Avira AntiVir Personal – Free Antivirus

Manual para usuarios

AVIRA

Marcas comerciales y Copyright

Marcas comerciales

AntiVir es una marca registrada de Avira GmbH.
Windows es una marca registrada de Microsoft Corporation in the EEUU y otros países.
Todas las marcas y productos mencionados son propiedade de sus respectivos propietarios.
Las marcas protegidas no se utilizan como tales en este manual. Esto no significa, de todas formas, que pueden usarse libremente.

Información de Copyright

Para Avira AntiVir Personal, se ha utilizado 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 Licencias de tercerosde la ayuda de Avira AntiVir Personal, en Licencias de terceros.

Contenido

1 Introducción 1

2 Símbolos y resaltados 2

3 Información de producto 3

3.1 Gama de prestaciones 3
3.2 Requisitos del sistema 4
3.3 Concesión de licencia y actualización a nuevas versiones 5

4 Instalación y desinstalación 7

4.1 Instalación 7
4.2 Instalación diferencial 11
4.3 Módulos de instalación 12
4.4 Desinstalación 12

5 Información general 14

5.1 Interfaz de usuario y uso 14
5.1.1 Centro de control 14
5.1.2 Configuración 16
5.1.3 Icono de bandeja 19
5.2 Toolbar 20
5.2.1 Información general 20
5.2.2 Utilización 20
5.2.3 Opciones 21
5.2.4 Desinstalación 23
5.3 Procedimientos 24
5.3.1 Ejecutar actualizaciones automáticas 24
5.3.2 Iniciar una actualización manualmente 26
5.3.3 Análisis directo: analizar la existencia de virus y malware con un perfil de análisis 26
5.3.4 Análisis directo: Analizar la existencia de virus y malware mediante Arrastrar y soltar 27
5.3.5 Análisis directo: analizar la existencia de virus y malware mediante el menú contextual 28
5.3.6 Análisis directo: analizar la existencia de virus y malware de forma automática 28
5.3.7 Análisis directo: analizar directamente la existencia de rootkits activos 29
5.3.8 Reaccionar a virus y malware detectados 30
5.3.9 Cuarentena: tratar con ficheros (*.qua) en cuarentena 32
5.3.10 Cuarentena: restaurar los ficheros de cuarentena 33
5.3.11 Cuarentena: mover fichero sospechoso a cuarentena 34
5.3.12 Perfil de análisis: añadir o eliminar un tipo de fichero de un perfil de análisis ..35
5.3.13 Perfil de análisis: crear acceso directo en el escritorio para el perfil de análisis .35
5.3.14 Eventos: Filtrar eventos 36

6 Escáner 38

7 Actualizaciones 40

8 Solución de problemas, sugerencias 41

8.1 Ayuda en caso de problemas 41
8.2 Atajos 43
8.2.1 En los cuadros de diálogo 43

8.2.2 En la Ayuda 44
8.2.3 En el Centro de control 44
8.3 Centro de Seguridad de Windows 45
8.3.1 General 45
8.3.2 El Centro de seguridad de Windows y su programa Antivir 46

9 Virus y más 48

9.1 Categorías de riesgos 48
9.2 Virus y otro tipo de Malware 51

10 Información y servicio 54

10.1 Dirección de contacto 54
10.2 Soporte Técnico 54
10.3 Archivos sospechosos 54
10.4 Informe falso positivo 55

11 Referencia: opciones de configuración 56

11.1 Escáner 56
11.1.1 Análisis 56
11.1.1.1. Acción en caso de detección 59
11.1.1.2. Excepciones 61
11.1.1.3. Heurística 62
11.1.2 Informe 63
11.2 Guard 64
11.2.1 Análisis 64
11.2.1.1. Acción en caso de detección 66
11.2.1.2. Excepciones 66
11.2.1.3. Heurística 69
11.2.2 Informe 70
11.3 WebGuard 71
11.3.1 Análisis 71
11.3.1.1. Acción en caso de detección 72
11.3.1.2. Accesos bloqueados 73
11.3.1.3. Excepciones 74
11.3.1.4. Heurística 76
11.3.2 Informe 77
11.4 Actualización 78
11.4.1 Actualización de producto 78
11.4.2 Configuración del reinicio 79
11.5 General 81
11.5.1 Categorías de riesgos 81
11.5.2 Seguridad 82
11.5.3 WMI 83
11.5.4 Directorios 83
11.5.5 Proxy 84
11.5.6 Eventos 84
11.5.7 Limitar informes 85
11.5.8 Advertencias acústicas 85
11.5.9 Advertencias 86

1 Introducción

Con su programa AntiVir 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.

En nuestro sitio Web puede utilizar múltiples opciones y otras posibilidades de información:

http://www.free-av.es

En el sitio Web de Avira puede...

- acceder a información sobre otros programas de escritorio AntiVir
- descargar los programas de escritorio AntiVir más actuales
- 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

2 Símbolos y resaltados

Se usan los siguientes iconos:

Icono / Denominación	Explicación
✓	Consta delante de una condición que debe cumplirse antes de ejecutar una acción.
▸	Consta delante de un paso de acción que se ejecuta.
→	Consta delante de un resultado que se deduce de la acción precedente.
Advertencia	Consta delante de una advertencia en caso de riesgo de pérdida grave de datos.
Nota	Consta delante de una nota con información especialmente importante o delante de una sugerencia que facilita el entendimiento y uso de su programa AntiVir.

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., título de la ventana, área de la ventana o botones de opción).
Negrita	Elementos en los que se hace clic de la interfaz de software (p. ej., opción de menú, sección o botón).

3 Información de producto

Este capítulo proporciona toda la información relevante para la adquisición y el uso de su programa AntiVir:

- consulte el capítulo: Gama de prestaciones
- consulte el capítulo: Requisitos del sistema
- consulte el capítulo: Concesión de licencia

Los programas AntiVir ofrecen herramientas completas y flexibles para proteger su equipo de forma fiable frente a virus, malware, programas no deseados y otros peligros.

▶ Tenga en cuenta las siguientes indicaciones:

Nota
La pérdida de datos valiosos suele tener consecuencias dramáticas. Incluso el mejor programa antivirus no puede protegerle totalmente contra la pérdida de datos. Haga regularmente copias de seguridad (backups) de sus datos.

Nota
Un programa que protege frente a virus, malware, programas no deseados y otros peligros sólo es fiable y eficaz si está actualizado. Asegúrese de disponer de la versión más reciente de su programa AntiVir mediante las actualizaciones automáticas. Configure el programa correspondientemente.

3.1 Gama de prestaciones

Su programa AntiVir dispone de las siguientes funciones:

- Centro de control para la supervisión, la administración y el control de todo el programa
- Configuración centralizada con configuración estándar y avanzada fáciles de usar, así como ayuda sensible al contexto
- Escáner (análisis a petición) con análisis controlado por perfil y configurable de todos los tipos conocidos de virus y malware
- Integración en el control de cuentas de usuario (User Account Control) de Windows Vista para poder realizar tareas para las que se requieren derechos de administrador.
- Guard (análisis en acceso) para la supervisión constante de cualquier acceso a los ficheros
- Avira SearchFree Toolbar (powered by Ask.com), una barra de búsqueda integrada en el explorador web con la que podrá navegar por Internet de forma rápida y cómoda.
- Para usuarios de Avira AntiVir Personal Edition y sólo en combinación con con la Avira SearchFree Toolbar: WebGuard para la supervisión de los datos y ficheros transmitidos desde Internet mediante el protocolo HTTP (supervisión de los puertos 80, 8080, 3128)

- Administración integrada de cuarentena para aislar y tratar los ficheros sospechosos
- Protección contra rootkits para detectar malware instalado de forma oculta en el sistema del ordenador (denominado rootkit)
  (No está disponible en Windows XP 64 Bit)
- Acceso directo a información detallada en Internet acerca de los virus y el malware detectado
- Actualización sencilla y rápida del programa, de las firmas de virus (VDF) y del motor de análisis mediante actualización con un único fichero y actualización incremental del VDF a través de un servidor Web en Internet
- Programador integrado para programar tareas únicas o periódicas, como actualizaciones o análisis
- Grado de detección muy alto de virus y malware mediante tecnologías de análisis innovadoras (motor de análisis) que incluyen procedimientos de análisis heurísticos
- Detección de todos los tipos de archivo convencionales, incluido la detección de archivos anidados y el reconocimiento de extensiones inteligentes
- Gran rendimiento por su capacidad de subprocesamiento múltiple (análisis simultáneo de muchos ficheros a gran velocidad)

3.2 Requisitos del sistema

Existen los siguientes requisitos del sistema::

- PC Pentium o superior, de un mínimo de 266 MHz
- Sistema operativo
- Windows XP, SP2 (32 o 64 bits) o
- Windows Vista (32 o 64 bits, SP 1)
- Windows 7 (32 o 64 bits)
- Al menos 150 MB de espacio libre en el disco duro (en caso de usar la cuarentena y para la memoria temporal, más)
- Al menos 256 MB de memoria RAM con Windows XP
- Al menos 1024 MB de memoria RAM con Windows Vista, Windows 7
- Para la instalación del programa: derechos de administrador
- Para todas las instalaciones: Windows Internet Explorer 6.0 o superior
- Si fuera necesario, conexión a Internet (consulte Instalación)

Avira SearchFree Toolbar

- Sistema operativo
- Windows XP, SP2 (32 o 64 bits) o
- Windows Vista (32 o 64 bits, SP 1)
- Windows 7 (32 o 64 bits)
- Explorador web

- Windows Internet Explorer 6.0 o superior o
- Mozilla Firefox 3.0 o superior

Nota
Desinstale en caso necesario las barras de búsqueda ya instaladas antes de la instalación de la Avira SearchFree Toolbar. De lo contrario, no será posible instalar la Avira SearchFree Toolbar.

Información para usuarios de Windows Vista

En Windows 2000 y Windows XP, muchos usuarios trabajan con derechos de administrador. Pero esto no es conveniente desde el punto de vista de la seguridad, ya que facilita que los equipos sean atacados por virus y programas no deseados.

Por esta razón, Microsoft introduce en Windows Vista el "control de cuentas de usuario". Ofrece mayor protección para los usuarios que han iniciado sesión como administradores: así, en Windows Vista, un administrador sólo tiene en un principio los privilegios de usuario normal. Las acciones para las que se requieren derechos de administrador están marcadas claramente en Windows Vista con un icono informativo. Además, el usuario debe confirmar explícitamente la acción que va a realizar. Únicamente tras esta confirmación se amplían los privilegios y el sistema operativo ejecuta la tarea administrativa en cuestión.

