analizar la existencia de virus y malware en la información que se va a preservar. Los ficheros afectados no se incluyen en la copia de seguridad.

> **Nota**
> Con los backups reflejados, a diferencia de los backups de versiones, no se preservan versiones de backup por separado. El backup reflejado contiene todo el volumen de datos en el momento del último backup. No obstante, aunque se eliminen ficheros del volumen de datos que se va a preservar, no se hará sincronización alguna durante el siguiente backup, es decir, los ficheros eliminados todavía se encontrarán en el backup.

> **Nota**
> En Avira Backup con configuración predeterminada, solo se hace copia de seguridad de los ficheros modificados y tiene lugar un análisis de virus y malware. Puede cambiar los parámetros de la configuración en Backup > Configuración.

Así se hace copia de seguridad de los datos con la herramienta de backup:

- Seleccione en el Centro de control la sección *SEGURIDAD DEL PC* **> Backup**.
  - ↪ Aparecen perfiles de copia de seguridad predefinidos.

- Seleccione uno de los perfiles de backup predefinidos.

  -O BIEN-

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

  -O BIEN-

  Cree un perfil de backup nuevo

- Introduzca en el campo **Directorio de destino** una ubicación de copia de seguridad para el perfil seleccionado.

  Como ubicación de la copia de seguridad puede indicar para el backup un directorio de su equipo o de una unidad de red conectada, así como un soporte de datos extraíble, por ejemplo, un lápiz de memoria USB o un disco.

- Haga clic en el icono  .
  - ↪ Aparece la ventana **Avira Backup** y se inicia el backup. El estado y los resultados del backup se muestran en la ventana de backup.

Si desea adaptar un perfil de backup:

- Despliegue el árbol de ficheros del perfil de análisis **Selección manual** de manera que estén abiertos todos los directorios y las unidades de los que va a hacer copia de seguridad:

- 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 de los que desea hacer copia de seguridad 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)

Si desea crear un perfil de backup nuevo:

- Haga clic en el icono  **Crear nuevo perfil**.
  - ↪ Aparece el perfil *Nuevo perfil* debajo de los perfiles existentes.
- Si fuera necesario, cambie el nombre del perfil de backup haciendo clic en el icono  .
- Seleccione los nodos y directorios de los que desea hacer copia de seguridad mediante un clic en la casilla del nivel de directorios.

  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)

4.3.21 Backup: Crear copias de seguridad automáticamente

A continuación, le mostramos cómo crear una tarea para llevar a cabo copias de seguridad automáticamente:

- Seleccione en el Centro de control la sección *ADMINISTRACIÓN* **> Programador**.
- Haga clic en el icono  .
  - ↪ 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 entrada **Tarea de backup**.
- Haga clic en **Siguiente**.
  - ↪ Aparece el cuadro de diálogo **Selección del perfil**.
- Seleccione el perfil que debe analizarse.

> **Nota**
> Únicamente se muestran los perfiles de backup para los que se ha indicado una ubicación de copia de seguridad.

- 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**
- **Plug and Play**

  En eventos **Plug and Play** se crea una copia de seguridad siempre que se conecta al equipo el soporte de datos extraíble seleccionado como ubicación de copia de seguridad para el perfil de backup. El evento de backup **Plug and Play** supone que se ha indicado un lápiz de memoria USB como ubicación de copia de seguridad.

- Según lo que seleccione, indique la fecha si fuera necesario.

- En caso necesario, seleccione la siguiente opción adicional (solo 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:
- **Minimizado**: solo barra de progreso
- **Maximizado**: toda la ventana de backup
- **Invisible**: ninguna ventana de diálogo
- 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

5. 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. 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 host 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: 2 horas.

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 reciben por Internet, a través de un servidor web del fabricante. Normalmente, se utiliza la conexión de red existente como conexión a los servidores de descarga de Avira. Esta configuración estándar puede ajustarse en Configuración > Actualización.

7. FireWall

Avira Internet 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 Internet Security en todos los sistemas operativos hasta Windows 7.

8. Backup

Tiene distintas posibilidades para hacer una copia de seguridad (backup) de sus datos:

Copia de seguridad mediante la herramienta Backup

Con la herramienta Backup, puede seleccionar o crear perfiles de copia de seguridad e iniciar manualmente una copia de seguridad para un perfil seleccionado .

Copia de seguridad mediante una tarea de backup en el Planificador

El Planificador ofrece la posibilidad de crear tareas de backup controladas por programación (tiempo) o por eventos. El Planificador ejecuta las tareas de backup automáticamente. Este procedimiento es adecuado si va a hacer regularmente copias de seguridad de determinados datos .

9. 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 y Vista) o el capítulo Centro de actividades de Windows (para Windows 7 o superior)

9.1 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.

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 (modo experto) 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 (modo experto).
- 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 (modo experto) **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*.
- Active el **Modo experto**.
- 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).

9.2 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.

9.2.1 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.

9.2.2 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.

9.2.3 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

9.3 Centro de seguridad de Windows

- desde Windows XP Service Pack 2 hasta Windows Vista -

9.3.1 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.

9.3.2 El Centro de seguridad de Windows y su producto Avira

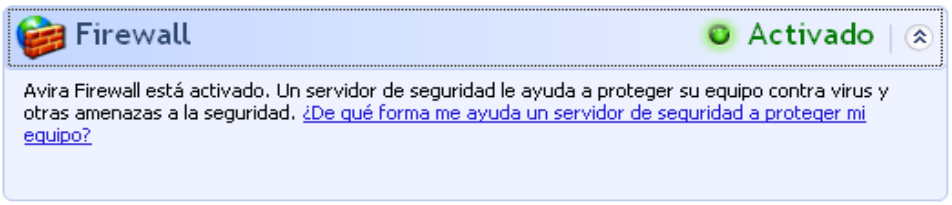
Firewall

Es posible que en el Centro de seguridad encuentre la siguiente información relativa al firewall:

- Firewall ACTIVO/Firewall activado
- Firewall INACTIVO/Firewall desactivado

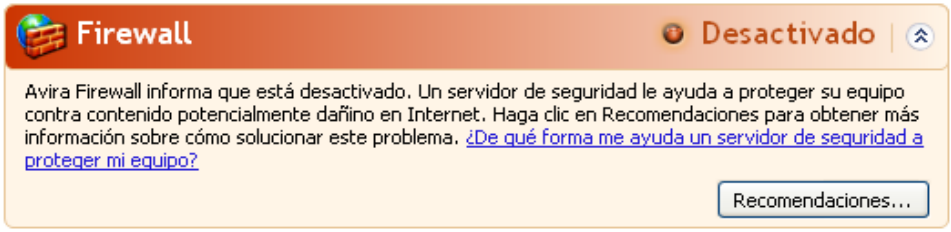
Firewall ACTIVO/Firewall activado

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 de **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.

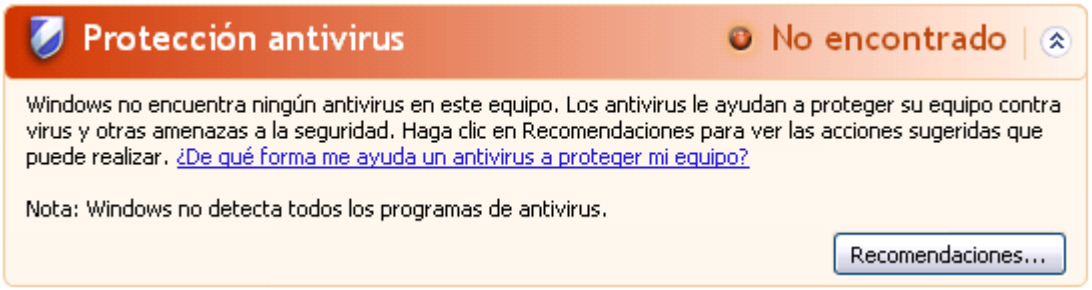
Software de protección/Protección contra software malicioso

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

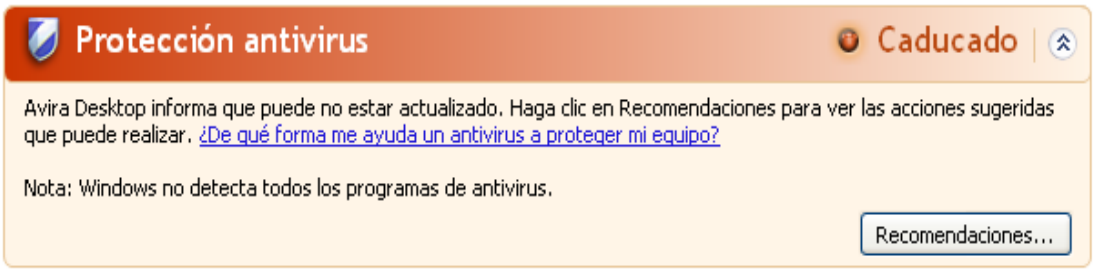
Este mensaje del Centro de seguridad de Windows aparece si no se ha encontrado ningún antivirus en el equipo.



Nota
Instale su producto Avira en el equipo para protegerlo de virus y otros programas no deseados.

Protección Antivirus NO ACTUAL

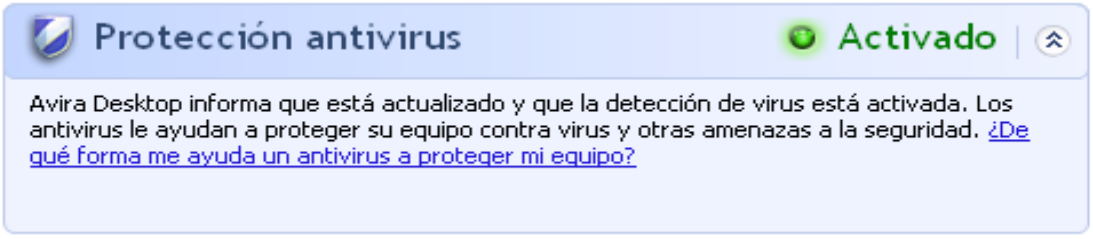
Si tiene instalado Windows XP Service Pack 2 o Windows Vista y posteriormente instala su producto Avira, o bien si instala Windows XP Service Pack 2 o Windows Vista en un sistema en el que ya esté instalado su producto Avira, recibirá el siguiente mensaje:



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

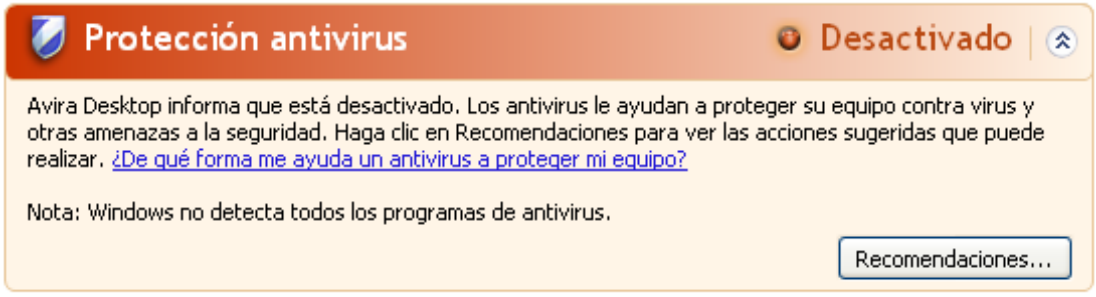
Tras instalar su producto Avira y actualizarlo a continuación, recibirá el siguiente mensaje:



Su producto Avira está actualizado y Avira Real-Time Protection está activo.

Protección Antivirus INACTIVA

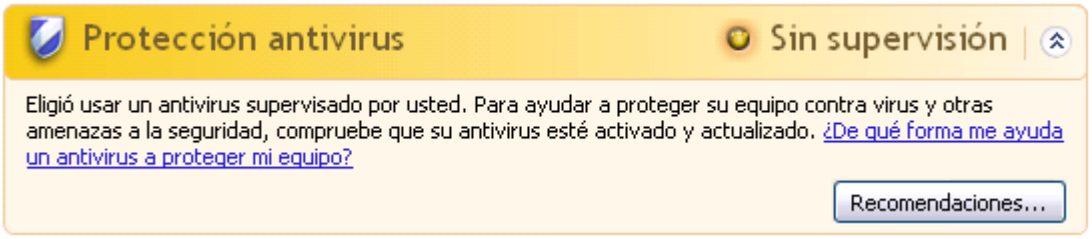
Recibirá el siguiente mensaje si desactiva Avira Real-Time Protection o si interrumpe el servicio Real-Time Protection.



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
La función no es compatible con Windows Vista.

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 o Windows Vista, 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.

9.4 Centro de actividades de Windows

- Windows 7 y Windows 8 -

9.4.1 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*).