El programa AntiVir requiere en Windows Vista privilegios de administrador para algunas acciones. Estas acciones se identifican con el siguiente símbolo:  . Si este símbolo aparece en un botón, se requieren privilegios de administrador para ejecutar esa acción. Si su cuenta de usuario actual no tiene derechos de administrador, el cuadro de diálogo de Windows Vista para el control de cuentas de usuario solicita la contraseña de administrador. Si no dispone de contraseña de administrador, no podrá ejecutar esa acción.

3.3 Concesión de licencia y actualización a nuevas versiones

Para poder utilizar su producto AntiVir, es necesaria una licencia. Se deben aceptar las condiciones de licencia.

La licencia se asigna como clave de activación. La clave de activación es un código de letras y números que se recibe al adquirir el producto AntiVir. En la clave de activación están registrados todos los datos de su licencia, es decir, los programas que tienen licencia y la duración de ésta.

La clave de activación se envía por email si ha adquirido su programa AntiVir por Internet o bien está indicada en el embalaje del producto.

Para asignar la licencia a su programa, debe introducir la clave de activación al activar el programa. La activación del producto puede llevarse a cabo durante la instalación. Pero también puede activar su programa AntiVir después de la instalación, en el Gestor de licencias en Ayuda::Gestión de licencias.

En Avira AntiVir Personal ya se encuentra una clave de activación válida. Por ello no es necesario activar el producto.

En el gestor de licencias tiene la posibilidad de iniciar la actualización a una versión superior de un producto de la familia de productos AntiVir Desktop: Debido a ello no se requiere una desinstalación manual del producto antiguo ni una instalación manual del nuevo producto. En caso de una actualización a una versión superior desde el gestor de licencias deberá introducir el código de activación del producto al que desea cambiar en el campo de entrada del gestor de licencias. Se realiza una instalación automática del nuevo producto.

A través del gestor de licencias se pueden llevar a cabo automáticamente las siguientes actualizaciones a versiones superiores de producto:

- Actualización a versión superior de Avira AntiVir Personal a Avira AntiVir Premium
- Actualización a versión superior de Avira AntiVir Personal a Avira Premium Security Suite
- Actualización a versión superior de Avira AntiVir Premium a Avira Premium Security Suite

4 Instalación y desinstalación

Este capítulo proporciona información en torno a la instalación y desinstalación de su programa AntiVir:

- consulte el capítulo Instalación: requisitos, tipos de instalación, ejecutar instalación
- consulte el capítulo Módulos de instalación
- consulte el capítulo Instalación diferencial
- consulte el capítulo Desinstalación: ejecutar desinstalación

4.1 Instalación

Antes de la instalación, compruebe si su equipo cumple los requisitos mínimos del sistema. De ser así, puede instalar el programa AntiVir.

Nota
Tiene la posibilidad de crear un punto de restauración durante el proceso de instalación. Un punto de restauración sirve para restablecer en el sistema operativo el estado anterior a la instalación. Si desea utilizar esta opción, asegúrese de que el sistema operativo permite crear puntos de restauración:
Windows XP: Propiedades del programa -> Restauración del sistema: Desactive la opción **Desactivar Restaurar sistema**.
Windows Vista / Windows 7: Propiedades del programa -> Protección del sistema: Marque en el área **Configuración de protección** la unidad en la que está instalada el sistema y pulse el botón **Configurar**. Active en la ventana **Protección del sistema** la opción **Configuración del sistema y restaurar versiones anteriores de fichero**.

Tipos de instalación

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

Exprés

- Su programa AntiVir se instala completo con todos los componentes del programa.
- Los ficheros de programa se instalan en un directorio estándar predefinido en `C:\Archivos de programa`.
- Su programa AntiVir se instala con la configuración estándar. 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 desactivar la creación de un icono de escritorio y un grupo de programas en el menú Inicio.
- En el asistente podrá establecer valores predefinidos de su programa AntiVir e iniciar un breve análisis del sistema que se ejecutará automáticamente después de la instalación.

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. Si existen diferentes soluciones, podrían interferir entre ellas.
- 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)
- Registro como usuario
- Si fuera necesario, ejecución de una actualización tras finalizar la instalación
- Tenga la clave de licencia preparada para su programa AntiVir si desea activar el programa.

Nota
Instalación basada en Internet:
Para la instalación basada en Internet del programa dispone de un programa de instalación que descarga los ficheros de programa actuales de los servidores Web de Avira GmbH antes de ejecutar la instalación. Este procedimiento garantiza que su programa AntiVir 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 programa AntiVir. Se recomienda ejecutar una actualización al acabar la instalación para actualizar el fichero de firmas de virus.

Nota
Para el registro, su programa AntiVir 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 GmbH. Si usa un Firewall , asegúrese de que éste no bloquee las conexiones necesarias y los datos entrantes o salientes.

Ejecutar instalación

El programa de instalación te guía durante la misma. Las ventanas contienen diferentes opciones para controlar la instalación.

Los botones más importantes, tienen asignadas las siguientes funciones:

- **Aceptar:** Confirmar acción.
- **Cancelar:** Cancelar acción.
- **Siguiente:** Continuar con el siguiente paso.
- **Anterior:** Volver al paso anterior.

Así se instala su programa AntiVir:

- Inicie el programa de instalación con un doble clic en el fichero de instalación descargado de Internet o bien coloque el CD del programa en la unidad.

Instalación basada en Internet

→ Aparece el cuadro de diálogo *Bienvenido...*

- Haga clic en **Continuar** para continuar con la instalación.

→ Aparece el cuadro de diálogo *Selección de idioma*.

- Seleccione el idioma con el que desea instalar su programa AntiVir y confirme la selección con **Continuar**.

→ Aparece el cuadro de diálogo *Descarga*. Se descargan todos los ficheros necesarios para la instalación de los servidores Web de Avira GmbH. Tras finalizar la descarga se cierra la ventana *Descarga*.

Instalación con un paquete de instalación

→ El asistente de instalación se abre y muestra el cuadro de diálogo *Avira AntiVir Personal*.

- Haga clic en *Aceptar* para iniciar la instalación.

→ Se descomprime el fichero de instalación. Se inicia la rutina de instalación.

→ Aparece el cuadro de diálogo *Bienvenido...*

- Haga clic en **Continuar**.

Continuación de Instalación basada en Internet e instalación con un paquete de instalación

→ Aparece el cuadro de diálogo con el contrato de licencia.

- Confirme que acepta el contrato de licencia y pulse **Continuar**.

→ Aparece el cuadro de diálogo *Uso privado*.

- Confirme que usará su programa AntiVir exclusivamente en el ámbito privado y no con fines industriales, y pulse **Continuar**.

→ Aparece el cuadro de diálogo *Generar número de serie*.

- Confirme, dado el caso, que se generará un número de serie aleatorio y se transferirá durante la actualización, y pulse **Continuar**.

→ Aparece el cuadro de diálogo *Seleccionar tipo de instalación*.

- Active la opción **Exprés** o **Personalizada.** Si desea crear un punto de restauración, active la opción **Crear punto de restauración del sistema**. Confirme sus datos con **Continuar**.

→ Aparecerá la ventana de diálogo *WebGuard con Avira SearchFree Toolbar (powered by Ask.com)*.

- Si desea instalar la Avira SearchFree Toolbar, confirme que acepta las condiciones del contrato de licencia de Ask.com y desea instalar el WebGuard con la Avira SearchFree Toolbar.

Nota
Desinstale en caso necesario las barras de búsqueda ya instaladas antes de la instalación de la Avira SearchFree Toolbar. De lo contrario, no será posible instalar la Avira SearchFree Toolbar.

- Active en caso necesario la opción **Ask.com como buscador predeterminado** y haga clic en **Continuar**.

Instalación personalizada

↪ Aparece el cuadro de diálogo *Seleccionar directorio de destino* .

▶ Confirme el directorio de destino indicado pulsando **Continuar**.

- O BIEN -

Mediante **Examinar** seleccione otro directorio de destino y confirme pulsando **Continuar**.

↪ Aparece el cuadro de diálogo *Instalar componentes*:

▶ Active o desactive los componentes pertinentes y confirme pulsando **Continuar**.

↪ En el siguiente cuadro de diálogo puede establecer si debe crearse un acceso directo en el escritorio y/o un grupo de programas en el menú Inicio.

▶ Haga clic en **Continuar**.

Continuación: Instalación exprés e instalación personalizada

↪ Se abre el asistente de licencia.

El asistente de licencia ofrece la posibilidad de registrarse como cliente y suscribirse al boletín de Avira. Para ello, es necesario indicar los datos personales.

▶ Indique, si fuera el caso, sus datos y confirme la información con **Continuar**.

↪ Al registrarse, el cuadro de diálogo siguiente muestra el resultado de la activación.

↪ Haga clic en **Continuar**.

↪ Se instalan los componentes del programa. El cuadro de diálogo muestra el progreso de la instalación.

↪ En el siguiente cuadro de diálogo puede seleccionar si debe abrirse el fichero Léame (Readme) y reiniciarse el equipo una vez finalizada la instalación.

▶ En caso necesario, confírmelo y concluya la instalación con *Finalizar*.

↪ Se cierra el asistente de instalación.

Continuación: Instalación personalizada
Asistente de configuración

↪ En caso de una instalación personalizada, en el siguiente paso se abre el asistente de configuración. En el asistente de configuración puede establecer importantes valores predefinidos para su programa AntiVir.

▶ En la ventana de bienvenida del asistente de configuración, haga clic en **Continuar** para iniciar la configuración del programa.

↪ El cuadro de diálogo *Configurar AHeAD* permite seleccionar un nivel de detección para la tecnología AHeAD. El nivel de detección seleccionado se aplica en la configuración de la tecnología AHead del escáner (análisis directo) y del Guard (análisis en tiempo real) .

▶ Seleccione un nivel de detección y continúe con la configuración pulsando **Continuar**.

↪ En la siguiente ventana de diálogo *Seleccionar categorías de riesgos avanzadas* podrá adaptar las funciones de protección de su programa AntiVir con la selección de categorías de riesgos.

▶ Si fuera necesario, active más categorías de riesgos y prosiga con la configuración pulsando *Continuar*.

↪ En caso de que haya seleccionado el módulo de instalación AntiVir Guard para su instalación, aparece el cuadro de diálogo *Modo de inicio del Guard*. Podrá definir el momento de inicio del Guard. El Guard se iniciará con el modo de inicio indicado cada

vez que se reinicie el equipo.

Nota
El modo de inicio especificado del Guard se guarda en el registro y no puede modificarse a través de la configuración.

- Active la opción pertinente y prosiga con la configuración pulsando *Continuar*.