9.4.2 El Centro de actividades de Windows y su producto Avira

Firewall de red

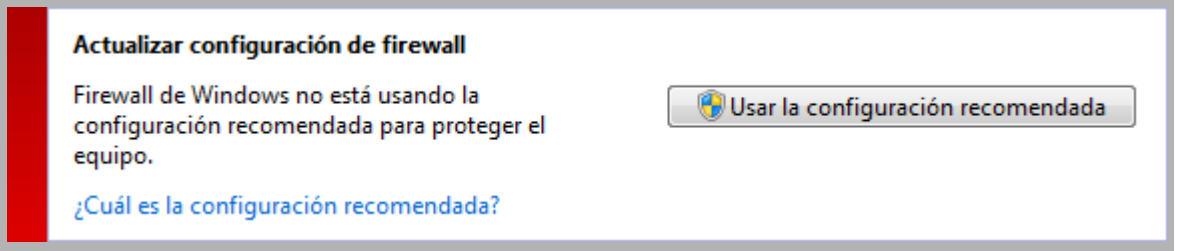
Es posible que en el Centro de actividades encuentre la siguiente información relativa al firewall:

- 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

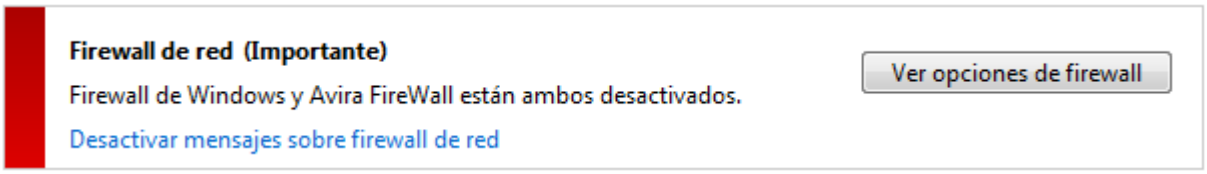
Tras instalar su producto Avira y desactivar el Firewall de Windows, recibirá el siguiente mensaje en **Centro de actividades > Seguridad > Firewall de red**: *Avira FireWall indica que está activado*. Esto significa que Avira FireWall es la solución de cortafuegos seleccionada (es importante distinguir 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.



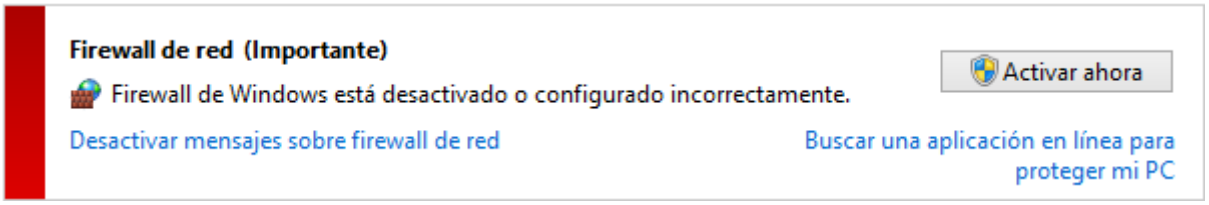
Firewall de Windows y Avira FireWall están ambos desactivados

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**.

- **En Windows 7**

  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.

Protección antivirus

El Centro de actividades de Windows le ofrece las siguientes indicaciones relativas a la protección antivirus:

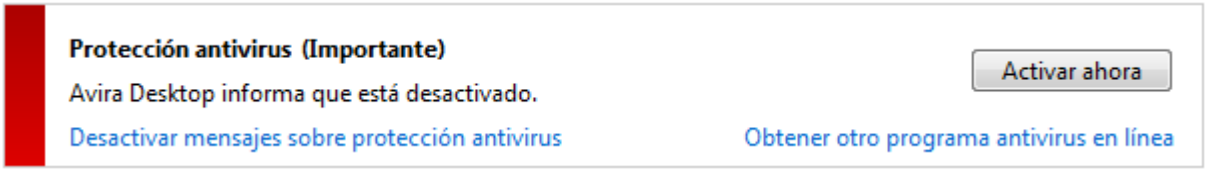
- Avira Desktop indica que está actualizado y que la detección de virus está activada
- Avira Desktop está desactivado
- Avira Desktop no actualizado
- Windows no encontró ningún software antivirus en este equipo
- Avira Desktop dejó de proteger el equipo

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

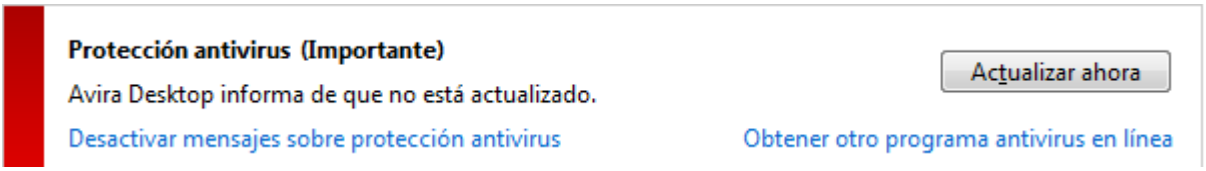
Recibirá el siguiente mensaje si desactiva Avira Real-Time Protection o si interrumpe el servicio Real-Time Protection.



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

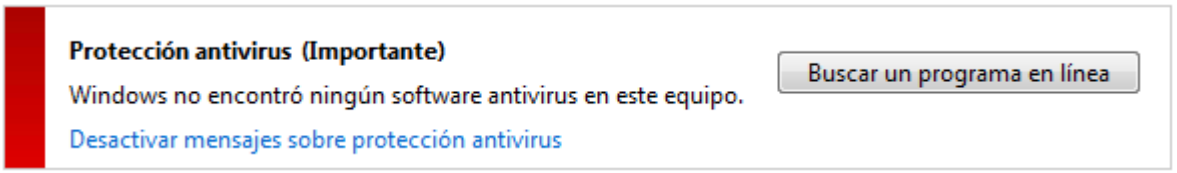
Recibirá el siguiente mensaje si acaba de instalar Avira y si por cualquier motivo el archivo de firmas de virus, el motor de análisis o los ficheros del programa de su producto Avira no se actualizaran automáticamente (p. ej., si actualiza una versión antigua de un sistema operativo de Windows, en el 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.

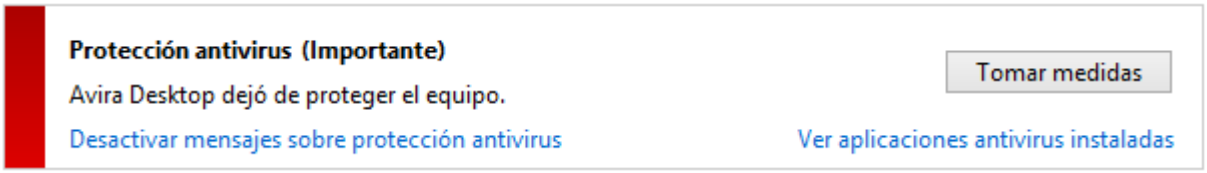


Nota
Tenga en cuenta que esta opción no se encuentra disponible en Windows 8. A partir de este sistema operativo, Windows Defender lleva a cabo la función de protección antivirus preestablecida de Microsoft.

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:

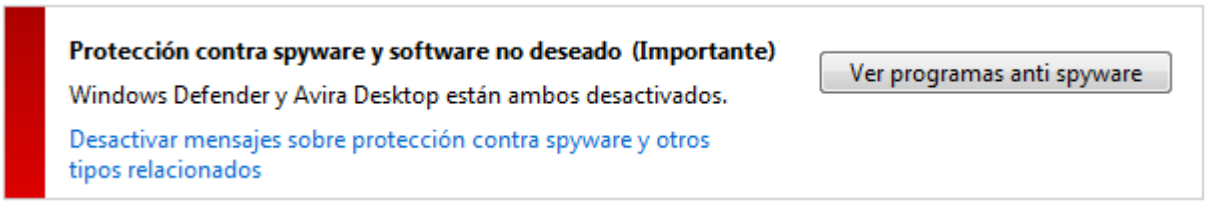
- Avira Desktop indica que está activado
- Tanto Windows Defender como Avira Desktop indican que están desactivados
- Avira Desktop no actualizado
- Windows Defender no está actualizado
- Windows Defender está desactivado

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

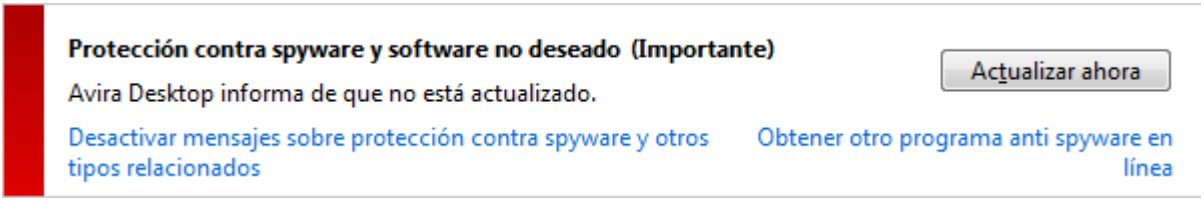
Recibirá el siguiente mensaje si desactiva Avira Real-Time Protection o si interrumpe el servicio Avira Real-Time Protection.



> **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

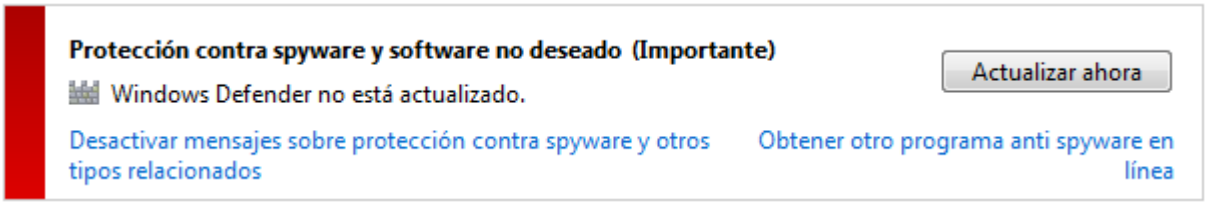
Recibirá el siguiente mensaje si acaba de instalar Avira o si por cualquier motivo el archivo de firmas de virus, el motor de análisis o los ficheros del programa de su producto Avira no se actualizaran automáticamente (p. ej., si actualiza una versión antigua de un sistema operativo de Windows, en el 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

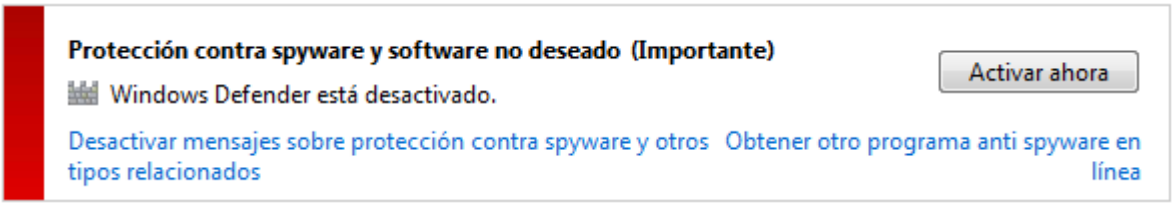
El siguiente mensaje puede aparecer si Windows Defender está activado. Esto podría significar que su producto Avira no se ha instalado correctamente. Compruebe esta posibilidad.



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.


Protección contra spyware y software no deseado (Importante)
Windows Defender está desactivado.
Activar ahora
Desactivar mensajes sobre protección contra spyware y otros tipos relacionados
Obtener otro programa anti spyware en línea

10. Virus y más

Avira Internet 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

10.1 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.

10.2 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.

11. Información y servicio

En este capítulo obtendrá información sobre cómo ponerse en contacto con nosotros.

- consulte el capítulo Dirección de contacto
- consulte el capítulo Soporte técnico
- consulte el capítulo Fichero sospechoso
- consulte el capítulo Notificar falsa alarma
- consulte el capítulo Sus comentarios para aumentar la seguridad

11.1 Dirección de contacto

Con mucho gusto atenderemos cualquier consulta o sugerencia en relación a los productos Avira. Encontrará nuestra dirección de contacto en el Centro de control en **Ayuda > Acerca de Avira Internet Security**.

11.2 Soporte técnico

El soporte técnico de Avira está siempre a su lado para resolver sus dudas y solventar cualquier problema técnico.

En nuestro sitio web podrá encontrar toda la información que necesite acerca de nuestro extenso servicio técnico:
http://www.avira.es/premium-suite-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 Internet Security > 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 Internet Security > 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 fichero de informes.

11.3 Fichero sospechoso

Puede enviarnos los ficheros y virus que nuestros productos no hayan podido detectar o eliminar. Para ello, le ofrecemos varias vías de contacto.

- Seleccione el fichero en el administrador de cuarentena del Centro de control y escoja la opción **Enviar fichero** a través del menú contextual o del botón correspondiente.
- Envíe el fichero seleccionado comprimido (WinZIP, PKZip, Arj, etc.) como adjunto de un correo electrónico a la siguiente dirección:
  virus-premium-suite@avira.es
  Dado que algunas puertas de enlace de correo electrónico trabajan con antivirus, debe enviar el fichero con una contraseña (no olvide facilitárnosla).
- Otra opción es enviarnos el fichero sospechoso a través de nuestro sitio web:
  http://www.avira.es/sample_upload

11.4 Notificar falsa alarma

Si piensa que su producto Avira ha detectado un fichero sospechoso que, con bastante probabilidad, está "limpio", comprima dicho fichero (WinZIP, PKZIP, Arj, etc.) y envíelo como adjunto de un correo electrónico a la siguiente dirección:
virus-premium-suite@avira.es

Dado que algunas puertas de enlace de correo electrónico trabajan con antivirus, debe enviar el fichero con una contraseña (no olvide facilitárnosla).