→ En el siguiente cuadro de diálogo, *Análisis del sistema*, puede activar o desactivar un breve análisis del sistema. El breve análisis del sistema se ejecuta una vez concluida la configuración y antes de reiniciar el equipo, y se analizan los programas iniciados, así como los ficheros del sistema más importantes para detectar virus y malware.

- Active o desactive la opción *Análisis breve del sistema* y prosiga con la configuración pulsando *Continuar*.

→ En el siguiente cuadro de diálogo puede concluir la configuración con *Finalizar*.

- Haga clic en *Finalizar* para concluir la configuración.

→ Se aplican los parámetros de configuración indicados y seleccionados.

→ Si ha activado la opción *Análisis breve del sistema*, aparece la ventana Luke Filewalker. El escáner lleva a cabo un breve análisis del sistema.

Continuación: Instalación exprés e instalación personalizada

→ Si en el último asistente de instalación ha seleccionado la opción **Reiniciar equipo**, se produce un reinicio del equipo.

→ Después del reinicio del equipo se muestra el fichero Léame si en el asistente de instalación ha seleccionado la opción **Mostrar Léame.txt**.

Tras la instalación correcta se recomienda comprobar en el Centro de control en *Información general:: Estado* comprobar la actualidad del programa.

- Si fuera necesario, lleve a cabo una actualización para actualizar el fichero de firmas de virus.
- A continuación, lleve a cabo un análisis completo del sistema.

4.2 Instalación diferencial

Puede añadir o quitar determinados componentes del programa en la instalación actual del programa AntiVir (consulte el capítulo Instalación y desinstalación::Módulos de instalación)

Si desea añadir o quitar módulos de programa a la instalación actual, puede usar la opción **Añadir o quitar programas** para **Cambiar/Eliminar** programas en el **Panel de control de Windows**.

Seleccione su programa AntiVir y haga clic en **Modificar**. En el cuadro de diálogo de bienvenida del programa, seleccione la opción **Modificar programa**. Será guiado/a a través de la instalación diferencial.

Nota
Si desinstala la Avira SearchFree Toolbar, se desinstalará asimismo el WebGuard.

4.3 Módulos de instalación

En caso de instalación personalizada o de instalación diferencial, puede seleccionar los siguientes módulos para añadir a la instalación o bien quitarlos de ella:

- **AntiVir Personal**
  Este módulo contiene todos los componentes necesarios para la instalación correcta de su programa AntiVir.
- **AntiVir Guard**
  El AntiVir Guard 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 programa AntiVir analiza automáticamente el fichero. En el caso de la operación de fichero Cambiar nombre, AntiVir Guard no realiza análisis alguno.
- **AntiVir WebGuard** (para usuarios de Avira AntiVir Personal Edition y sólo en combinación con con la Avira SearchFree Toolbar)
  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 explorador directamente a la ejecución en el explorador Web, de modo que un análisis en tiempo real, como el que ofrece el AntiVir Guard, no es posible en este caso. Ésta es una vía de acceso de virus y programas no deseados a su sistema informático. El WebGuard es 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.
- *AntiVir Protección contra rootkits*
  La protección contra rootkits de AntiVir 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 malware.
- **Extensión del shell**
  La extensión del shell crea en el menú contextual del Windows Explorer (botón derecho del ratón) la entrada Analizar ficheros seleccionados con AntiVir. Esta entrada permite analizar directamente determinados ficheros o directorios.

4.4 Desinstalación

Si desea desinstalar el programa AntiVir del equipo, puede utilizar la opción **Agregar o Quitar Programas** para **Cambiar/Quitar** programas en el Panel de Control de Windows.

Procedimiento para desinstalar su programa AntiVir (descrito con el ejemplo de Windows XP y Windows Vista):

- Por medio del menú **Inicio**, abra el **Panel de control**.
- Haga doble clic en **Programas** (Windows XP: **Software**).
- Seleccione su programa AntiVir en la lista y haga clic en **Eliminar**.

→ Se le pregunta si confirma que desea quitar el programa.

▶ Confirme con **Sí**.

→ Se quitan todos los componentes del programa.

▶ Pulse **Finalizar** para completar la desinstalación.

→ Es posible que aparezca un cuadro de diálogo recomendando el reinicio del equipo.

▶ Confirme con **Sí**.

→ El programa AntiVir se ha desinstalado, si fuera necesario, el equipo se reiniciará. Al hacerlo, se eliminan todos los directorios, ficheros y entradas del registro del programa.

Nota
La Avira SearchFree Toolbar no se encuentra incluida en la desinstalación del programa, debe desinstalarse por separado siguiendo los pasos anteriormente mencionados. Para ello debe estar activada en Firefox la Avira SearchFree Toolbar mediante el administrador de complementos (no es válido para Internet Explorer). Tras la desinstalación, la barra de búsqueda ya no está integrada en su explorador web.

Nota
Si desinstala la Avira SearchFree Toolbar, se desinstalará asimismo el WebGuard.

5 Información general

En este capítulo dispone de una descripción general de las funciones y el uso de su programa AntiVir.

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

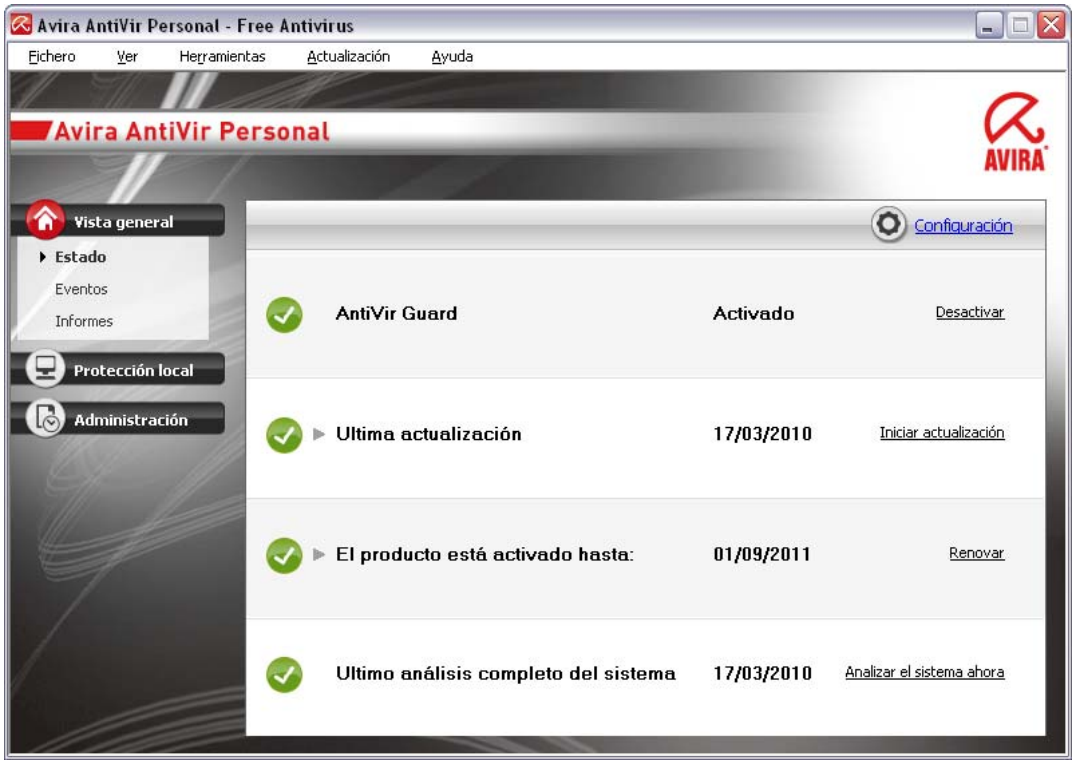
5.1 Interfaz de usuario y uso

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

- Centro de control: Monitorización y control del programa AntiVir
- Configuración: Configuración del programa AntiVir
- Icono de bandeja en la bandeja del sistema de la barra de tareas: apertura del Centro de control y otras funciones

5.1.1 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 programa AntiVir.



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

- **Barra de menús:** en los menús del Centro de control puede activar funciones de programa generales y consultar información sobre el programa.

- **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 *Descripción general* - sección **Estado**.
- **Vista:** en esta ventana se muestra la sección seleccionada en el área de exploración. En función de cada sección, en la barra superior de la ventana de detalles encontrará botones para ejecutar funciones o acciones. En algunas secciones, aparecen datos u objetos de datos en listas. Puede ordenar las listas pulsando en el campo según el cual quiera ordenar la lista.

Inicio y finalización del Centro de control

Puede iniciar el Centro de control de las siguientes maneras:

- Con un doble clic en el icono del programa de su escritorio
- Por medio de la entrada de programa en el menú Inicio | Programas.
- A través del icono de bandeja de su programa AntiVir.

Para finalizar el Centro de control, use la opción de menú **Salir** del menú **Fichero** o bien pulse el aspa de cierre en el Centro de control.

Usar el Centro de control

Así se navega por el Centro de control

▶ Seleccione un área de actividades en la barra de exploración.

→ Se abre el área de actividades y aparecen otras secciones. Está seleccionada la primera sección del área de actividades y se muestra en la vista.

▶ Si lo desea, pulse en otra sección para mostrarla en la ventana de detalles.

- O BIEN -

▶ Elija una sección por medio del menú *Ver*.