11.5 Sus comentarios para aumentar la seguridad

En Avira, la seguridad de nuestros clientes es nuestra máxima prioridad. Por ello, no nos limitamos únicamente a someter todas nuestras soluciones y actualizaciones a las más estrictas pruebas de calidad y seguridad llevadas a cabo por nuestro equipo de expertos. 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-premium-suite@avira.es

12. Referencia: Opciones de configuración

La referencia de la configuración documenta todas las opciones de configuración disponibles.

12.1 Scanner

La sección **Scanner** de la configuración sirve para configurar el análisis directo, es decir, el análisis a petición. (Opciones disponibles solo si el modo experto está activado.)

12.1.1 Análisis

Aquí puede definir el comportamiento básico de la rutina de búsqueda en el caso de un análisis directo (Opciones disponibles solo si el modo experto está activado). 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.

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.

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. (Opciones disponibles solo si el modo experto está activado.)

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 está seleccionada previamente por defecto la acción **Cuarentena** para tratar los virus. Puede seleccionar otras opciones mediante un menú contextual.

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.

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.

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. (Opciones disponibles solo si el modo experto está activado.)

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(Opciones disponibles solo si el modo experto está activado.)

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.

Heurística

Esta sección de configuración trata sobre la configuración de la heurística del motor de análisis. (Opciones disponibles solo si el modo experto está activado.)

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.

12.1.2 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. (Opciones disponibles solo si el modo experto está activado.)

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.

12.2 Real-Time Protection

La sección Real-Time Protection de la configuración sirve para configurar el análisis en tiempo real. (Opciones disponibles solo si el modo experto está activado.)

12.2.1 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. (Opciones disponibles solo si el modo experto está activado.)

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.

Modo de análisis

Aquí se define el momento en el que debe analizarse un fichero.

Analizar al leer

Si esta opción está activada, Real-Time Protection analiza los ficheros antes de que la aplicación o el sistema operativo los lea o ejecute.

Analizar al escribir

Si esta opción está activada, Real-Time Protection analiza el fichero al escribir. Solo puede acceder al fichero de nuevo cuando se haya completado el proceso.

Analizar al leer y escribir

Si esta opción está activada, Real-Time Protection analiza los ficheros antes de abrirlos, leerlos y ejecutarlos y después de escribirlos. Este ajuste está activado de forma estándar y es el recomendado.

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. (Opciones disponibles solo si el modo experto está activado.)

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).

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. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

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.

Heurística

Esta sección de configuración trata sobre la configuración de la heurística del motor de análisis. (Opciones disponibles solo si el modo experto está activado.)

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.

12.2.2 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. (Opciones disponibles solo si el modo experto está activado.)

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.

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.

12.3 Actualización

En la sección **Actualización** puede configurar la ejecución automática de las actualizaciones. Tiene la posibilidad de ajustar diferentes intervalos de actualización,.

Actualización automática

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. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

12.3.1 Servidor web

Servidor web

La actualización puede realizarse desde un servidor de web en Internet . (Opciones disponibles solo si el modo experto está activado.)

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.

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`

12.4 Backup

En **Configuración > Seguridad del PC > Backup** puede configurar el componente Backup. (Opciones disponibles solo si el modo experto está activado.)

12.4.1 Configuración

En **Configuración** puede establecer el comportamiento del componente Backup.

Solo copiar ficheros modificados

Si la opción está activada, se crea una copia de seguridad incremental: solo se hace una copia de seguridad de los ficheros del perfil de backup que hayan cambiado

desde la última copia de seguridad de los datos. Si está desactivada la opción, con cada copia de seguridad de un perfil de copia de seguridad se crea una copia de seguridad completa: se hace una copia de seguridad de todos los ficheros del perfil de copia de seguridad. Este ajuste está activado de forma estándar y se recomienda, puesto que las copias de seguridad incrementales son más rápidas y usan menos recursos que las copias de seguridad completas.

Antes de guardar analizar si es malware

Si está activada la opción, durante la copia de seguridad se analizan los ficheros que se incluirán en la copia de seguridad en busca de virus y malware. Los ficheros afectados no se incluyen en la copia de seguridad. Este ajuste está activado de forma estándar y se recomienda.

12.4.2 Excepciones

En **Excepciones** puede definir los ficheros y los tipos de fichero que se incluyen o no se incluyen al hacer una copia de seguridad.

Ficheros a excluir por el backup

La lista de esta ventana contiene ficheros y rutas que no se incluirán en la copia de seguridad durante la copia de seguridad.

> **Nota**
> La suma de las entradas de la lista no puede superar el máximo de 6000 caracteres.

> **Nota**
> Los ficheros incluidos en esta lista se anotan en el fichero de informe.

Campo de entrada

En este campo se introduce el nombre del fichero que no se incluirá en la copia de seguridad. De forma estándar consta la ruta del directorio temporal para la configuración local del usuario que ha iniciado sesión.

El botón abre una ventana en la que puede seleccionar el fichero o la ruta pertinente. Si ha introducido un nombre de fichero con ruta completa, no se incluirá en la copia de seguridad exactamente ese fichero. Si ha introducido un nombre de fichero sin ruta, todo fichero con ese nombre no se incluirá en la copia de seguridad (indistintamente de la ruta o la unidad en que se encuentre).

Añadir

Este botón permite incluir en la ventana de visualización 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.

Restablecer lista

Este botón restablece los valores estándar predefinidos.

Tenga en cuenta los siguientes puntos:

- Los comodines * (varios caracteres) y ? (un único carácter) solo están permitidos en los nombres de ficheros.
- La lista se procesa de arriba a abajo.
- Si se excluye un directorio, todos sus subdirectorios se excluyen automáticamente.
- También se pueden excluir extensiones de fichero por separado (incluidos los comodines).
- Para excluir objetos a los que se tiene acceso con nombres de fichero DOS cortos (convención de nombres DOS 8.3), el nombre de fichero en cuestión también debe incluirse en la lista.

Nota
Un nombre de fichero que contenga un comodín no puede acabar con una barra diagonal inversa. Por ejemplo:
`C:\Archivos de programa\Aplicación\Aplic*.exe\`
Esta entrada no es válida y no se trata como una excepcion.

Ejemplos

- `aplicación.exe`
- `\Archivos de programa\`
- `C:\*.*`
- `C:\*`
- `*.exe`
- `*.xl?`
- `*.*`
- `C:\Archivos de programa\Aplicación\aplicación.exe`
- `C:\Archivos de programa\Aplicación\aplic*.exe`
- `C:\Archivos de programa\Aplicación\aplic*`
- `C:\Archivos de programa\Aplicación\aplic????.e*`

- `C:\Archivos de programa\`
- `C:\Archivos de programa`
- `C:\Archivos de programa\Aplicación\*.mdb`

Listas de extensiones de fichero

Considerar todas las extensiones de fichero

Si está activada la opción, se hace una copia de seguridad de todos los ficheros del perfil de copia de seguridad.

Activar la lista de extensiones de fichero omitidas

Si está activada la opción, se incluyen todos los ficheros del perfil de copia de seguridad en la copia de seguridad, a excepción de los ficheros cuyas extensiones de fichero se incluyeron en la lista de extensiones de fichero omitidas.

Extensiones de fichero

Con este botón se abre un cuadro de diálogo que muestra todas las extensiones de fichero que no se incluirán en la copia de seguridad en el caso de una copia de seguridad con la opción activada **Activar la lista de extensiones de fichero omitidas**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Activar la lista de extensiones de fichero consideradas

Si está activada la opción, solo se incluyen los ficheros en la copia de seguridad, cuyas extensiones de fichero se introdujeron en la lista de extensiones de fichero consideradas.

Extensiones de fichero

Con este botón se abre un cuadro de diálogo que muestra todas las extensiones de fichero que no se incluirán en la copia de seguridad en el caso de una copia de seguridad con la opción activada **Activar la lista de extensiones de fichero consideradas**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

12.4.3 Informe

El componente Backup dispone de una amplia función de registro.

Registro

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Si está activada la opción, el componente Backup no crea ningún registro. Renuncie a realizar el registro sólo en casos excepcionales.

Predeterminado

Si está activada la opción, el componente Backup incluye información importante (sobre la copia de seguridad, detecciones de virus, advertencias y errores) en el fichero de informe; la información menos relevante se omite para mayor claridad. Este ajuste está activado de forma estándar.

Extendido

Si la opción está activada, el componente Backup incluye también la información de menor importancia en el fichero de informe.

Completo

Si la opción está activada, el componente Backup incluye toda la información acerca del proceso de backup y del análisis de virus en el fichero de informe.

12.5 FireWall

12.5.1 Configurar el FireWall

Avira Internet Security le permite configurar Avira FireWall:

- Avira FireWall

12.5.2 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. (Opciones disponibles solo si el modo experto está activado.)

- 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.

- Para cambiar a la configuración avanzada de las reglas de aplicación, debe activar primero el **Modo experto**.
- 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. (Opciones disponibles solo si el modo experto está activado.)
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. (Opciones disponibles solo si el modo experto está activado.)

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

Opciones disponibles solo si el modo experto está activado.

Configuración avanzada

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

Opciones disponibles solo si el modo experto está activado.

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.

12.6 Web Protection

La sección **Web Protection** en **Configuración > Seguridad en Internet** sirve para configurar Web Protection.

12.6.1 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. (Opciones disponibles solo si el modo experto está activado.)

Análisis

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. (Opciones disponibles solo si el modo experto está activado.)

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.

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.

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. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

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.

12.6.2 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.

12.7 Mail Protection

La sección Mail Protection de la configuración sirve para configurar Mail Protection.

12.7.1 Análisis

Mail Protection se usa para analizar los correos electrónicos entrantes en cuanto a la presencia de virus, malware y correo no solicitado. 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.

Analizar emails entrantes

Si esta opción está activada, los correos electrónicos entrantes se analizan en cuanto a la presencia de virus y malware, así como el correo no solicitado. 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. (Opciones disponibles solo si el modo experto está activado.)

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de POP3. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de IMAP. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de SMTP. (Opciones disponibles solo si el modo experto está activado.)

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 solo disponible con el modo experto activado y no 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. (Opciones disponibles solo si el modo experto está activado.)

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**.

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. (Opciones disponibles solo si el modo experto está activado.)

> **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. (Opciones disponibles solo si el modo experto está activado.)

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. (Opciones disponibles solo si el modo experto está activado.)

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.

12.7.2 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.

> **Nota**
> Al introducir direcciones de correo electrónico, puede utilizar comodines: el comodín ***** para varios caracteres y el comodín **?** para un solo carácter. Sin embargo, los comodines solo pueden utilizarse con aquellas direcciones de correo electrónico que no deban analizarse en cuanto a correo no solicitado. Por esta razón, se emite un mensaje de error si intenta excluir una dirección con comodines del análisis de malware activando la casilla de verificación **Malware** en la lista de exclusiones. Cuando introduzca direcciones con comodines, tenga en cuenta que la secuencia de caracteres indicada debe coincidir con la estructura de una dirección de correo electrónico (*@*.*)

Advertencia
Al utilizar comodines, tenga en cuenta los ejemplos que se indican. Utilice los comodines solo en casos concretos y compruebe rigurosamente qué direcciones de correo electrónico va a incorporar a la lista blanca de correo no solicitado si indica comodines.

Ejemplos: empleo de comodines en las direcciones de correo electrónico (lista blanca de correo no solicitado).

- `virus@avira.* /` = engloba todos los correos electrónicos con esta dirección y el dominio de nivel principal deseado: virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = engloba todos los correos electrónicos enviados por el dominio **avira.com**: info@avira.com, virus@avira.com, kontakt@avira.com, mitarbeiter@avira.com
- `info@*.com` = engloba todas las direcciones de correo electrónico con el dominio de nivel principal **com** y la dirección **info**: el dominio de nivel secundario puede ser cualquiera: info@nombre1.com, info@nombre2.com,...

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.

Spam

Si esta opción está activada, no se vuelve a analizar la dirección de correo electrónico para detectar correo no solicitado.

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.

Importar libreta de direcciones de Outlook

Este botón permite importar las direcciones de correo electrónico de la libreta de direcciones del programa de correo MS Outlook a la lista de excepciones. No se analiza la presencia de correo no solicitado en las direcciones de correo electrónico importadas.

Importar libreta de direcciones de Outlook Express (Windows XP) / Importar libreta de direcciones de correo de Windows (Windows Vista, Windows 7)

Este botón permite importar las direcciones de correo electrónico de la libreta de direcciones del programa de correo MS Outlook Express a la lista de excepciones. No se analiza la presencia de correo no solicitado en las direcciones de correo electrónico importadas.

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**. (Opciones disponibles solo si el modo experto está activado.)

También se depositan en la memoria caché copias de los correos electrónicos recibidos. Los correos electrónicos se utilizan para las funciones de aprendizaje (*Email legítimo – utilizar para aprendizaje*, *Email no solicitado – utilizar para aprendizaje*) del módulo AntiSpam.