Nota
La exploración usando el teclado de la barra de menús se activa con la tecla [Alt]. Si está activada la exploración, puede desplazarse por el menú usando las teclas de flecha. Con la tecla Intro se activa la opción de menú seleccionada en ese momento.
Para abrir y cerrar los menús en el Centro de control o para explorarlos, podrá usar las siguientes combinaciones de teclas: [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

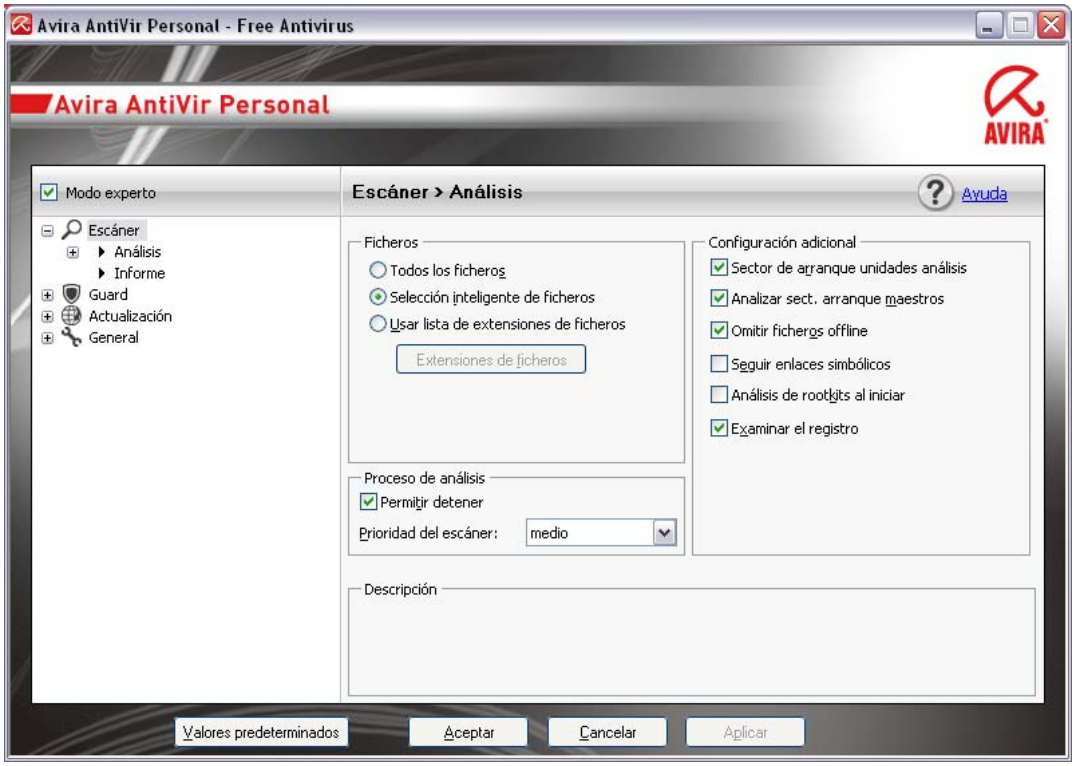
Descripción general del Centro de control

- **Descripción general**: en **Información general** encontrará todas las secciones con las que puede supervisar la funcionalidad de su programa AntiVir.

- La sección **Estado** ofrece la posibilidad de ver de una sola mirada qué módulos del programa están activos y aporta información sobre la última actualización realizada. Además, se ve si dispone de una licencia válida.
- La sección Eventos ofrece la posibilidad de informarse sobre los eventos que generan los módulos de programa.
- La sección Informes ofrece la posibilidad de consultar los resultados de las acciones realizadas.
- **Protección local**: en **Protección local** constan los componentes con los que se analizan los ficheros del sistema informático para detectar la existencia de virus o software malintencionado (malware).
- La sección Analizar permite configurar o iniciar fácilmente el análisis directo. Los perfiles predefinidos permiten llevar a cabo un análisis con opciones predeterminadas ya adaptadas. Del mismo modo, puede adaptar a sus propias necesidades el análisis de detección de virus y programas no deseados por medio de la selección manual (no se guarda)
- La sección Guard muestra información sobre los ficheros analizados, así como otros datos estadísticos que puede restablecer en cualquier momento y permite abrir el fichero de informe. Dispondrá de información detallada acerca de la última detección de virus o programas no deseados " prácticamente con sólo pulsar un botón".
- **Protección online** : en **Protección online** 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 WebGuard muestra información sobre las URL analizadas y los virus detectados, así como otros datos estadísticos que puede restablecer en cualquier momento y permite abrir el fichero de informe. Dispondrá de información detallada acerca de la última detección de virus o programas no deseados " prácticamente con sólo pulsar un botón".
- **Administración**: en **Administración** encontrará herramientas con las que aislar y administrar ficheros sospechosos o infectados por virus, así como programar tareas periódicas.
- La sección Cuarentena contiene lo que se denomina Gestor de cuarentena. Es el elemento central para ficheros ya puestos en cuarentena o para ficheros sospechosos que se quieren poner en cuarentena. Además, existe la posibilidad de enviar un determinado fichero por email al Avira Malware Research Center.
- La sección Programador permite crear tareas de análisis y actualización, así como programadas, y adaptar o eliminar tareas existentes.

5.1.2 Configuración

En la configuración puede establecer los parámetros de su programa Antivir . Tras la instalación, su programa AntiVir 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 programa AntiVir 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.
- Por medio del Centro de seguridad de Windows: a partir de Windows XP Service Pack 2.
- A través del icono de bandeja de su programa AntiVir.
- En el Centro de control a través de la opción de menú Herramientas | Configuración.
- En el Centro de control pulsando 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, aparece 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 las secciones de configuración subordinadas, pulse en el signo menos 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: [Alt] + letra subrayada en el nombre de opción o en la denominación del botón.

Nota
Sólo 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 los parámetros establecidos se aplican.

- O BIEN -

- Haga clic en el botón **Aplicar**.

→ Se aplica la configuración. La ventana de configuración permanece abierta.

Si quiere finalizar la configuración sin aceptar los parámetros establecidos:

- Pulse el botón **Cancelar**.

→ La ventana de configuración se cierra y los parámetros establecidos se descartan.

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.

Descripción general de las opciones de configuración

Dispone de las siguientes opciones de configuración:

- **Escáner**: Configuración del análisis directo

  Opciones de análisis

  Acciones en caso de detección

  Opciones al analizar archivos

  Excepciones del análisis directo

  Heurística del análisis directo

  Configuración de la función de informe

- **Guard**: Configuración del análisis en tiempo real

  Opciones de análisis

  Acciones en caso de detección

  Excepciones del análisis en tiempo real

Heurística del análisis en tiempo real

Configuración de la función de informe

– **WebGuard**: Configuración del WebGuard

Opciones de análisis, activación y desactivación del WebGuard

Acciones en caso de detección

Accesos bloqueados: filtro Web para direcciones URL conocidas no deseadas (malware, suplantación de identidad (phishing), etc.)

Excepciones del análisis del WebGuard: direcciones URL, tipos de fichero, tipos MIME

Heurística del WebGuard

Configuración de la función de informe

– **General**:

Categorías de riesgos avanzadas para análisis directo y análisis en tiempo real

Seguridad: indicador de estado de actualización, indicador de estado de análisis completo del sistema, protección del producto

WMI: Activar compatibilidad con WMI

Configuración del registro de eventos

Configuración de las funciones de informe

Configuración de los directorios usados

Actualización: configuración de la conexión con el servidor de descarga, configuración de la actualización del producto

Configuración de advertencias acústicas al detectar malware

5.1.3 Icono de bandeja

Tras la instalación verá el icono de bandeja de su programa AntiVir en la bandeja del sistema de la barra de tareas:

Icono	Descripción
	AntiVir Guard está activado
	AntiVir Guard está desactivado

El icono de bandeja muestra el estado del servicio de .

Por medio del menú contextual del icono de bandeja puede acceder rápidamente a las funciones principales de su programa AntiVir. Para activar el menú contextual, pulse con el botón derecho del ratón en el icono de bandeja.

Entradas en el menú contextual

– **Activar AntiVir Guard** Activa o desactiva el AntiVir Guard.

– **Activar AntiVir WebGuard**: Activa o desactiva el AntiVir WebGuard.

– **Iniciar AntiVir**: Abre el Centro de control.

- **Configurar AntiVir**: Abre la Configuración.
- **Iniciar actualización**: Inicia una Actualización.
- **Ayuda**: Abre la ayuda online.
- **Acerca de AntiVir Personal:** Abre un cuadro de diálogo con información sobre su programa AntiVir: Información del producto, información sobre la versión, información sobre la licencia.
- **Avira en Internet**: Abre el portal Web de Avira en Internet. Debe de existir una conexión activa a Internet

5.2 Toolbar

5.2.1 Información general

Tras finalizar la instalación con éxito, la Avira SearchFree Toolbar queda integrada en su explorador web. Al acceder al explorador por primera vez, se abre una ventana de estado que contiene información importante sobre el funcionamiento de la Toolbar.

La Toolbar se compone de un cuadro de búsqueda, un logotipo de Avira vinculado con el sitio Web de Avira, dos indicadores de estado y el menú **Opciones**.

- **Barra de búsqueda**
  Utilice la barra de búsqueda para realizar búsquedas de forma rápida y gratuita en Internet utilizando el motor de búsqueda Ask.com.
- **Indicadores de estado**
  Los indicadores de estado proporcionan información sobre el estado del WebGuard y el estado de actualización de Avira AntiVir y le ayudan a detectar qué acciones debe llevar a cabo para proteger su PC en caso necesario.
- **Opciones**
  Por medio del menú Opciones puede acceder a las opciones de la barra, borrar el historial, acceder a la Ayuda y la información acerca de Toolbar y desinstalar Avira SearchFree Toolbar directamente por medio del explorador web (sólo Firefox).

5.2.2 Utilización

Barra de búsqueda

Utilizando la barra de búsqueda puede buscar en Internet uno o varios términos.

Indique para ello el término en el cuadro de búsqueda y pulse a continuación la tecla Intro o haga clic en **Buscar**. El motor de búsqueda Ask.com examina entonces Internet por usted y muestra todos los resultados encontrados en la ventana del navegador.

Puede consultar cómo configurar la Avira SearchFree Toolbar en Internet Explorer y Firefox según desee en **Opciones.**

Indicador de estado

WebGuard

 WebGuard está activado.

Avira WebGuard está activado, su ordenador está protegido.

 WebGuard está desactivado.

Avira WebGuard está desactivado. Revise su aplicación y active WebGuard para estar protegido.

Estado de actualización

A la derecha se encuentra el mensaje de estado con información sobre el estado de actualización de Avira. Por medio de iconos y mensajes puede informarse de que acciones debe llevar a cabo para proteger su PC en caso necesario.

 Actualización diaria terminada.

Si pasa con el puntero del ratón por encima del icono, podrá leer el siguiente mensaje: **Avira está actualizado, su ordenador está protegido.**

- No es necesario realizar ninguna acción.

 Actualizar Avira.

Si pasa con el puntero del ratón por encima del icono, podrá leer el siguiente mensaje: **Avira no está actualizado. Haga clic aquí para descargar la actualización más reciente para que su PC esté protegido.**

- Haga clic en el icono amarillo o el texto para actualizar Avira AntiVir. Esto tiene lugar conforme a los valores predefinidos que ha configurado en Avira AntiVir.

→ Durante la actualización podrá leer el mensaje **Actualizando...**

→ Una vez finalizada la actualización con éxito, vuelve a aparecer el icono verde con el mensaje **Actualización diaria ejecutada**.

 Avira no está disponible.

Si pasa con el puntero del ratón por encima del icono, podrá leer el siguiente mensaje: **Avira no está disponible. Para garantizar su protección, compruebe si su aplicación aún está instalada y se está ejecutando.**

- Haga clic en el icono gris o el texto para acceder a la página de ayuda de Avira. En ella encontrará las instrucciones para el procedimiento posterior.

5.2.3 Opciones

La Avira SearchFree Toolbar es compatible con Internet Explorer y Firefox y se puede configurar según desee en ambos exploradores web:

Opciones de configuración de Internet Explorer
Opciones de configuración de Firefox

Internet Explorer

En el explorador web Internet Explorer se dispone de las siguientes opciones de configuración en el menú **Opciones** para la Avira SearchFree Toolbar:

Opciones de la Barra

Análisis

- **Seleccionar motor Ask**
  En el menú **Seleccionar motor Ask** puede elegir qué motor de búsqueda Ask se debe utilizar para la solicitud de búsqueda. Hay motores de búsqueda disponibles de EE.UU., Brasil, Alemania, España, Europa, Francia, Italia, Países Bajos, Rusia y Gran Bretaña.

- **Iniciar búsquedas en**
  En el menú de la opción **Iniciar búsquedas en** puede elegir dónde debe aparecer el resultado de una solicitud de búsqueda, en la **Ventana actual**, en una **Nueva ventana** o en una **Nueva pestaña**.
- **Mostrar búsquedas recientes**
  Si está activada la opción **Mostrar búsquedas recientes** , puede ver bajo el cuadro de entrada de texto de la barra de búsqueda los términos buscados hasta el momento.
- **Autoborrar historial de búsquedas al salir del navegador**
  Active la opción **Autoborrar historial de búsquedas al salir del navegador** si no desea guardar el historial de búsquedas, sino borrarlo al cerrar el explorador web.

Otras opciones

- **Seleccionar idioma barra**
  En **Seleccionar idioma barra** puede elegir el idioma en el que debe aparecer la Avira SearchFree Toolbar. Los idiomas disponibles son: inglés, alemán, español, francés, italiano y portugués.

N**ota**
El idioma predeterminado para la Avira SearchFree Toolbar es el de su programa, siempre que esté disponible. Si la Toolbar no está disponible en su idioma, el idioma predeterminado es el inglés.

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

Borrar historial

Active la opción **Borrar historial** si no desea guardar, sino borrar de inmediato las búsquedas realizadas.

Ayuda

Haga clic en **Ayuda** para acceder al sitio Web con las preguntas de uso frecuente (FAQ) sobre la Toolbar.

Desinstalar

Puede desinstalar la Avira SearchFree Toolbar también directamente en Internet Explorer: Desinstalación en el explorador web.

Información

Haga clic en **Acerca de** para ver qué versión de la Toolbar está instalada.

Firefox

En el explorador web Firefox se dispone de las siguientes opciones de configuración en el menú **Opciones** para la Avira SearchFree Toolbar:

Opciones de la Barra

Análisis

- **Seleccionar motor Ask**
  En el menú **Seleccionar motor Ask** puede elegir qué motor de búsqueda Ask se debe utilizar para la solicitud de búsqueda. Hay motores de búsqueda disponibles de EE.UU., Brasil, Alemania, España, Europa, Francia, Italia, Países Bajos, Rusia y Gran Bretaña.
- **Mostrar búsquedas recientes**
  Si está activada la opción **Mostrar búsquedas recientes** , puede ver los términos buscados hasta el momento haciendo clic en la flecha de la barra de búsqueda. Seleccione uno de los términos si desea volver a ver el resultado de la búsqueda.
- **Autoborrar historial de búsquedas al salir del navegador**
  Active la opción **Autoborrar historial de búsquedas al salir del navegador** si no desea guardar el historial de búsquedas, sino borrarlo al cerrar el explorador web.
- **Mostrar resultados de búsqueda de Ask al introducir palabras clave o direcciones URL no válidas en el campo de dirección del explorador**
  Si esta opción está activada, cada vez que introduce palabras clave o una dirección URL no válida en el campo de dirección del explorador web, se inicia una solicitud de búsqueda y aparece el resultado de la búsqueda.

Otras opciones

- **Seleccionar idioma barra**
  En **Seleccionar idioma barra** puede elegir el idioma en el que debe aparecer la Avira SearchFree Toolbar. Los idiomas disponibles son: inglés, alemán, español, francés, italiano y portugués.

Nota
El idioma predeterminado para la Avira SearchFree Toolbar es el de su programa, siempre que esté disponible. Si la Toolbar no está disponible en su idioma, el idioma predeterminado es el inglés.

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

Borrar historial

Haciendo clic en **Borrar historial** borrará todos los términos buscados hasta el momento con Avira SearchFree Toolbar.

Ayuda

Haga clic en **Ayuda** para acceder al sitio Web con las preguntas de uso frecuente (FAQ) sobre la Toolbar.

Desinstalar

Puede desinstalar la Avira SearchFree Toolbar también directamente en Firefox: Desinstalación en el explorador web.

Información

Haga clic en **Acerca de** para ver qué versión de la Toolbar está instalada.

5.2.4 Desinstalación

Procedimiento para desinstalar la Avira SearchFree Toolbar (descrito con el ejemplo de Windows XP y Windows Vista):

- Por medio del menú **Inicio**, abra el **Panel de control**.

- Haga doble clic en **Programas** (Windows XP: **Software**).
- Seleccione **Avira SearchFree Toolbar con WebGuard** en la lista y haga clic en **Eliminar**.

→ Se le preguntará si confirma que desea desinstalar el producto.

- Confirme con **Sí**.

→ Avira SearchFree Toolbar con WebGuard se desinstala, si fuera necesario, el equipo se reinicia. Al hacerlo, se eliminan todos los directorios, ficheros y entradas del registro de Avira SearchFree Toolbar con webGuard.

Instalación a través del explorador web.

Además, tiene la posibilidad de desinstalar la Avira SearchFree Toolbar directamente en el navegador:

- Abra a la derecha, en la barra de búsqueda, el menú **Opciones**.
- Haga clic en **Desinstalar**.

→ Si aún tiene abierto su explorador web, se le pedirá que lo cierre.

- Cierre el explorador web y haga clic en **Aceptar**.

→ Avira SearchFree Toolbar con WebGuard se desinstala, si fuera necesario, el equipo se reinicia. Al hacerlo, se eliminan todos los directorios, ficheros y entradas del registro de Avira SearchFree Toolbar con webGuard.

Nota
Si desinstala la Avira SearchFree Toolbar, se desinstalará asimismo el WebGuard.

Nota
Tenga en cuenta que para desinstalar la Avira SearchFree Toolbar de Firefox, debe estar activada la Toolbar en el administrador de complementos.

5.3 Procedimientos

5.3.1 Ejecutar actualizaciones automáticas

Así se crea una tarea con el programador AntiVir con la que actualizar automáticamente su programa AntiVir:

- En el Centro de control seleccione la sección **Administración :: Programador**.
- Haga clic sobre 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 **Continuar**.

→ Aparece el cuadro de diálogo *Tipo de tarea*.

- Seleccione **Tarea de actualización** en la lista de selección.
- Haga clic en **Continuar**.

↪ Aparece el cuadro de diálogo *Momento de inicio de la tarea*.

▶ Seleccione cuándo se ejecutará la actualización:

- **Inmediatamente**
- **Diariamente**
- **Semanalmente**
- **Intervalo**
- **Una vez**

Nota
Recomendamos llevar a cabo actualizaciones frecuentes y periódicas. El intervalo de actualización recomendado es de: 24 horas.

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

▶ En caso necesario, seleccione opciones adicionales (sólo 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 **Continuar**.

↪ Aparece el cuadro de diálogo *Selección del modo de visualización*.

▶ Seleccione el modo de visualización de la ventana de tareas:

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

▶ Haga clic en **Finalizar**.

↪ La tarea recién creada aparece en la página de inicio de la sección **Administración :: Analizar** 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

5.3.2 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. La actualización del producto sólo tiene lugar si, en General:: Actualización, ha activado la opción **Descargar actualizaciones de producto e instalar automáticamente**.

Así se inicia manualmente una actualización de su programa AntiVir:

- Haga clic con el botón derecho del ratón en el icono de bandeja de AntiVir en la barra de tareas.

→ Aparece un menú contextual.

- Seleccione **Iniciar actualización**.

→ Aparece el cuadro de diálogo *Updater*.

- O BIEN -

- En el Centro de control seleccione la sección **Información general:: Estado**.
- En el área *Ultima actualización* haga clic en el enlace **Iniciar actualización**.

→ Aparece el cuadro de diálogo Updater.

- O BIEN -

- En el Centro de control, en el menú **Actualización**, seleccione el comando de menú *Iniciar actualización*.

→ Aparece el cuadro de diálogo Updater.

Nota
Recomendamos llevar a cabo actualizaciones automáticas periódicamente. El intervalo de actualización recomendado es de: 24 horas.

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

5.3.3 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.

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

– En Windows XP y 2000:

 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 sólo tiene derechos limitados, p. ej., de acceso a directorios y ficheros. El Centro de control sólo 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. Sólo 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:

▶ En el Centro de control seleccione **Protección local :: Analizar**.

→ Aparecen perfiles de análisis predefinidos.

▶ Seleccione uno de los perfiles de análisis predefinidos.

- O BIEN -

▶ Adapte el perfil de análisis *Selección manual*.

▶ Haga clic en el icono (Windows XP:  o Windows Vista: ).

▶ Aparece la ventana *Luke Filewalker* y el análisis directo comienza.

→ 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 que deben analizarse:

▶ Seleccione los nodos que desea analizar mediante un clic en casilla:

5.3.4 Análisis directo: Analizar la existencia de virus y malware mediante Arrastrar y soltar

Así se analiza la existencia de virus y malware mediante Arrastrar y soltar de forma precisa:

✓ Esta abierto el Centro de control de su programa AntiVir.

▶ Seleccione el fichero desea analizar.

▶ Arrastre con el botón izquierdo del ratón el fichero seleccionado al *Centro de control*.

→ Aparece la ventana *Luke Filewalker* y el análisis directo comienza.

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

5.3.5 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 desea analizar.

→ Aparece el menú contextual del Explorador de Windows.

- Seleccione en el menú contextual **Analizar los ficheros seleccionados con AntiVir**.

→ Aparece la ventana *Luke Filewalker* y el análisis directo comienza.

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

5.3.6 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:

- En el Centro de control seleccione 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 **Continuar**.

→ Aparece el cuadro de diálogo *Tipo de tarea*.

- Seleccione la **Tarea de análisis**.
- Haga clic en **Continuar**.

→ Aparece el cuadro de diálogo *Selección del perfil*.

- Seleccione el perfil que debe analizarse.
- Haga clic en **Continuar**.

→ Aparece el cuadro de diálogo *Momento de inicio de la tarea*.