> **Nota**
> El módulo AntiSpam debe estar activado para que los correos electrónicos recibidos se guarden en la memoria caché.

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. (Opciones disponibles solo si el modo experto está activado.)

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.

AntiSpam

Mail Protection de Avira comprueba en los correos electrónicos la presencia de virus y programas no deseados. Además, puede protegerlo contra el correo no solicitado. (Opciones disponibles solo si el modo experto está activado.)

Activar el módulo AntiSpam

Si esta opción está activada, la función AntiSpam de Mail Protection no está activada.

Marcar el asunto del email

Si esta opción está activada, si se detecta un correo electrónico no solicitado, se añade una nota al asunto original para marcarlo como tal.

Simple

Se añade [SPAM] o [Phising] al asunto de los correos electrónicos detectados como tales. Esta opción está activada de forma estándar.

Detallado

Se añade una nota en el asunto indicando la probabilidad de suplantación de identidad en el caso de detectarse correo no solicitado o suplantación de identidad.

Registrar

Si esta opción está activada, Mail Protection genera un fichero de informe especial AntiSpam.

Usar listas negras (RBL) en tiempo real

Si esta opción está activada, se consulta la llamada "lista negra", la cual proporciona información adicional para clasificar los correos electrónicos de origen dudoso como correos no solicitados.

Time-out: n segundo(s)

Si la información de la lista negra no está disponible después de n segundos, se cancela la consulta a la lista.

Eliminar base de datos de aprendizaje

Al pulsar el botón, se elimina la base de datos de aprendizaje.

Añadir destinatarios de correo saliente automáticamente a la lista blanca

Si esta opción está activada, las direcciones de los destinatarios de los correos electrónicos salientes se incorporan automáticamente a la lista blanca de correo no solicitado (lista de correos electrónicos que no se analizan en cuanto a correo no solicitado, en **Mail Protection > General > Excepciones**). Los correos electrónicos entrantes enviados desde las direcciones que constan en la lista blanca no se analizan en cuanto a correo no solicitado. Se continúa analizando la presencia de virus y malware. Esta opción está desactivada de forma estándar.

Nota
Esta opción 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).

12.7.3 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.

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.

12.8 Protección infantil

Haga uso de las funciones de Avira *PROTECCIÓN INFANTIL* para garantizar una experiencia segura en Internet tanto para sus hijos como para cualquier persona que utilice su ordenador.

- Mediante la función **Safe Browsing** puede asignar roles de usuario a los usuarios de Windows de su equipo. Para cada rol, puede especificar qué direcciones URL y categorías de contenido están permitidas y cuáles prohibidas, y establecer el tiempo máximo de disfrute de Internet y los horarios concretos para navegar por la red.

Temas relacionados:

- Qué es Safe Browsing

12.8.1 Safe Browsing

Su programa Avira ofrece la función **Safe Browsing** para filtrar los contenidos de Internet no deseados o ilegales, así como para limitar el tiempo de navegación. La función **Safe Browsing** forma parte del componente *PROTECCIÓN INFANTIL*.

Es posible asignar funciones de usuario a los usuarios del equipo. Puede configurar una función de usuario, que comprende un conjunto de reglas con los siguientes criterios:

- Direcciones URL prohibidas o permitidas (direcciones de Internet)
- Categorías de contenido prohibidas
- Tiempo de uso de Internet y, eventualmente, horarios de uso permitidos según el día de la semana

Para poder bloquear contenidos de Internet según determinadas categorías, se utilizan extensas listas de filtros de direcciones URL en las que estas se clasifican en categorías de contenido en función del contenido de los sitios Web. Las listas de filtros de URL se actualizan, adaptan y amplían varias veces por hora. Las funciones **Infantil**, **Juvenil** y **Adulto** vienen preconfiguradas con las categorías prohibidas correspondientes.

El uso temporal de Internet se registra según las consultas de Internet que se realizan en un intervalo mínimo de 5 minutos.

Si la función **Safe Browsing** está activa, durante la navegación por Internet se cotejan todos los sitios web a los que accede el navegador con la función de usuario. Si se trata de un sitio web prohibido, este será bloqueado y aparecerá un mensaje en el navegador. Si se supera el tiempo de uso máximo permitido, o si se intenta navegar fuera del horario estipulado, todos los sitios web serán bloqueados. Se mostrará asimismo un mensaje en el navegador.

Advertencia
Tenga en cuenta que debe activar el servicio "**Web Protection**" para poder utilizar la función "**Safe Browsing**".

Advertencia
Proteja la configuración de su producto Avira mediante una contraseña una vez que haya activado la función **Safe Browsing**. Si la configuración no está protegida con contraseña, cualquier usuario del equipo puede modificar o desactivar los ajustes de **Safe Browsing** . Puede activar la protección con contraseña en Configuración > General > Contraseña.

Temas relacionados:

- Activar Safe Browsing
- Asignar una función
- Configuración de Safe Browsing

Activar Safe Browsing

- Abra el centro de control de Avira y haga clic en **Estado** en la barra de navegación.

  Debe activar **Web Protection** para poder usar la función **Safe Browsing**.
- Si está desactivado, active **Web Protection** en la vista **Estado** en *Seguridad en Internet*. Para ello, haga clic en el interruptor rojo junto a **Web Protection**.

  Cuando está activado, el interruptor junto a **Web Protection** es de color verde ("ACTIVADO").

  Active la función **Safe Browsing** en la vista **Estado** haciendo clic en el interruptor rojo junto a **Safe Browsing**.

  Cuando está activado, el interruptor junto a Safe Browsing es de color verde ("ACTIVADO").
- Para configurar el rol de un niño o de cualquier otra persona en **Safe Browsing**, en la vista **Estado** haga clic en el botón de configuración junto a **Safe Browsing**.

Temas relacionados:

- Qué es Safe Browsing

- Asignar una función
- Configuración de Safe Browsing

Asignar una función

Requisitos:

✓ Asegúrese de crear una cuenta de usuario de Windows propia para cada persona que utiliza su ordenador. En su producto Avira, puede asignar un rol de Safe Browsing a cada una de estas cuentas.
✓ Active la función **Safe Browsing** en su producto Avira.
✓ Compruebe las propiedades de cada rol antes de asignarlos a los usuarios.

▸ En la vista **Estado**, haga clic en el botón de configuración situado junto a **Safe Browsing**.

▸ Seleccione de la lista **Selección de usuario** el usuario al que desea asignar un rol.

Esta lista contiene las cuentas de usuario de Windows que se han creado en su equipo.

▸ Haga clic en **Añadir**.

↪ Se añade el usuario a la lista.

En Avira Internet Security existen los siguientes roles de usuario preconfigurados:

- **Infantil**
- **Joven**
- **Adulto**

Al añadir una cuenta de usuario a la lista, se asigna por defecto el rol **Infantil**.

▸ Puede asignar otro rol haciendo clic varias veces en el rol del usuario.

Nota
A los usuarios del equipo que no tengan asignados ningún rol en la configuración de la función **Safe Browsing**, el programa les asignará por defecto el usuario **Predeterminado** con el rol **Infantil**. También puede modificar el rol del usuario **Predeterminado**.

▸ Haga clic en **Aplicar** para guardar la configuración.

Temas relacionados:

- Modificar las propiedades de una función
- Añadir y borrar una función

Modificar las propiedades de una función

▸ En la vista **Estado**, haga clic en el botón de configuración situado junto a **Safe Browsing**.

- Si no está activo, haga clic en el interruptor verde junto a **Modo experto**.

  Cuando está activado, el interruptor junto a **Modo experto** es de color amarillo ("ACTIVADO").

  ↪ Las opciones de **Funciones** se muestran en la ventana de configuración de la función **Safe Browsing**.

- Haga clic en el nombre de la función que desee modificar (por ejemplo, **Juvenil**) y, a continuación, haga clic en **Cambiar**.

  ↪ Aparecerá la ventana con las **Propiedades** de la función.

- Realice los cambios que desee y, después, haga clic en **Aceptar**.

Temas relacionados:

- Propiedades de la función
- Configuración de Safe Browsing

Añadir y borrar una función

- En la vista **Estado**, haga clic en el botón de configuración situado junto a **Safe Browsing**.
- Si no está activo, haga clic en el interruptor verde junto a **Modo experto**.

  Cuando está activado, el interruptor junto a **Modo experto** es de color amarillo ("ACTIVADO").

  ↪ Las opciones de **Funciones** se muestran en la ventana de configuración de la función **Safe Browsing**.

- Para borrar una función (por ejemplo, **Joven**), haga clic en **Eliminar**.

> **Nota**
> No podrá borrar una función si existe algún usuario que la tenga asignada.

- Para añadir una función, introduzca el nombre de la función (máximo 30 caracteres) en el campo de entrada y haga clic en **Añadir**.
- Para ajustar las propiedades de la nueva función, seleccione esta de la lista y haga clic en **Cambiar**.

Temas relacionados:

- Configuración de Safe Browsing
- Propiedades de la función
- Asignar una función

Si ha asignado una contraseña para la función **Safe Browsing**, se oculta la configuración de **Safe Browsing** y se muestra el botón **Protegido por contraseña**.

Protegido por contraseña

Haga clic en el botón "**Protegido por contraseña**" e introduzca la contraseña para "**Safe Browsing**" en la ventana "**Introducir contraseña**" para activar la configuración de **Safe Browsing**.

Activar Safe Browsing

Si esta opción está activada, todas las páginas web que se solicitan al navegar en Internet, se comprueban según la función que se ha asignado al usuario conectado en **Safe Browsing**. Las páginas web solicitadas se bloquean si se han clasificado como prohibidas en la función asignada.

Nota
Si **Safe Browsing** está activado, el programa concede por defecto a los usuarios del equipo a los que no se les ha asignado ninguna función en la configuración de la función **Safe Browsing** el usuario *Predeterminado* con la función **Infantil**. Puede modificar la función del usuario estándar.
Tras la instalación, se crean las funciones de usuario **Infantil**, **Juvenil** y **Adulto**. En las funciones preconfiguradas, la limitación temporal del uso de Internet está desactivada.

Selección de usuario

Usuario

La lista contiene todos los usuarios del sistema.

Añadir

Con este botón puede añadir el usuario seleccionado a la lista de los usuarios protegidos.

Eliminar

Este botón elimina una entrada seleccionada en la lista.

Lista "Usuario - Función"

En la lista se muestran todos los usuarios añadidos con la función que se ha asignado al usuario. Cuando se añade un usuario, el programa asigna por defecto la función **Infantil**. Si se hace clic con el ratón en la función mostrada, tiene la posibilidad de cambiar la función.

Nota
El usuario *Predeterminado* no puede borrarse.

Funciones (Opciones disponibles solo si el modo experto está activado.)

Campo de entrada

En este campo puede introducir el nombre de la función que quiere añadir a las funciones de usuario.

Cambiar

Mediante el botón "**Cambiar**" puede configurar la función seleccionada. Aparece un cuadro de diálogo en el que puede definir las URL prohibidas y permitidas para la función, así como seleccionar por categoría el contenido prohibido de las web. (Véase Propiedades de la función.)

Añadir

Con este botón puede añadir la función introducida en el campo de entrada a la lista de las funciones disponibles.

Eliminar

Este botón elimina una función marcada en la lista.

Lista

La lista muestra todas las funciones incorporadas. Si se hace doble clic en una función mostrada, puede abrir el cuadro de diálogo para definir la función.

Nota
No se pueden eliminar las funciones que ya se han asigando a un usuario.

Temas relacionados:

- Qué es Safe Browsing
- Propiedades de la función
- Duración del uso
- Período de uso

Propiedades de la función

En la ventana **Propiedades de la función** tiene la posibilidad de definir una función seleccionada para el uso de Internet. (Opciones disponibles solo si el modo experto está activado.)

Puede permitir o prohibir de forma explícita el acceso a diferentes URLs. Es posible bloquear determinadas categorías de contenido web en función de la selección. Tiene la posibilidad de limitar temporalmente el uso de Internet.

Controlar el acceso a las siguientes URLs

En la lista se muestran todas las URLs incorporadas con las reglas asignadas *Bloquear* o *Permitir*. Al añadir una URL, se asigna por defecto la regla *Bloquear*. Cuando se hace clic en ella, puede modificar la regla asignada.

Añadir URL

En este campo puede indicar las URLs que la función Protección infantil debe controlar. 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 oder .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). También puede utilizar el comodín ***** para varios caracteres. Utilice también los puntos de inicio o final, junto con los comodines, para identificar los niveles del dominio.

Nota
Se designa la prioridad de las reglas de las URLs en función del número de partes del nombre introducidas (etiquetas) del dominio. Cuantas más partes del nombre del dominio se introducen, mayor es la prioridad de las reglas. Ejemplo:
URL: www.avira.com - Regla: Permitir
URL: .avira.com - Regla: Bloquear
El conjunto de reglas permite todas las URLs del dominio 'www.avira.com'. Se bloquea la URL 'forum.avira.com'.

Nota
Los caracteres . o * engloban todas las URLs. Utilice estos caracteres si, por ejemplo, solo quiere autorizar para la función *Infantil* algunas páginas web indicadas de forma explícita, como p. ej., en el siguiente conjunto de reglas:
URL: ***** o **.** - Regla: Bloquear
URL: kids.yahoo.com - Regla: Permitir
URL: kids.nationalgeographic.com - Regla: Permitir
El conjunto de reglas bloquea todas las URLs con la excepción de las URLs con los dominios 'kids.yahoo.com' y 'kids.nationalgeographic.com'.

Añadir

Con este botón puede añadir la URL introducida a la lista de las URLs controladas.

Eliminar

Este botón elimina una URL marcada de la lista de las URLs controladas.

Se bloquea el acceso a las URLs de las siguientes categorías:

Si esta opción está activada, se bloquea el contenido de la página web que se encuentra entre las categorías seleccionadas en la lista de la categoría.

Duración de uso permitida

Con el botón **Duración de uso permitida** puede abrir un cuadro de diálogo en el que puede ajustar una limitación temporal del uso de Internet para la función que va a configurar. Tiene la posibilidad de determinar el uso de Internet por mes, semana o de forma diferenciada según los días de la semana y los días del fin de semana. En otro cuadro de diálogo es posible determinar los períodos de uso exactos por día de la semana. Véase Duración del uso.

Ejemplos: URL que deben controlarse

- `www.avira.com` -O- `www.avira.com/*`
  = engloba todas las URLs 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*,...
  No se incluyen las URLs con el dominio www.avira.de.
- `avira.com` -O- `*.avira.com`
  = engloba todas las URLs 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.*`
  = engloba todas las URLs 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*.*`
  Engloba todas las URLs 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`
  = engloba todas las URLs con el dominio de nivel principal '`net`' : *www.nombre1.net*, *www.nombre2.net*,...

Temas relacionados:

- Qué es Safe Browsing
- Configuración de Safe Browsing
- Duración del uso
- Período de uso

Duración del uso

En la ventana **Duración del uso** tiene la posibilidad de definir la duración máxima del uso de Internet para una función de usuario. El uso temporal de Internet se registra según las consultas de Internet que se realizan en un intervalo mínimo de 5 minutos. El tiempo de navegación máximo deseado para una función se puede determinar por semana, mes o de forma diferenciada según los días de la semana y los días del fin de semana.

Limitar el horario de uso de Internet

Con esta opción limita la duración de uso de Internet para todos los usuarios del equipo a los que se han asignado la función. Si se supera la duración de uso permitida, se bloquean páginas web que el usuario del equipo solicita, es decir, a las que accede. En el explorador web, aparece un mensaje de advertencia.

Limitaciones de horario por semana, mes, día (L-V, S-D)

La duración del uso deseada se puede introducir mediante la barra deslizante o mediante las teclas de flecha situadas a la derecha junto a los campos de entrada. Asimismo, puede introducir la duración del uso directamente en los campos de tiempo. Tenga en cuenta el formato indicado para introducir el tiempo.

El programa no compara los diferentes datos sobre la duración del uso. El programa utiliza el valor inferior correspondiente para limitar la duración del uso.

Período de uso exacto

Mediante el botón **Período de uso exacto** accede a un cuadro de diálogo en el que puede determinar las horas del día para la duración de uso máxima definida. Véase Período de uso.

Temas relacionados:

- Qué es Safe Browsing
- Configuración de Safe Browsing
- Propiedades de la función
- Período de uso

Período de uso

En la ventana **Período de uso** define los períodos de uso permitidos para la duración máxima de uso de Internet indicada de la función: puede autorizar horas del día determinadas por día de la semana para el uso de Internet.

Permitir uso de Internet solo a las horas indicadas

Con esta opción define las horas del día para "navegar" para todos los usuarios del equipo a los que se han asignado la función configurada. Si los usuarios del equipo de la función utilizan Internet fuera de las horas del día autorizadas, se bloquean las páginas web solicitadas. En el explorador web, aparece un mensaje.

- Para autorizar las horas del día para el uso de Internet, marque los períodos de tiempo deseados.

  Existen las siguientes posibilidades para marcar las horas del día autorizadas o bloqueadas:

  - **Para autorizar las horas del día para el uso de Internet:** haga clic en los campos de tiempo no marcados que desee o arrastre el botón izquierdo del ratón sobre los campos de tiempo no marcados.

- **Para bloquear las horas del día para el uso de Internet:** haga clic en los campos de tiempo marcados que desee o arrastre el botón izquierdo del ratón sobre los campos de tiempo marcados.

Haga clic con el botón derecho del ratón en los campos de tiempo del día deseado para mostrar en un cuadro de diálogo los períodos de tiempo indicados. Ejemplo: *uso de Internet bloqueado desde las 00:00 hasta las 11:00.*

Temas relacionados:

- Qué es Safe Browsing
- Configuración de Safe Browsing
- Propiedades de la función
- Duración del uso

12.9 Protección móvil

Avira protege no solo su ordenador frente al malware y los virus, sino también los móviles y smartphones que funcionan con el sistema operativo Android frente a robos o pérdida. Con ayuda de las listas negras de Avira Free Android Security puede además bloquear las llamadas y los SMS no deseados. Solo tiene que añadir a la lista negra los números de teléfono del registro de llamadas, la lista de mensajes o sus contactos o crear manualmente los contactos que quiere bloquear.

Encontrará más información en nuestro sitio web:

http://www.avira.es/android

12.9.1 Android Security

Avira Free Android Security

Avira Free Android Security consta de dos componentes:

- La aplicación en sí misma, que se instala en el dispositivo Android.
- La Consola Web de Android de Avira, que sirve para registrar y controlar las funciones.

Requisitos del sistema

Sistema operativo:

- Android 2.2 (Froyo)
- Android 2.3.7 (Gingerbread)
- Android 4.0.x (Ice Cream Sandwich)
- Android 4.1.x (Jelly Bean)

Memoria RAM:

- 1,28 MB de memoria RAM libre.

Navegador:

- Mozilla Firefox
- Google Chrome
- Opera
- Internet Explorer IE7 o superior.

> **Nota**
> Java debe estar instalado y activado y es necesaria una conexión a Internet que funcione.

Servicios

En el caso de que no pueda encontrar su dispositivo, Avira Free Android Security ofrece a través de la Consola Web de Avira cuatro funciones para proteger sus datos personales:

Alerta remota

Puede iniciar en el dispositivo una alarma de 20 segundos.

Determinación remota de la ubicación

Activa un comando de posición que determina los parámetros de la ubicación del dispositivo.

Bloqueo remoto

Puede bloquear el dispositivo de inmediato usando un PIN de cuatro números.

Borrado remoto

Puede quitar datos de la tarjeta SIM o de tarjetas de memoria internas y externas. Mediante la Consola Web puede restablecer el dispositivo a los valores de fábrica.

> **Nota**
> Para iniciar el comando **Restablecimiento remoto a valores de fábrica** para borrar todos las datos tras la pérdida o el robo del dispositivo, tiene que activar la opción **Administrador de dispositivos** durante la configuración.

La función de la lista negra de Avira Free Android Security le permite bloquear las llamadas y los SMS no deseados.

Lista negra

Puede añadir a la lista negra los contactos del registro de llamadas, la lista de mensajes o sus contactos o crear manualmente los contactos que quiere bloquear.

La Consola Web

La Consola Web de Avira es una aplicación basada en navegador para controlar las funciones de seguridad. En el Panel de la Consola Web puede administrar su cuenta e iniciar funciones remotas, como **Ubicar**, **Bloquear**, **Iniciar alerta** o **Borrar**.

La Consola Web de Avira incluye una barra de título, una barra lateral y la pantalla principal con varias pestañas. En la barra de título se muestran sus datos de acceso y enlaces al Soporte y la administración de la cuenta. En la barra lateral se muestran los dispositivos registrados. En la pantalla principal de la Consola Web puede encontrar todas las funciones de seguridad de la aplicación, así como información sobre la función de la **lista negra** en su dispositivo.

La barra de títulos de la consola Web

Detalles de la cuenta

En la barra de título se muestran los enlaces al **Soporte** de Avira, su **Cuenta**, para **Cerrar sesión** y sus datos de acceso.

- Haga clic en el enlace **Cuenta**.
  - ↪ Se abre la ventana **Detalles de la cuenta** en la que se muestran los campos siguientes:

Fecha de creación

Indica la fecha y la hora en la que ha registrado la cuenta.

Nombre

Aquí puede introducir su nombre.

Apellidos

Aquí puede introducir sus apellidos.

Idioma

Seleccione el idioma deseado en el menú desplegable.

Provincia

Seleccione la provincia deseada en el menú desplegable.

Tipo de cuenta

Indica el tipo de cuenta que utiliza.

Guardar cambios

- Haga clic en **Guardar cambios** para guardar las modificaciones en los datos de la cuenta.

Administrador de contraseñas

La barra de título de la Consola Web de Avira contiene el enlace a su **Cuenta**, donde puede administrar su contraseña.

- Haga clic en el enlace **Cuenta**.
  - ↪ Se abre la ventana **Administrador de contraseñas** en la que se muestran los campos siguientes:

Contraseña

Introduzca una contraseña nueva para su cuenta de Avira Free Android Security.

Confirmación de la contraseña

Vuelva a introducir la contraseña para confirmarla.

Cambiar contraseña

- Haga clic en el botón para guardar los cambios realizados.

Seguridad de la cuenta

La barra de título de la Consola Web de Avira contiene el enlace a su **Cuenta**, donde puede definir una pregunta de seguridad, que sirve para proteger aún más su cuenta. Si ha olvidado los datos de acceso o quiere modificar su dirección de correo electrónico, puede identificarse con ayuda de la pregunta de seguridad.

- Haga clic en el enlace **Cuenta**.
  - ↪ Se abre la ventana **Seguridad de la cuenta** en la que se muestran los campos siguientes:

Pregunta de seguridad

Se abre el menú desplegable con las preguntas de seguridad para que seleccione la que solo usted puede responder. Seleccione la pregunta que encaje con usted.

Respuesta

- Introduzca la respuesta en el campo.
- Asegúrese de que no se ha equivocado al escribir la respuesta y que puede memorizarla fácilmente.

Guardar cambios

- Haga clic en el botón para guardar los cambios realizados.Haga clic en Guardar cambios para guardar la pregunta de seguridad y la respuesta.

Administración de dispositivos

La barra de título de la Consola Web de Avira contiene el enlace a su **Cuenta**, donde puede administrar su dispositivo.

↪ Haga clic en el enlace **Cuenta**.

↪ Se abre la ventana **Administración de dispositivos** en la que se muestran los campos siguientes:

Dispositivos disponibles

Abra el menú desplegable para seleccionar un dispositivo.

Borrar dispositivo

- Haga clic en el botón para borrar de su cuenta el dispositivo seleccionado.

Procedimientos

¿Cómo modifico mi dirección de correo electrónico?

Póngase en contacto con el Soporte de Avira si tiene que cambiar su dirección de correo electrónico. Esta dirección de correo electrónico sirve tanto para ponernos en contacto con usted como para identificarlo como usuario. Por lo tanto, no puede cambiar su dirección de correo electrónico por su cuenta con la Consola Web o en una aplicación del dispositivo.

¿Cómo puede proteger los datos guardados en mi dispositivo?

La opción más sencilla y rápida para proteger los datos guardados en su dispositivo es bloquear el dispositivo.

- Conéctese a la Consola Web.
- Vaya a la pestaña **Bloquear**.
- Introduzca un PIN de cuatro cifras.
- Confirme el PIN.
- Haga clic en **Bloquear**.

↪ El PIN puede utilizarse ahora para bloquear y desbloquear el dispositivo.

Nota
El PIN solo es válido temporalmente. Para cada comando para bloquear/desbloquear, es necesario un PIN nuevo.

¿Cómo desbloqueo mi dispositivo si me he olvidado del PIN o he introducido tres veces un PIN incorrecto?

En este caso, tiene que iniciar sesión en la Consola Web y modificar su PIN.

- Conéctese a la Consola Web.
- Vaya a la pestaña **Bloquear**.
- Introduzca un PIN de cuatro cifras.
- Confirme el PIN.
- Haga clic en **Bloquear**.
  - ↪ El PIN puede utilizarse ahora para bloquear y desbloquear el dispositivo.

¿Cómo modifico mi PIN?

Solo puede cambiar su PIN en la Consola Web. No es posible modificarlo en la aplicación.

- Conéctese a la Consola Web.
- Vaya a la pestaña **Bloquear**.
- Introduzca un PIN de cuatro cifras.
- Confirme el PIN.
- Haga clic en **Bloquear**.
  - ↪ El PIN puede utilizarse ahora para bloquear y desbloquear el dispositivo.

¿Cómo encuentro mi dispositivo si lo he perdido o me lo han robado?

Si ha perdido o le han robado su dispositivo, Avira Free Android Security dispone de dos opciones para recuperarlo:

Inicio de una alerta

Gracias a la función **Iniciar alerta** le resultará más sencillo encontrar el dispositivo. Es especialmente útil si lo ha perdido en un lugar muy cercano, p. ej., en su casa.