- Seleccione cuándo se ejecutará el análisis:
  - **Inmediatamente**
  - **Diariamente**
  - **Semanalmente**
  - **Intervalo**
  - **Una vez**
- Según lo que seleccione, indique la fecha si fuera necesario.

- En caso necesario, seleccione la siguiente opción adicional (sólo 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 **Continuar**.

→ Aparece el cuadro de diálogo *Selección del modo de visualización*.

- Seleccione el modo de visualización de la ventana de tareas:
  - **Minimizado**: sólo barra de progreso
  - **Maximizado**: toda la ventana de tarea
  - **Invisible**: ninguna ventana de tarea
- Seleccione la opción *Apagar equipo* si desea que el equipo de 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 :: Planificador* como activado (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

5.3.7 Análisis directo: analizar directamente la existencia de rootkits activos

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

Así se analiza directamente la existencia de rootkits activos:

- En el Centro de control seleccione **Protección local :: Analizar**.

→ Aparecen perfiles de análisis predefinidos.

- Seleccione el perfil de análisis predefinido **Análisis 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 el análisis directo comienza.

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

5.3.8 Reaccionar a virus y malware detectados

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

En el componente Guard no existen opciones de acción configurables. En caso de detección recibirá una notificación en el escritorio. En la notificación de escritorio podrá eliminar el malware detectado o pasar el malware para el consiguiente tratamiento de virus al componente escáner a través del botón Detalles. El escáner avisa la detección en una ventana, en la que dispondrá de distintas opciones para el tratamiento del fichero afectado a través de un menú (ver Detección::Escáner).

Opciones de acción del escáner:

– **Interactivo**

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

– **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 para , WebGuard:

– **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.

Al detectar virus y programas no deseados en el modo de acción interactivo la reacción es que, 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 (AntiVir Guard, AntiVir Scanner, AntiVir WebGuard) que notifica la detección y del malware detectado.

Acciones del escáner y del Guard:

– **Reparar**

El fichero se repara.

Sólo puede activar esta opción si el fichero detectado se puede reparar.

– **Mover a 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 GmbH.

– **Eliminar**

El fichero se elimina. 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.

– **Cambiar nombre**

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

– **Omitir**

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

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

– **Ignorar siempre**

Opción de acción en las detecciones de Guard: El Guard 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 Repairtool**

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 programa AntiVir 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 del WebGuard:

– **denegar acceso**

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

– **Mover a cuarentena**

La página Web solicitada por el servidor Web o los datos y ficheros transmitidos se mueven a la cuarentena. El fichero infectado puede ser restaurado a través de la cuarentena si es de vital importancia, o si es necesario, o enviarse al Avira Malware Research Center.

– **Omitir**

La página Web solicitada por el servidor Web o los datos y archivos transmitidos son pasados por el WebGuard a su navegador.

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

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

5.3.9 Cuarentena: tratar con ficheros (*.qua) en cuarentena

Así puede tratar los ficheros que están en la cuarentena:

- En el Centro de control seleccione 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 programa AntiVir y se sospecha de que exista una falsa alarma. Así puede confirmar tras un nuevo análisis de que se trataba de una falsa alarma y puede 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  .

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  .

→ Aparece un cuadro de diálogo con un formulario para indicar sus datos de

contacto

- Indique los datos completos.
- Seleccione un tipo: **Fichero sospechoso** o **Falsa alarma**.
- Pulse **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 programa AntiVir 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.

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 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 el capítulo: Cuarentena: restaurar los ficheros de cuarentena

5.3.10 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 sólo tiene derechos limitados, p. ej., de acceso a directorios y ficheros. El Centro de control sólo 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. Utilice la función *Restaurar objeto seleccionado* solamente en casos excepcionales. Restaure únicamente aquellos ficheros que pudieron repararse mediante un nuevo análisis.

✓ Fichero analizado y reparado con nuevo análisis.

▶ En el Centro de control seleccione la sección **Administración :: Cuarentena**.

Nota

Los emails y los adjuntos de emails sólo se pueden restaurar con la opción  y con la extensión **.eml*.

Si desea restaurar un fichero en su ubicación original:

▶ Seleccione el fichero y haga clic en el icono (Windows 2000/XP:  , Windows Vista ).

Esta opción no está disponible para emails.

Nota

Los emails y los adjuntos de emails sólo se pueden restaurar con la opción  y con 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.

5.3.11 Cuarentena: mover fichero sospechoso a cuarentena

Así puede mover un fichero sospechoso a la cuarentena:

▶ En el Centro de control seleccione la sección **Administración :: Cuarentena**.

▶ Haga clic en  .

→ Aparece la ventana predeterminada de Windows para seleccionar ficheros.

▶ Seleccione el fichero y confirme.

→ El fichero se mueve a la cuarentena.

Los ficheros que están en la cuarentena se pueden analizar con el escáner AntiVir:

- consulte el capítulo: Cuarentena: tratar con ficheros (*.qua) en cuarentena

5.3.12 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 (sólo posible con la selección manual):

✓ Se encuentra en el Centro de control, en la sección **Protección local ::** *Analizar*.

▶ 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 el 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 (* e ?) como caracteres comodín.

5.3.13 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 programa AntiVir.

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

✓ Se encuentra en el Centro de control, en la sección **Protección local ::** *Analizar*.

▶ 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.

5.3.14 Eventos: Filtrar eventos

En el Centro de control en **Información general :: Eventos** se muestran eventos generados por los componentes de su programa AntiVir (de forma parecida a como lo hace el visor de eventos del sistema operativo Windows). Los componentes del programa son:

- Updater
- Guard
- Escáner
- Programador
- WebGuard
- Servicio de ayuda

Se muestran los siguientes tipos de evento:

- Información
- Advertencia
- Error
- Detección

Así se filtran los eventos mostrados:

- En el Centro de control seleccione la sección **Información general:: 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 esos eventos.

  - O BIEN -

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

6 Escáner

El componente escáner permite ejecutar con precisión análisis para detectar virus y programas no deseados (análisis directo). Dispone de las siguientes posibilidades de analizar ficheros afectados:

- **Análisis directo mediante menú contextual**
  El análisis directo a través del menú contextual (botón derecho del ratón - entrada **Analizar ficheros seleccionados con AntiVir**) se recomienda, por ejemplo, cuando se desee analizar ficheros y directorios individuales en Windows Explorer. Otra ventaja es que no es necesario arrancar primero el Centro de control mediante el menú contextual para realizar un análisis directo.
- **Análisis directo con Arrastrar y soltar**
  Si se arrastra un fichero o directorio a la ventana del Centro de control, el escáner analiza el fichero o el directorio y todos los subdirectorios que contenga. Esto es recomendable si desea analizar ficheros o directorios individualmente, por ejemplo, aquéllos que se encuentran en el escritorio.
- Análisis mediante perfiles
  Esto es lo recomendado si, con frecuencia hace un análisis de determinados ficheros o carpetas (por ejemplo en algún directorio de trabajo o unidad extraíble). No necesita seleccionar estas carpetas y unidades otra vez en cada nuevo análisis, use simplemente el perfil deseado.
- **Análisis directo mediante el programador**
  El programador le permite programar la ejecución de tareas de análisis en el tiempo.

Al analizar la existencia de rootkits, virus del sector de arranque y al analizar procesos activos se requieren procedimientos especiales. Dispone de las siguientes opciones:

- Análisis de rootkits mediante el perfil de análisis *Análisis de malware activo*
- Análisis de procesos activos mediante el perfil de análisis **Procesos activos**
- Análisis de virus del sector de arranque mediante el comando de menú **Analizar virus del sector de arranque** en el menú **Herramientas**

7 Actualizaciones

La eficacia de un software antivirus crece y disminuye con la actualidad del programa, sobre todo la del fichero de firmas de virus y la del motor de análisis. Para la ejecución de actualizaciones, se ha integrado el componente Updater en su AntiVir . El Updater se encarga de que su programa AntiVir funcione siempre con la vigencia más reciente y pueda así detectar los virus que aparecen a diario. Updater actualiza los siguientes componentes:

- Fichero de firmas de virus:

  El fichero de firmas de virus contiene los patrones de detección de los programas malintencionados que utiliza su programa AntiVir en los análisis de virus y malware, así como en la reparación de objetos infectados.

- Motor de análisis:

  El motor de análisis contiene los métodos que usa su programa AntiVir para analizar la existencia de virus y malware.

- Ficheros de programa (actualización de producto):

  Los paquetes de actualización para actualizar los productos proporcionan más funciones para cada uno de los componentes del programa.

Al ejecutar una actualización, se comprueba el grado de vigencia o actualidad del fichero de firmas de virus y del motor de análisis y, si fuera necesario, se actualizan. Según los parámetros establecidos en la configuración, Updater ejecuta, además, una actualización de producto o bien le informa sobre la disponibilidad de actualizaciones de producto. Después de una actualización de producto puede ser preciso un reinicio de su equipo. Si sólo se lleva a cabo una actualización del fichero de firmas de virus y del motor de análisis, no se requiere el reinicio del equipo.

Nota
Por razones de seguridad, Updater comprueba si el fichero host de Windows del equipo se ha modificado en lo que se refiere, por ejemplo, a una manipulación por parte de malware de la URL de actualización con el fin de que Updater se dirija a páginas de descarga no deseadas. Si se manipuló el fichero host de Windows, queda constancia en el fichero de informe de Updater.

Una actualización se ejecuta automáticamente con el siguiente intervalo: 24 horas. Puede modificar o desactivar la actualización automática a través de la configuración (Configuración::Actualización).

En el Centro de control en el programador puede configurar las tareas de actualización que Updater ejecutará con los intervalos indicados. También puede iniciar la actualización manualmente:

- En el Centro de control: en el menú Actualizar y en la sección Estado
- Por medio del menú contextual del icono de bandeja

Las actualizaciones se reciben de Internet a través de un servidor Web del productor. De forma estándar se utiliza la conexión de red existente como conexión con los servidores de descargas de Avira GmbH. Puede cambiar esta configuración predeterminada en la configuración en General :: Actualización.

8 Solución de problemas, sugerencias

En este capítulo encontrará indicaciones importantes sobre la solución de problemas y otras sugerencias para el uso de su programa AntiVir.

consulte el capítulo Ayuda en caso de problemas

consulte el capítulo Comandos de teclado

consulte el capítulo Centro de seguridad de Windows

8.1 Ayuda en caso de problemas

Aquí encontrarás información sobre las causas y las soluciones a los posibles problemas

- El chat en Web no funciona: no se muestran los mensajes de chat

Aparece el mensaje de error *Error de establecimiento de conexión al descargar el fichero...* cuando se intenta iniciar una actualización.