- Inicie sesión en la Consola Web.
- Seleccione la pestaña **Alerta** y haga clic en **Iniciar alerta**.
  - ↪ El dispositivo emite durante 20 segundos un sonido fuerte para que sea más sencillo encontrarlo. La alerta dura 20 segundos, durante los cuales no es

posible apagarla ni interrumpirla. La alerta se emite aunque el dispositivo esté en silencio.

Nota
Si el dispositivo está apagado o la batería está descargada, no se emite la alerta.

Búsqueda del dispositivo

Si no sabe dónde ha perdido el dispositivo o sospecha que se lo pueden haber robado, puede localizar la ubicación del dispositivo.

Nota
El seguimiento de ubicación dura hasta 3 minutos. Durante la localización de un dispositivo, no puede volver a iniciar el comando **Ubicar**. Sin embargo, puede iniciar el comando **Ubicar** para otro dispositivo registrado en su cuenta.

- Inicie sesión en la Consola Web.
- Seleccione la pestaña **Ubicar**.
  - ↪ En la Consola Web de Avira se muestra una sección de Google Maps.
- Haga clic debajo del mapa mostrado en **Ubicar**.
  - ↪ Durante el seguimiento de ubicación se muestra el tiempo transcurrido. La ubicación exacta del dispositivo se muestra en el mapa. Los datos geofísicos se muestran en grados de latitud y longitud.

¿Cómo registro un dispositivo nuevo?

Puede añadir hasta 5 dispositivos a su cuenta. Todos los dispositivos añadidos mediante la aplicación a la misma cuenta de Google o a la misma dirección de correo electrónico se registran en la misma cuenta de Avira Free Android Security, es decir, una cuenta de correo electrónico dispone de una cuenta de Avira Free Android Security con hasta 5 dispositivos diferentes.

- Utilice el dispositivo que quiere añadir a su cuenta para descargar Avira Free Android Security.
- Instale la aplicación en el dispositivo.
- Seleccione la cuenta de Google o introduzca otra dirección de correo electrónico y toque **Aceptar contrato de licencia y continuar**.
  - ↪ Recibirá un correo electrónico en la dirección en la que se ha confirmado el registro de un dispositivo nuevo para su cuenta existente de Avira Free Android Security.
  - ↪ Si inicia sesión en la Consola Web, el dispositivo nuevo ya está añadido en el área **Todos los dispositivos** situada a la derecha de la Consola Web.

- Ahora puede hacer clic en la pestaña "Dispositivo" en **Editar** para introducir la configuración para cambiar el nombre del dispositivo y el número de teléfono.

Nota
Dado que solo se pueden añadir 5 dispositivos a una cuenta de Avira Free Android Security, tiene que borrar la aplicación de un dispositivo registrado antes de poder añadir otro. Como opción, también puede seleccionar un dispositivo en la lista desplegable en la configuración de la **Cuenta** en la Consola Web en **Administración de dispositivos** y hacer clic en **Borrar dispositivo**.

Solución de problemas

Solución de problemas

Mensajes de error

Mensajes	Descripción
Establezca una conexión con una red móvil o Wi-Fi para continuar.	Durante el registro, no se ha encontrado ninguna conexión a la red. Active una conexión a la red para continuar.
El servicio no está disponible actualmente. Vuelva a intentarlo más tarde.	El servicio de Google no está disponible actualmente.
Avira Free Android Security está bloqueado. Escriba aquí para ayudarnos a resolver el error.	Se ha producido un error inesperado, por lo que se ha tenido que detener la aplicación. Al tocar aquí, nos transmite automáticamente el protocolo del error.
Para registrar el dispositivo, necesita una cuenta de Google. Cree una cuenta y vuelva a intentarlo.	No se ha encontrado ninguna cuenta de Google en el dispositivo.

Se ha modificado la contraseña de su cuenta de Google. Abra la aplicación Google Mail o Google Play para actualizar la contraseña en el dispositivo.	La contraseña de la cuenta estándar de Google de este dispositivo no es válida. Compruebe si ha modificado la autenticación para su cuenta de Google. Actualice y sincronice la contraseña del dispositivo accediendo a la aplicación Google Mail o Google Play.
Demasiadas aplicaciones en el dispositivo utilizan el servicio de Push para Google (GCM). Desinstale una de estas aplicaciones y vuelva a intentarlo.	Google establece un límite superior para las aplicaciones activadas para GCM instaladas en un dispositivo.
Se ha producido un error. Vuelva a intentarlo más tarde.	Se ha producido un error desconocido.
Hay más de cinco dispositivos registrados en esta cuenta. Borre un dispositivo para poder añadir otro.	Se ha alcanzado el número máximo de cinco dispositivos registrados en Avira Free Android Security.
Este dispositivo ya no está registrado en una cuenta de Avira Free Android Security. Por tanto, se ha restablecido la aplicación.	Se ha restablecido su registro, porque este dispositivo se ha borrado de la lista de los dispositivos registrados.
Se ha producido un error del servidor. Vuelva a intentarlo más tarde.	Se ha producido un error del servidor desconocido.
Se ha producido un error inesperado, por lo que se ha tenido que detener la aplicación. Ayúdenos a solventar este error. Solo tiene que hacer clic en "Aceptar" para transmitirnos automáticamente el protocolo del error. También puede añadir comentarios a este error.	La aplicación ha finalizado debido a un error inesperado. Ayúdenos a solventar este error haciendo clic en Aceptar. De esta forma, nos transmite automáticamente el protocolo del error.
Error inesperado. Puede encontrar más información en la barra de notificaciones.	Se ha producido un error inesperado.

¡Muchas gracias!	Le agradecemos que nos haya notificado este problema. La información se ha enviado correctamente.
Si pierde o le roban el dispositivo, puede restablecerlo a los valores de fábrica con Avira Free Android Security y así borrar datos del dispositivo. Para realizar el restablecimiento remoto a los valores de fábrica, el administrador de dispositivos tiene que estar activado.	Si pierde o le roban el dispositivo, puede restablecerlo a los valores de fábrica con Avira Free Android Security y así borrar datos del dispositivo. Para ello, tiene que estar activada la función **Administrador de dispositivos**.
Establezca una conexión con una red móvil o Wi-Fi para continuar.	Active una conexión a la red para continuar.
La opción Borrado mediante restablecimiento remoto a valores de fábrica está activada/desactivada.	La función de borrado mediante el comando **Restablecimiento remoto a valores de fábrica** está activada/desactivada.
El dispositivo se ha registrado correctamente en Avira Free Android Security.	El dispositivo se ha registrado correctamente en Avira Free Android Security.
Se ha enviado un correo electrónico a <Max.Mustermann@gmail.com>. Lea la información y las notas adicionales en su cuenta de correo electrónico.	Se ha enviado un correo electrónico con las instrucciones de activación a <Max.Mustermann@gmail.com>. Lea este correo para poder empezar a usar nuestro software.
Si tiene preguntas, póngase en contacto con el foro de Soporte o con los empleados de Avira.	Si tiene preguntas, póngase en contacto con nuestro foro o con nuestros empleados.
Error al registrar. Vuelva a iniciar la aplicación e inténtelo de nuevo.	Se ha producido un error inesperado durante el registro. Vuelva a iniciar la aplicación y repita el registro.

Error al registrar. Probablemente está utilizando una tecnología no compatible con Avira Free Android Security. Vuelva a iniciar la aplicación e inténtelo de nuevo.	Probablemente su dispositivo utiliza una tecnología no compatible con Avira Free Android Security. Compruebe los siguientes requisitos del sistema: Sistema operativo: Android 2.2 (Froyo) – Android 2.3.7 (Gingerbread). Memoria RAM: 1,28 MB de memoria RAM libre. Navegador: Mozilla Firefox, Google Chrome, Opera e Internet Explorer IE7 o superior.
Error al crear un contacto	No se ha podido añadir el contacto a la lista negra, ya que existe en la lista.
El nombre ya se encuentra en la lista negra.	Este nombre ya se encuentra en la lista negra y, por tanto, no puede añadirse una segunda vez.
El contacto ya se encuentra en la lista negra.	Este contacto ya se encuentra en la lista negra y, por tanto, no puede añadirse una segunda vez.
El número ya se encuentra en la lista negra por <Max Mustermann>.	Este número de teléfono ya se encuentra en la lista negra en la entrada <Max Mustermann> y, por tanto, no puede añadirse una segunda vez.

Glosario

Abreviatura	Descripción
GCM	El servicio de Android Cloud to Device Messaging (GCM) de Google permite el envío de datos desde servidores a aplicaciones del dispositivo.

IMEI	El número de identificación internacional de equipos móviles (IMEI) es un número inequívoco, similar a una huella dactilar única, con el que se pueden identificar dispositivos.
Tarjeta SIM	La tarjeta del módulo de identificación de abonado (Subscriber Identification Module) es una tarjeta de un operador en la que se guardan datos diversos, como el número de serie, el número del teléfono o el PIN.
PIN	Un número de identificación personal (Personal Identification Number), en la mayor parte de los casos se trata de un número de cuatro cifras.
SO	El sistema operativo del dispositivo.
GPS	El sistema de posicionamiento global es un sistema por satélite que proporciona datos sobre la ubicación y la hora para los receptores de GPS.
Tecnología de red de celdas	Técnica de red avanzada con la que se reciben señales de teléfonos móviles y se transmiten mediante ondas de radio a otras redes de celdas.
Wi-Fi	Un estándar que posibilita el intercambio de datos y el acceso inalámbrico a Internet.
WLAN	Acceso inalámbrico a la red.
Nube	Una ubicación remota de servidores y una infraestructura de TI. Los datos guardados en la nube no se guardan localmente en su ordenador.

Número de teléfono alternativo	Los números de teléfono a los que se puede llamar desde un dispositivo bloqueado con ayuda del botón **Llamar al propietario**.
Latitud	Coordenada geográfica que indica la posición norte-sur en la Tierra.
Longitud	Coordenada geográfica que indica la posición este-oeste en la Tierra.

Servicio

Soporte

Servicio de soporte

En nuestra página web, http://www.avira.de/support, puede consultar toda la información necesaria acerca de nuestro completo servicio de soporte.

Foro de la comunidad

Antes de ponerse en contacto con la línea de atención al clienet, le recomendamos que visite nuestro foro de usuarios en http://forum.avira.com.
Es probable que su problema se haya tratado y solucionado en la comunidad.

Preguntas frecuentes

Lea también la sección “Preguntas frecuentes” de nuestra página web:
http://www.avira.com/de/support-for-home-knowledgebase
Es posible que su pregunta ya se haya planteado y otros usuarios la hayan respondido.

Contacto

Dirección

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Alemania

Internet

Puede encontrar más información acerca de nosotros y nuestros productos en:
http://www.avira.com.

Modo de uso

La Consola Web

Tras la instalación correcta, tiene que registrar el dispositivo para poder acceder a la Consola Web de Avira.

- La Consola Web de Avira incluye una barra de título, una barra lateral y la pantalla principal con varias pestañas.
- En la barra de título se muestran sus datos de acceso y enlaces al Soporte y la administración de la cuenta. Aquí selecciona también la configuración del idioma para la Consola Web de Avira.
- En la barra lateral se muestran los dispositivos registrados.
- Cada dispositivo se muestra en un campo separado:
  - Haga clic en la pestaña del dispositivo en el botón **Editar** para abrir la pestaña **Configuración** de la Consola Web, en la que puede administrar el nombre y el número de teléfono del dispositivo.
- En la parte inferior de la barra lateral hay un enlace con el que se puede introducir y guardar una pregunta de seguridad personal.
- En la pantalla principal de la Consola Web puede encontrar todas las funciones de seguridad para controlar su dispositivo Android, así como información sobre el contenido de la lista negra.

Las pestañas de la Consola Web

La Consola Web incluye las pestañas siguientes:

- El panel
- Ubicar
- Borrado
- Alerta
- Bloquear
- Lista negra
- Configuración

El panel de la Consola Web de Avira Free Android Security

La pestaña **Panel** contiene diferente información sobre cada dispositivo, así como botones de control para iniciar acciones que sirven para proteger el dispositivo.

Información sobre el dispositivo

- Marca: La marca del dispositivo.

- Modelo: El nombre del modelo del dispositivo.
- IMEI: El número de identificación internacional de equipos móviles (IMEI) es un número inequívoco de 15 cifras con el que se pueden identificar teléfonos móviles y también algunos teléfonos por satélite.
- Versión del sistema operativo: El número de versión del sistema operativo Android.
- Versión de la aplicación: El número de versión de la aplicación Avira instalada actualmente. Si utiliza una versión antigua, se muestra un símbolo de advertencia de color rojo.
- Admin. de dispositivos: Indica si la administración de dispositivos está activada. Si está desactivada, se muestra un símbolo de advertencia de color rojo.
- Batería: Información sobre la carga de la batería (en porcentaje).
- Número de teléfono: El número de teléfono guardado en la tarjeta SIM.
- Red: La red de telefonía móvil a la que pertenece la tarjeta SIM.
- Provincia: El país del que procede la tarjeta SIM.
- **Actualizar**: El botón "Actualizar" para actualizar la información del dispositivo.

Seguimiento de ubicación

- Última búsqueda: La hora a la que se ha buscado un dispositivo, p. ej., "hace 5 horas", "hace 3 días".
- Latitud: El dato exacto de la latitud de la ubicación del dispositivo.
- Longitud: El dato exacto de la longitud de la ubicación del dispositivo.

Bloqueo del dispositivo

- Última acción: La última acción que se ha realizado a través de la Consola Web, p. ej., "Bloquear".
- Última acción: La hora a la que se ha bloqueado o desbloqueado un dispositivo.

Inicio de una alerta

- Iniciada por última vez: Período de tiempo desde que se ha enviado por última vez una alarma al dispositivo.

Borrado de datos

- Última eliminación: Período de tiempo desde que se ha borrado por última vez en el dispositivo.
- Tipo: El tipo de borrado que se ha realizado en el dispositivo.

Lista negra

- Utilice esta función para bloquear llamadas y SMS no deseados.

Búsqueda de dispositivos

En la pestaña **Ubicar** se muestra una sección de Google Maps. El estado del seguimiento de ubicación se muestra en el mapa.

- Haga clic en el botón **Ubicar** para iniciar el seguimiento de ubicación del dispositivo perdido.
  - ↪ El seguimiento de ubicación puede durar varios minutos en función del rendimiento de la red y la potencia de la señal.

Avira Free Android Security busca el dispositivo con ayuda del GPS, la tecnología de red de celdas y WLAN.

El tiempo transcurrido se muestra durante el seguimiento de ubicación.

- ↪ Como resultado se muestra en el mapa la ubicación exacta del dispositivo perdido. Es posible ampliar y reducir el mapa.

Borrado

> **Nota**
> Si su versión de Avira Free Android Security no es compatible con la función Borrar, actualice la aplicación en el dispositivo, de la forma descrita en nuestra base de datos de conocimientos. A continuación, solo tiene que actualizar esta página para acceder a la funcionalidad completa de la **función de borrado**.

La pestaña **Borrado** contiene tres opciones para eliminar datos del dispositivo. También puede combinar estas opciones de borrado. La función de borrado causa una pérdida permanente de datos, es decir, los datos eliminados mediante la función de borrado no pueden recuperarse.

> **Nota**
> Debe bloquear el dispositivo antes de poder ejecutar un comando de borrado. Le recomendamos encarecidamente que guarde los datos importantes antes de iniciar un comando de borrado.

Tarjeta SIM

Al iniciar la función de borrado para la **Tarjeta SIM**, se borran todos los datos de la tarjeta SIM. Se eliminan todos los datos de contacto y los SMS guardados en la tarjeta SIM. Estos datos no se pueden recuperar. El borrado de la tarjeta SIM no afecta a los datos guardados en el dispositivo o la tarjeta SD.

> **Nota**
> En función del tipo de tarjeta, es posible que no se pueda borrar la tarjeta SIM.

- Haga clic en **Tarjeta SIM** para borrar todos los datos guardados en la tarjeta SIM.
- Confirme el borrado haciendo clic en **Aceptar**.
  - ↪ Se muestra el mensaje **Se ha borrado correctamente la tarjeta SIM.**.
- Haga clic en **Aceptar** para cerrar el mensaje y volver a la pestaña Borrado.

Almacenamiento total

Al iniciar la función de borrado **Almacenamiento total**, se borran todos los datos guardados en el dispositivo o la tarjeta SD. Estos datos no se pueden recuperar. La función **Almacenamiento total** no afecta a los datos guardados en la tarjeta SIM.

- Haga clic en **Borrar almacenamiento** para iniciar el borrado de los datos guardados directamente en el dispositivo o la tarjeta SD.
- Confirme el borrado haciendo clic en **Aceptar**.
  - ↪ Se muestra el mensaje **Se ha borrado correctamente el almacenamiento.**.
- Haga clic en **Aceptar** para cerrar el mensaje y volver a la pestaña Borrado.

Restablecimiento remoto a valores de fábrica

Mediante **Restablecimiento remoto a valores de fábrica** se restablece la configuración del dispositivo al estado estándar y, además, se borran las cuentas, aplicaciones y datos de las aplicaciones guardados en el dispositivo. La opción **Restablecimiento remoto a valores de fábrica** no afecta a los datos guardados en la tarjeta SIM o SD.

Nota
Para iniciar el comando **Restablecimiento remoto a valores de fábrica** con el fin de borrar todos las datos tras la pérdida o el robo del dispositivo, tiene que activar la opción **Administrador de dispositivos** durante la configuración.

- Haga clic en **Restablecimiento remoto a valores de fábrica** para restablecer la configuración del dispositivo al estado estándar.
- Confirme este tipo de borrado haciendo clic en **Aceptar**.
- Vuelva a hacer clic en **Aceptar** para continuar.
- Para cerrar el mensaje sobre el proceso correcto de **Restablecimiento remoto a valores de fábrica**, haga clic en **Aceptar**.

Advertencia
Mediante la opción **Restablecimiento remoto a valores de fábrica** se desinstala también Avira Free Android Security. A continuación, no puede enviar al dispositivo ningún comando a través de la Consola Web, es decir, no puede bloquear ni buscar el dispositivo.

Borrado combinado

Con el **Borrado combinado** puede iniciar simultáneamente uno, dos o los tres tipos de borrado.

- Seleccione los tipos de borrado que quiere iniciar o haga clic en **Seleccionar todos** para iniciar al mismo tiempo una combinación de todos los tipos de borrado.
- Haga clic en **Realizar acciones seleccionadas**.
- Confirme la selección haciendo clic en **Aceptar**.
  - ↪ En función de su selección y el tamaño de la memoria del dispositivo, esta acción puede tardar hasta 60 minutos.
- Vuelva a hacer clic en **Aceptar** para continuar.
- Para cerrar el mensaje sobre el proceso correcto de **Borrado combinado**, haga clic en **Aceptar**.

Los resultados de los tres tipos de borrado tienen el aspecto siguiente:

Almacenamiento afectado	Tarjeta SIM	Almacenamiento total	Restablecimiento remoto a valores de fábrica
SMS en el dispositivo			borrado
SMS en la tarjeta SIM	borrado		
Contacto en caso de pérdida en el dispositivo			borrado
Contacto en caso de pérdida en la tarjeta SIM	borrado		
Datos en la tarjeta SD		borrado	
Datos del almacenamiento USB interno		borrado	

Cuentas, aplicaciones, datos de las aplicaciones			borrado

Alerta

En la pestaña **Alerta** inicie una alarma fuerte que emitirá el dispositivo. Gracias a esta función puede encontrar rápidamente el dispositivo.

- Haga clic en el botón **Iniciar alerta** para iniciar la función de alerta.
  - ↳ El dispositivo emite durante 20 segundos un sonido fuerte. Durante este tiempo, no es posible apagar ni interrumpir la alerta.

Bloqueo

En la pestaña **Bloquear** puede introducir un PIN de cuatro cifras para bloquear y desbloquear el dispositivo. Puede introducir un mensaje propio que se muestra en la pantalla de bloqueo del dispositivo. Tiene la posibilidad de añadir un número de teléfono al que se puede llamar en el dispositivo bloqueado con ayuda del botón **Llamar al propietario**.

> **Nota**
> Para iniciar el proceso de borrado, el dispositivo tiene que estar bloqueado. Además, recomendamos que se bloquee el dispositivo por motivos de protección de los datos.

- Introduzca en el campo **Introducir PIN** un PIN de cuatro cifras.
- Confirme el PIN en el campo siguiente.
  - ↳ Ahora puede desbloquear manualmente el dispositivo si antes ha introducido un PIN. Si ha olvidado el PIN que ha introducido, tiene que desbloquear el dispositivo a través de la Consola Web.
- Introduzca en el campo **Mensaje si se pierde el dispositivo** un mensaje que resulte adecuado para mostrarlo en el dispositivo bloqueado. Por ejemplo, introduzca un texto y su dirección de correo electrónico para que la persona que lo encuentre pueda ponerse en contacto con usted más fácilmente.
- Introduzca en el campo **Número de teléfono alternativo** un número de teléfono al que se puede llamar en el dispositivo bloqueado con ayuda del botón **Llamar al propietario**. Utilice un número de teléfono fiable, p. ej., su número privado o el número de teléfono de un amigo.
- Haga clic en **Bloquear** para guardar el PIN en el dispositivo y bloquearlo.

- Haga clic en **Desbloquear** si quiere desbloquear el dispositivo a través de la Consola Web.

Lista negra

Si no quiere que le molesten determinadas llamadas o SMS, tiene la posibilidad de añadir estos números de teléfono a la lista negra. Esta función le permite bloquear llamadas y SMS no deseados. Puede añadir números de teléfono de sus contactos, su registro de llamadas y sus mensajes o introducir manualmente un número de teléfono.

Adición de números de teléfono de los protocolos de sus dispositivos a la lista negra

Añada fácilmente a la lista negra números de los protocolos de sus llamadas y mensajes o de sus contactos.

- Abra Avira Free Android Security en su dispositivo.
- Toque **Lista negra**.
  - ↪ Se abre la pantalla **Lista negra**.
- Toque el botón **Añadir**.
  - ↪ Se abre la pantalla **Añadir contactos a la lista negra**.
- Busque el protocolo en el que quiere seleccionar un número de teléfono para añadirlo a la lista negra y toque el campo correspondiente.

  Si no quiere añadir ningún número de teléfono a la lista negra, toque **Cancelar**.

  Toque los números de teléfono que quiere bloquear.
  - ↪ La pantalla siguiente muestra los números de teléfono y el nombre del contacto que quiere bloquear.
- Seleccione el tipo de forma de contacto que quiere bloquear. Tiene la posibilidad de elegir entre **Llamadas y SMS** o solo **Llamadas** o solo **SMS**.
- Haga clic en **Guardar** para guardar los números de teléfono en la lista negra.
- Los números de teléfono bloqueados se muestran en la pantalla **Lista negra**.

> **Nota**
> Si el contacto que quiere añadir ya se encuentra en la lista negra, se muestra un mensaje de error.

Adición manual de números de teléfono a la lista negra

Otra forma de añadir números de teléfono a la lista negra es escribiendo dichos números.

- Abra Avira Free Android Security en su dispositivo.
- Toque **Lista negra**.

↳ Se abre la pantalla **Lista negra**.

- Toque el botón **Añadir**.
  ↳ Se abre la pantalla **Añadir contactos a la lista negra**.
- Toque **Crear contacto manualmente** si quiere introducir un número de teléfono.
  ↳ Se abre la pantalla **Introducir detalles de contacto**.
- Toque el campo **Nombre** para abrir el teclado e introducir caracteres.
- Toque el campo **Número de teléfono** para abrir el teclado e introducir números.
- Seleccione el tipo de forma de contacto que quiere bloquear. Tiene la posibilidad de elegir entre **Llamadas y SMS** o solo **Llamadas** o solo **SMS**.
- Haga clic en **Guardar** para guardar los números de teléfono en la lista negra.

Edición de la lista negra

Puede editar los números de teléfono y el nombre de los contactos bloqueados.

- Abra Avira Free Android Security en su dispositivo.
- Toque **Lista negra**.
  ↳ Se abre la pantalla **Lista negra**.
- Toque el contacto que quiere editar.
  ↳ Se abre la pantalla **Introducir detalles de contacto**.
- Toque el campo **Nombre** para abrir el teclado y editar el nombre.
- Toque el campo **Número de teléfono** para abrir el teclado y editar los números de teléfono.
- Haga clic en **Guardar**, para guardar el contacto editado en la lista negra.
- Haga clic en **Cancelar** si no quiere guardar los cambios realizados.

Eventos bloqueados

Tiene la opción de comprobar el historial de todos los contactos bloqueados en la pestaña **Eventos bloqueados**. Puede ordenar la lista cronológicamente y según el tipo de forma de contacto, como llamadas o SMS. Se muestra el nombre del contacto, la fecha y la hora, así como el tipo y la forma del contacto.

- Toque el botón **Todos** para elegir entre los eventos **Todos**, **Hoy** o **Nuevo**.
- Toque el botón **Llamadas y SMS** para mostrar las llamadas y los mensajes bloqueados. Seleccione la opción **Llamadas** para comprobar qué contacto bloqueado ha intentado llamarlo. O bien seleccione **SMS** para recuperar los mensajes de texto bloqueados.

Borrado de las entradas de los eventos bloqueados

Puede borrar entradas de **Eventos bloqueados**. Ordene la lista según los eventos **Todos**, **Hoy** o **Nuevo** y seleccione entre **Llamadas y SMS**, **Llamadas** o solo **SMS**. Puede borrar los eventos por separado o todos los eventos. Si, por ejemplo, filtra por **Todos** y **Llamadas**, se muestran en forma de lista todas las llamadas bloqueadas. A continuación, tiene la posibilidad de borrar simultáneamente todas las llamadas bloqueadas de sus contactos. O bien marque por separado cada contacto y borre después las llamadas mostradas.

- Toque el contacto cuyos eventos bloqueados quiere borrar.
  - ↪ Se muestran la hora y el número de las llamadas y/o SMS entrantes.
- Toque el campo **SMS** para ver el contenido de los SMS bloqueados.
  - ↪ Ahora puede abrir y leer los mensajes de texto.
  - ↪ Puede borrar los SMS por separado o todos los SMS.