Causa: Su conexión está inactiva. Por ello no se puede establecer una conexión con el servidor Web en Internet.

▶ Compruebe que los servicios de Internet como la navegación o el correo funcionan. Si no, restablece la conexión.

Causa: El servidor proxy no se puede alcanzar.

▶ Compruebe si la información de inicio de sesión para el servidor proxy ha cambiado y cambie su configuración si es necesario.

Causa: El fichero update.exe no está totalmente aprobado por su Firewall .

▶ Asegúrese de que el fichero update.exe está totalmente aprobado por su Firewall .

Si no:

▶ Compruebe los parámetros en la configuración (Modo experto) en General :: Actualización.

Los virus y el malware no se pueden mover ni borrar.

Causa: El fichero ha sido cargado por Windows y está activo

▶ Actualice su producto AntiVir.

▶ Si usa el sistema operativo Windows XP, desactive la Restauración del Sistema.

▶ Arranque el equipo en modo seguro

▶ Inicie el programa AntiVir y la configuración (modo experto).

▶ Seleccione Escáner:: Análisis :: Ficheros :: Todos los ficheros y pulse **Aceptar**.

▶ Inicie un análisis de todos los discos locales

▶ Arranque el equipo en modo normal

▶ Inicie un análisis en modo normal

- Si no se ha encontrado virus o malware, active la Restauración del Sistema.

El icono de bandeja muestra un estado desactivado.

Causa: AntiVir Guard está desactivado.

- Pulse en el Centro de control en la sección Descripción general :: Estado, en el área AntiVir Guard en el enlace **Activar**.

Causa: AntiVir Guard está siendo bloqueado por un Firewall.

- Habilite una autorización general para AntiVir Guard en la configuración de su Firewall . AntiVir Guard sólo trabaja con la dirección 127.0.0.1 (host local). No se ha establecido conexión con Internet.

Si no:

- Compruebe el tipo de inicio del servicio AntiVir Guard. Si fuera el caso, active el servicio: En la barra de inicio seleccione "Inicio | Configuración | Panel de control". Inicie, en el Panel de Control, los "Servicios" con un doble clic (en Windows 2000 y Windows XP los servicios se encuentran en la subcarpeta "Herramientas Administrativas"). Busque la entrada *Avira AntiVir Guard*. El inicio debe ser "Automático" y el estado, "Iniciado". Si es necesario, inicie el servicio manualmente, seleccionando la línea y pulsando sobre "Iniciar". Si aparece un error, compruebe los eventos que aparecen.

El equipo se vuelve extremadamente lento cuando realizo una copia de seguridad.

Causa: Durante el proceso de backup, AntiVir Guard analiza todos los ficheros usados en el procedimiento de ejecución de copias de seguridad de datos.

- En la configuración (modo experto) seleccione Guard:: Análisis :: Excepciones e introduzca el nombre de proceso del software de backup.

Mi Firewall notifica la existencia de AntiVir Guard.

Causa: La comunicación de AntiVir Guard se realiza mediante el protocolo de Internet TCP/IP. Un Firewall monitoriza todas las conexiones con este protocolo.

- Habilite una autorización general para AntiVir Guard. AntiVir Guard sólo trabaja con la dirección 127.0.0.1 (host local). No se ha establecido conexión con Internet.

Nota
Recomendamos que se instalen regularmente las actualizaciones de Microsoft para evitar posibles agujeros de seguridad.

El chat en Web no funciona: no se muestran los mensajes de chat, en el explorador se cargan datos.

Este fenómeno puede aparecer en chats basados en el protocolo HTTP con "transfer-encoding= chunked".

Causa: WebGuard analiza por completo los datos enviados para detectar virus y programas no deseados antes de cargarlos en el explorador Web. En las transferencias de datos con "r;r;transfer-encoding= chunked" el WebGuard no puede detectar la longitud del mensaje o la cantidad de datos.

▶ Indique en la configuración la URL del chat en Web como excepción (consulte configuración: WebGuard::Excepciones).

8.2 Atajos

Los comandos de teclado -conocidos como accesos directos - ofrecen una rápida posibilidad de encontrar módulos individuales, ejecutar acciones y navegar por el programa .

A continuación hacemos un repaso de los comando de teclado disponibles. Consulte las indicaciones adicionales sobre la funcionalidad en el capítulo correspondiente de la ayuda.

8.2.1 En los cuadros de diálogo

Comando de teclado	**Descripción**
Ctrl + Tab Ctrl + Avanzar Página	Navegación en el Centro de control Cambiar a la sección siguiente.
Ctrl + May+ Tab Ctrl + Retroceder Página	Navegación en el Centro de control Cambiar a la sección anterior.
← ↑ → ↓	Navegación en las secciones de configuración En primer lugar, seleccione una sección de configuración mediante el ratón.
Tab	Cambiar a la siguiente acción u opciones de grupo.
May+ Tab	Cambiar a la opción previa u opciones de grupo
← ↑ → ↓	Cambiar entre las opciones en una lista desplegable o entre varias opciones en un grupo de opciones.
Espacio	Activar o desactiva una marca. si la opción activa es una de marcar.
Alt + letra subrayada	Selecciona opción o lanzar comando
Alt + ↓ F4	Abre la lista desplegable seleccionada
Esc	Cerrar el campo de lista desplegable seleccionado. Cancelar el comando y cerrar el cuadro de diálogo.
Intro	Ejecutar comando de la opción o botón activos

8.2.2 En la Ayuda

Comando de teclado	Descripción
Alt + Espacio	Mostrar el menú del sistema
Alt + Tab	Conmuta entre la ayuda y otras posibles ventanas abiertas.
Alt + F4	Cerrar ayuda
May+ F10	Mostrar el menú de contexto de la ayuda.
Ctrl + Tab	Cambiar a la sección siguiente en la ventana de exploración.
Ctrl + May+ Tab	Cambiar a la sección anterior en la ventana de exploración.
Retr. Pág.	Cambia al asunto. el cual se muestra sobre los contenidos, en el índice o en la lista de los resultados encontrados.
Av. Pág.	Cambiar al tema que se muestra debajo del tema actual en el índice de materias, el índice o en la lista de resultados encontrados.
Retr. Pág. Av. Pág.	Avanzar y retroceder por un tema.

8.2.3 En el Centro de control

General

Comando de teclado	Descripción
F1	Mostrar la Ayuda
Alt + F4	Cerrar Centro de control
F5	Refrescar la pantalla
F8	Abrir la configuración
F9	Iniciar actualización

Sección Analizar

Comando de teclado	Descripción
F3	Iniciar análisis con el perfil seleccionado
F4	Crear un acceso directo en el escritorio para el perfil seleccionado

Sección Cuarentena

Comando de teclado	Descripción
F2	Volver a analizar objeto

F3	Restaurar objeto
F4	Enviar objeto
F6	Restaurar objeto en...
Enter	Propiedades
Insertar	Añadir fichero
Suprimir	Eliminar objeto

Sección Programador

Comando de teclado	Descripción
F2	Modificar tarea
Enter	Propiedades
Insertar	Insertar nueva tarea
Suprimir	Eliminar tarea

Sección Informes

Comando de teclado	Descripción
F3	Mostrar fichero de informe
F4	Imprimir fichero de informe
Enter	Mostrar informe
Suprimir	Borrar informes

Sección Eventos

Comando de teclado	Descripción
F3	Exportar eventos
Enter	Mostrar evento
Suprimir	Eliminar eventos

8.3 Centro de Seguridad de Windows

- Windows XP Service Pack 2 o posterior -

8.3.1 General

El Centro de Seguridad de Windows comprueba el estado del equipo en aspectos importantes de seguridad.

Si se detecta un problema en algunos de estos puntos (por ejemplo por tener un antivirus que ha caducado), el Centro de Seguridad crea una alerta y da recomendaciones para proteger al equipo.

8.3.2 El Centro de seguridad de Windows y su programa Antivir

Software de protección / Protección contra software malicioso

Puede recibir la siguiente información del Centro de Seguridad con respecto a su protección Antivirus.

Sin protección antivirus

Protección Antivirus Caducada

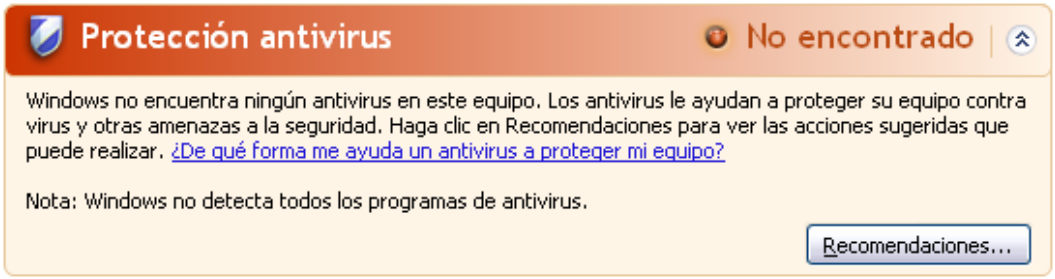
Protección Antivirus ACTIVA

Protección Antivirus INACTIVA

Protección antivirus NO MONITORIZADA

Protección Antivirus NO ENCONTRADA

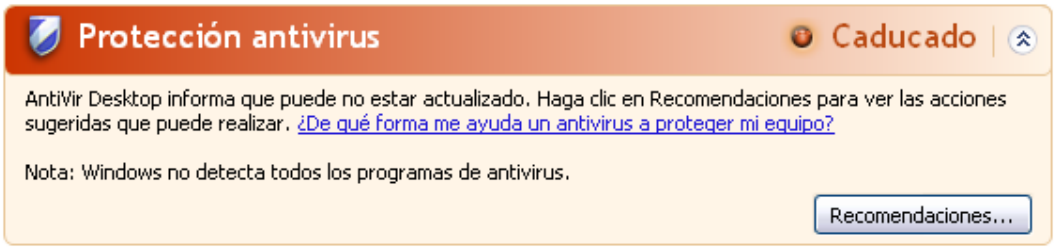
Esta información aparece cuando el Centro de Seguridad de Windows no ha encontrado ningún software antivirus en su equipo.



Nota
Instale su programa AntiVir en su equipo para protegerlo contra virus y otros programas no deseados.