  Toque **Seleccionar todos** para marcar todos los SMS que van a borrarse o ponga una marca en SMS individuales.

  Toque **Eliminar** para quitar todos estos mensajes de texto o toque **Atrás** para interrumpir el proceso de borrado.
  - ↪ Se le solicita que confirme el borrado de los SMS bloqueados.

  Toque **Eliminar** para borrar del historial los SMS seleccionados.

  Toque **Cancelar** para detener el proceso de borrado.
- Toque el campo **Llamadas** para ver todas las llamadas del contacto bloqueado.
  - ↪ Ahora puede borrar las llamadas por separado o todas las llamadas.

  Toque **Seleccionar todos** para marcar todo el historial de llamadas para borrarlo o ponga una marca en llamadas separadas.

  Toque **Eliminar** para quitar todas las llamadas o toque **Atrás** para interrumpir el proceso de borrado.
  - ↪ Se le solicita que confirme el borrado de las llamadas bloqueadas.

  Toque **Eliminar** para borrar del historial las llamadas seleccionadas.

  Toque **Cancelar** para detener el proceso de borrado.

Informes

En la pestaña **Configuración** se muestran en el área **Informes** todas las actividades de Avira Free Android Security realizadas a través de la Consola Web.

La información registrada se ordena por fecha y hora.

Como ejemplo de la información mostrada en el informe de actividades cabe citar:

Fecha	Hora	Mensaje
Martes, 7 de agosto de 2012	15:17	Se ha actualizado satisfactoriamente la información del dispositivo.
Martes, 7 de agosto de 2012	14:05	Se ha encontrado el dispositivo.
Lunes, 13 de agosto de 2012	18:11	Se ha desbloqueado el dispositivo.

Configuración

En la pestaña Configuración, administre el nombre y el número de teléfono del dispositivo. Además, en el área **Informes** puede comprobar todas las actividades de Avira Free Android Security realizadas a través de la Consola Web.

- Haga clic en la barra de navegación en el dispositivo que quiere administrar.
- Introduzca el nombre del dispositivo en el campo **Nombre del dispositivo**.
- Introduzca en el campo **Número de teléfono** el número de teléfono del dispositivo.
- Haga clic en **Guardar cambios** para guardar los cambios realizados en la configuración de este dispositivo.
  - ↪ La Consola Web de Android de Avira indica que la configuración se ha guardado satisfactoriamente.

Instalación y desinstalación

Instalación y desinstalación

Descarga e instalación

Descargue la aplicación Avira Free Android Security directamente desde Google Play en el dispositivo e instálela. Tras instalarla correctamente, se le solicita que registre el dispositivo en la pantalla Registro de Avira Free Android Security. Para ello puede utilizar su cuenta de Google o una dirección de correo electrónico de otro proveedor. Para realizar el registro, necesita una conexión estable a Internet.

- Toque **Abrir** en el dispositivo para abrir el formulario de registro.

- Introduzca su cuenta de Google u otra dirección de correo electrónico.
- Para continuar, toque **Aceptar contrato de licencia y continuar**.
  - ↪ Avira envía a la dirección de correo electrónico indicada una confirmación de su nueva cuenta de Avira Free Android Security. El correo electrónico de confirmación contiene un enlace con el que puede determinar su contraseña personal para iniciar sesión en la Consola Web de Android.
- Haga clic en el enlace del correo electrónico de confirmación para introducir una contraseña y activar la Consola Web de Android.
  - ↪ La Consola Web le permite el control remoto de sus dispositivos.

Para iniciar el comando **Restablecimiento remoto a valores de fábrica** con el fin de borrar todos las datos tras la pérdida o el robo del dispositivo, tiene que activar la opción **Administrador de dispositivos** durante la configuración.

- Para activar la función Administrador de dispositivos, toque **Activar**.
  - ↪ Se abre el cuadro de diálogo **Activar administrador de dispositivos**.
- Confirme la activación del **Administrador de dispositivos** pulsando el botón **Activar**.
  - ↪ Al activar el administrador de dispositivos, hace posible que Avira Free Android Security borre todos los datos de su dispositivo mediante **Restablecimiento remoto a valores de fábrica**.

Si no está seguro de si quiere instalar el administrador de dispositivos durante la configuración, puede retomar la activación de esta opción de configuración en cualquier momento. Realice los pasos siguientes:

- Abra Avira Free Android Security en su dispositivo.
- Toque el botón **Configuración**.
  - ↪ Ahora puede ver si está activada la opción **Borrado por restablecimiento remoto a valores de fábrica**.
- Toque el botón **Configuración de borrado**.
  - ↪ Se abre el cuadro de diálogo **Activar administrador de dispositivos**.
- Toque el botón **Activar** en la parte inferior del cuadro de diálogo.
- Confirme la activación del Administrador de dispositivos pulsando de nuevo el botón **Activar**.
  - ↪ Ahora puede ver si está activada la función **Borrado por restablecimiento remoto a valores de fábrica**.

- **Nota**
  Puede activar o desactivar en cualquier momento el **Administrador de dispositivos** mediante la aplicación Avira Free Android Security de su dispositivo.

Seleccione **Configuración > Configuración de borrado > Borrado por restablecimiento remoto a valores de fábrica > Activar/Desactivar**.

Instalación mediante el PC

Puede descargar la aplicación Avira Free Android Security mediante un PC.

- Abra Google Play en su ordenador.
- Busque la aplicación Avira Free Android Security.
- Haga clic en **Instalar** para descargar la aplicación en el PC.
  - ↪ Se le solicita que inicie la sesión para instalar la aplicación.
- Haga clic en **Conectar** para acceder a su cuenta de Google.
- Introduzca sus datos de acceso.
- Haga clic en **Aceptar** para descargar la aplicación en el dispositivo seleccionado.
  - ↪ La aplicación Avira Free Android Security se descarga en este dispositivo.
- Haga clic en **Aceptar** para cerrar el cuadro de diálogo Descarga.
  - ↪ Se le dirige de nuevo a Google Play, donde el botón **Instalado** indica que ya se ha descargado la aplicación en el dispositivo.

Desinstalación

Para desinstalar Avira Free Android Security, tiene que llevar a cabo dos acciones. Desinstale la aplicación del dispositivo y bórrelo de su cuenta de la Consola Web de Android de Avira.

Nota
Asegúrese de que ha desactivado el **Administrador de dispositivos** antes de desinstalar Avira Free Android Security.

Para desinstalar Avira Free Android Security, pase al Administrador de dispositivos de su dispositivo.

- Toque la aplicación Avira Free Android Security y seleccione **Desinstalar**.
- Confirme la desinstalación.

Asimismo, tiene que borrar el dispositivo de la cuenta de Avira Free Android Security de la Consola Web.

- Abra la Consola Web de Avira.
- Haga clic en la barra de título en el enlace **Cuenta**.
- Pase a la Administración de dispositivos y abra el menú desplegable **Dispositivos disponibles**.

- Seleccione el dispositivo del que quiere borrar la aplicación Avira Free Android Security.
- Haga clic en el botón **Borrar dispositivo** para borrar de su cuenta el dispositivo.

Repetición de la instalación

Tras haber desinstalado todos los dispositivos, ya no puede acceder a la Consola Web de Avira.

No obstante, puede volver a instalar Avira Free Android Security en un dispositivo usando su cuenta de correo electrónico anterior.

- Inicie sesión en la Consola Web usando sus datos de acceso anteriores.
- Después de iniciar la sesión, puede cambiar su contraseña navegando hasta **Administrador de contraseñas**.

  Seleccione **Cuenta > Administrador de contraseñas**, introduzca la contraseña nueva y confírmela.
- Si ha olvidado su contraseña, haga clic en Inicio de sesión en el enlace **¿Ha olvidado su contraseña?**.
  - ↪ Se le solicita que envíe su dirección de correo electrónico, tras lo cual recibirá un enlace de restauración para que pueda volver a crear su contraseña.

Creación de la cuenta para Android

Con el fin de tener controlado siempre su smartphone y proteger sus datos personales con ayuda de diferentes funciones remotas a través de la Consola Web, primero debe crear una cuenta en Avira Free Android Security. Puede crear una cuenta antes de descargar la aplicación en su dispositivo.

- Abra el centro de control del producto de Avira.
- Haga clic en **Centro de control > Protección móvil > Android Security**.
  - ↪ Se abre la página de descarga de Avira Free Android Security.
- Haga clic en **Descargar ahora**.
  - ↪ Se abre la página web de aplicaciones para Android Google Play.

  Haga clic en **Instalar**.
  - ↪ Se le solicita que inicie sesión en Google para descargar la aplicación Avira Free Android Security.

  Haga clic en **Registrarse**.

  Introduzca su dirección de correo electrónico y su contraseña.

  Haga clic en **Registrarse**.

  Seleccione el dispositivo en el que quiere descargar Avira Free Android Security.

Haga clic en **Instalar**.

↪ La aplicación se descarga en el dispositivo Android.

- Abra Avira Free Android Security en el dispositivo.

  Toque **Primeros pasos**.

  ↪ Se abre la pantalla Su cuenta.

  Introduzca sus datos de acceso.

  Para continuar, toque **Aceptar contrato de licencia y continuar**.

  ↪ Avira le enviará un correo electrónico de confirmación para su cuenta nueva, en el que se incluye un enlace con el que puede determinar su contraseña personal para iniciar sesión en la Consola Web de Android.

  Haga clic en el enlace del correo electrónico de confirmación para introducir una contraseña y activar la Consola Web de Android.

  ↪ La Consola Web le permite el control remoto de sus dispositivos a través de la siguiente página web: https://android.avira.com.

Creación rápida de la cuenta para Android

Con el fin de tener controlado siempre su smartphone y proteger sus datos personales con ayuda de diferentes funciones remotas a través de la Consola Web, primero debe crear una cuenta en Avira Free Android Security. Puede crear una cuenta antes de descargar la aplicación en su dispositivo.

- Abra la página web de Avira Free Android Security.

  ↪ Se muestra el enlace a la página de descarga de Avira Free Android Security.

- Haga clic en el botón **Registrarse ahora**.

  ↪ Se abre la página de registro.

- Introduzca su dirección de correo electrónico para Google u otra dirección de correo electrónico que prefiera.

  Haga clic en **Crear cuenta**.

  ↪ Avira envía un correo electrónico de confirmación a la dirección de correo electrónico indicada. Este correo electrónico de confirmación incluye un enlace con el que puede acceder a la Consola Web de Avira Free Android Security.

- Haga clic en el enlace del correo electrónico de confirmación.

  ↪ Se le reenvía a la Consola Web de Avira Free Android Security.

  ↪ La Consola Web le permite el control remoto de sus dispositivos a través de la página https://android.avira.com.

- **Nota**
  Si ha descargado en su dispositivo la aplicación Avira Free Android Security después de haberse registrado en la Consola Web, procure usar los mismos datos de inicio de sesión en la pantalla **Su cuenta** que ha usado durante la configuración.

Inicio de sesión en una cuenta de Android

- Haga clic en **Centro de control > Protección móvil > Android Security**.
  - ↪ Se abre la página de descarga de Avira Free Android Security.
- Haga clic en **Registrar**.
  - ↪ Se abre la página de inicio de sesión de Avira Free Android Security.

  Introduzca su dirección de correo electrónico registrada y su contraseña.

  Haga clic en **Registrar** para abrir la Consola Web con sus funciones para el control remoto.

12.10 General

12.10.1 Categorías de riesgos

Selección de categorías de riesgos avanzadas (Opciones disponibles solo si el modo experto está activado).

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.

12.10.2 Protección avanzada

Protección avanzada

ProActiv (Opciones disponibles solo si el modo experto está activado.)

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 (Opciones disponibles solo si el modo experto está activado.)

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.

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.

12.10.3 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 (Opciones disponibles solo si el modo experto está activado.)

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.
Safe BrowsingSafe Browsing	Si esta opción está activada, es necesaria la contraseña definida para activar o desactivar Protección infantil.
Cuarentena	Si esta opción está activada, es necesaria la contraseña definida para activar o desactivar todas las áreas del Gestor de cuarentena. Si se hace clic en la casilla correspondiente, se activa o desactiva la solicitud de la contraseña.
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.

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.

12.10.4 Seguridad

Opciones disponibles solo si el modo experto está activado.

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 .

12.10.5 WMI

Opciones disponibles solo si el modo experto está activado.

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 , en una interfaz. Por medio de WMI, tiene la posibilidad de consultar datos operativos del programa.

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.

12.10.6 Eventos

Opciones disponibles solo si el modo experto está activado.

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.

12.10.7 Informes

Opciones disponibles solo si el modo experto está activado.

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.

12.10.8 Directorios

Opciones disponibles solo si el modo experto está activado.

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.

12.10.9 Advertencias acústicas

Opciones disponibles solo si el modo experto está activado.

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.

12.10.10 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.

Versión 2° trimestre de 2013.

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Alemania

Teléfono: +49 7542-500 0
Fax: +49 7542-500 3000
Internet: http://www.avira.es