Protección Antivirus NO ACTUAL

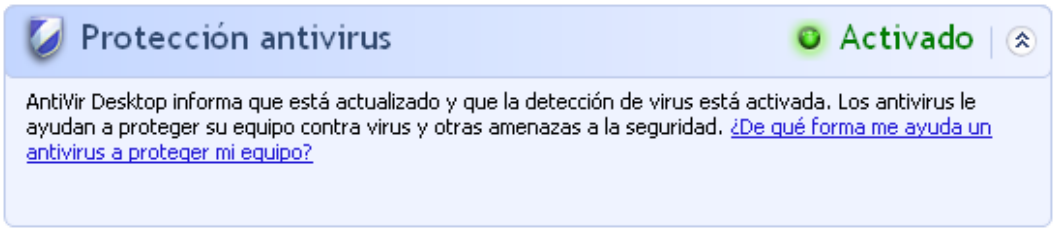
Si ya ha instalado Windows XP Service Pack 2 o Windows Vista e instala después su programa AntiVir, o si instala Windows XP Service Pack 2 o Windows Vista en un sistema que ya tenga instalado su programa AntiVir, recibirá el siguiente mensaje:



Nota
Para que el Centro de seguridad de Windows reconozca a su programa AntiVir como un producto actualizado, debe de llevarse a cabo una actualización forzosamente tras la instalación. Actualice su sistema mediante una Actualización.

Protección Antivirus ACTIVA

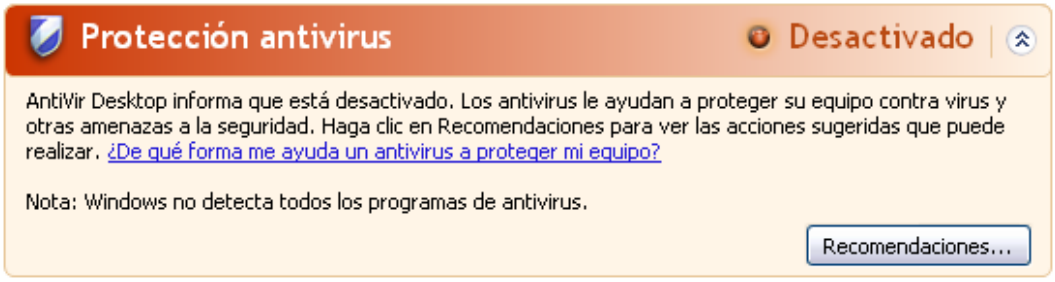
Tras la instalación de su programa AntiVir y la actualización subsecuente, se recibe la siguiente indicación:



Su programa Anti Vir está actualizado y AntiVir Guard está activo.

Protección Antivirus INACTIVA

Recibirá el siguiente mensaje si desactiva AntiVir Guard o detiene el servicio Guard.



Notas

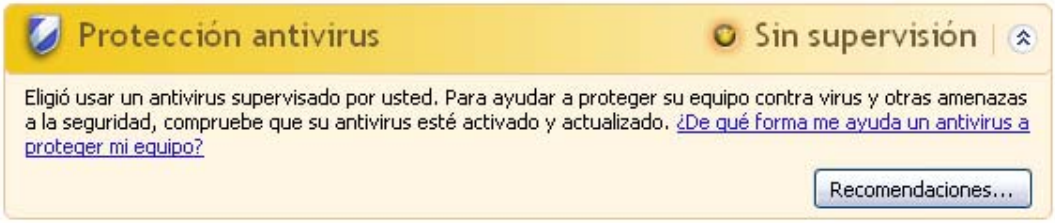
Puede activar o desactivar el AntiVir Guard en la sección Descripción general :: Activar o desactivar el estado del Centro de Control. Además, puede ver que está activado el AntiVir Guard si el paraguas rojo en la barra de tareas está abierto.

Protección Antivirus NO MONITORIZADA

Si recibe el siguiente mensaje del Centro de Seguridad de Windows, ha decidido que quiere monitorizar su software de antivirus por si mismo.

Nota

Windows Vista no admite esta función.



Nota

Su programa AntiVir es compatible con el Centro de seguridad de Windows. Puede activar esta opción siempre que lo desee con el botón "Recomendaciones...".

Nota

Incluso si ha instalado Windows XP Service Pack 2 o Windows Vista, necesita una solución antivirus. Aunque Windows XP Service Pack 2 monitoriza el software de Antivirus, no contiene ninguna función antivirus en si mismo. Por lo tanto ¡necesita una solución Antivirus adicional para estar protegido!

9 Virus y más

9.1 Categorías de riesgos

Programa de marcación telefónica con coste (DIALER)

Algunos servicios en Internet son de pago. A éstos pueden accederse mediante dialers (marcadores) que pudieran estar conectados a la línea telefónica (normalmente los 9XX). Instalados en el equipo, estos programas (denominados dialer) se encargan de establecer conexiones a través de números de tarifa de cobro adicional, cuya configuración puede abarcar un espectro muy amplio.

La comercialización de contenidos en línea a través de la factura telefónica es legal y puede tener ventajas para el usuario. Los dialers serios no permiten que surjan dudas acerca del uso consciente y moderado por parte del cliente Únicamente se instalan en la máquina del usuario si éste da su conformidad al respecto. Esta conformidad debe darse a raíz de un etiquetado o una petición unívocos y claramente reconocibles. El establecimiento de la conexión de los programas tipo dialer serios se muestra de forma inequívoca. Además, los dialer serios informan con exactitud y de forma llamativa sobre el importe de los costes que implican.

Lamentablemente, existen dialers que se instalan en los equipos disimuladamente, de manera cuestionable o incluso con intenciones fraudulentas. Por ejemplo, reemplazan la conexión de acceso telefónico a redes predeterminada del usuario de Internet con su ISP (proveedor de servicios de Internet) y llaman en cada conexión a un número 0190/0900 que genera gastos y presenta tarifas exorbitantes. Además, es posible que, hasta no recibir la próxima factura telefónica, el usuario afectado no se dé cuenta de que un programa no deseado tipo dialer ha estado marcando cada vez que se establecía una conexión a Internet un número con tarifa de cobro adicional, por lo que sus gastos han crecido drásticamente.

Para protegerse en general frente a programas no deseados de marcación telefónica con coste (dialers de 0190/0900), recomendamos contactar con la compañía que le ofrece el servicio de telefonía para que bloquee ese rango de números.

Su programa AntiVir detecta los programas de marcación telefónica con coste conocidos.

Si en la configuración de Categorías de riesgos se activa con una marca la opción **Programas de marcación telefónica con coste (DIALER)**, si se detecta un programa de este tipo se emite el correspondiente mensaje de advertencia. Así puede eliminar el potencial peligro de los dialers no deseados. De todas formas si hay algún dialer que desee utilizar, puede declararlo como archivo excepcional y excluirlo del análisis en el futuro.

Juegos (GAMES)

Los juegos pueden ser evitados a la hora de trabajar. La cantidad de juegos accesibles desde Internet puede ser una amenaza a la productividad. La selección de posibles juegos en Internet es inmensa. Incluso el juego por email se está haciendo popular: existen numerosas variantes de juegos de este tipo desde los de ajedrez hasta los especializados en "estrategias navales" (batallas con torpedos incluidas). Las rondas de juego se envían a través de programas de correo a los contrincantes y éstos las contestan.

Las investigaciones demuestran que el tiempo dedicado a jugar con el equipo en horario laboral alcanza ya magnitudes económicamente importantes. Así que no sorprende que las empresas se tomen en serio este tipo de posibles problemas.

Su programa AntiVir reconoce los juegos de ordenador. Activando en la configuración de Categorías de riesgos la opción **Juegos (GAMES)** con una marca, recibirá la correspondiente advertencia en caso de que su programa AntiVir realice una detección. El juego ha terminado en el sentido literal, porque tiene la posibilidad de eliminarlo fácilmente.

Programas broma (JOKES)

Los programas de broma sólo deberían estar destinados a poner un toque de humor sin llegar a ocasionar perjuicios ni multiplicarse a sí mismos. El equipo suele empezar a emitir una melodía o a mostrar algo inusual en pantalla tras haber activado el programa de broma. Ejemplos clásicos son: DRAIN.COM (lavadora en la disquetera) o BUGSRES.COM (come pantallas).

Pero... ¡cuidado! Los síntomas de los programas de broma pueden ser también el resultado de virus o troyanos. Cuanto menos, intentan llamar la atención y entonces el usuario por desconocimiento puede provocar aún más daño.

Su programa AntiVir puede detectar los programas de broma ampliando sus rutinas de análisis e identificación y eliminarlos, tratándolos como programas no deseados, si fuera necesario. Activando en la configuración Categorías de riesgos la opción **Programas broma (JOKES)** con una marca se informa en caso de realizarse una detección.

Riesgo de seguridad-confidencialidad (Security privacy risk - SPR)

Software que puede comprometer la seguridad del sistema, iniciar actividades de programas no deseadas, violar su privacidad o espiar datos y/o comportamientos, lo que probablemente no sea deseado.

Su programa AntiVir detecta el software de "Riesgo de seguridad-confidencialidad". Si se activa la opción **Riesgo de seguridad-confidencialidad (SPR)** en Categorías de riesgos avanzadas con una marca, se recibirán alertas si su programa AntiVir detecta software de este tipo.

Software de control de puerta trasera (backdoor - BDC)

Para el robo de datos o la manipulación del equipo, se introduce un programa backdoor "por la puerta trasera" sin que el usuario lo detecte. Este programa puede ser controlado por terceras personas vía Internet o en un entorno de red.

Su programa AntiVir reconoce el "software de control de puerta trasera". Activando en la configuración de Categorías de riesgos la opción **Software de control de puerta trasera (BDC)** con una marca, recibirá la correspondiente advertencia en caso de que su programa AntiVir realice una detección.

Adware/Spyware (ADSPY)

Software que muestra anuncios publicitarios, mensajes o envía datos del usuario a terceras personas a menudo sin el consentimiento ni el conocimiento de éste.

Su programa AntiVir reconoce el "adware/spyware". Activando en la configuración de Categorías de riesgos la opción **Adware/Spyware (ADSPY)** con una marca, recibirá la correspondiente advertencia en caso de que su programa AntiVir realice una detección.

Utilidades de compresión poco habituales (PCK)

Ficheros que se han comprimido con un formato de compresión atípico y que, por lo tanto, son posiblemente sospechosos.

Su programa AntiVir reconoce "utilidades de compresión poco habituales". Si se configura **Utilidades de compresión poco habituales (PCK)** en Categorías de riesgos, recibirá una advertencia si su programa AntiVir realiza una detección.

Ficheros de doble extensión (HEUR-DBLEXT)

Estos ficheros enmascaran su extensión de una forma sospechosa. A menudo se considera como malware.

Su programa AntiVir detecta "ficheros de doble extensión". Si en la configuración de Categorías de riesgos avanzadas se activa la opción **Ficheros de doble extensión (HEUR-DBLEXT)** con una marca, recibirá la alerta correspondiente si su programa AntiVir realiza una detección.

Suplantación de identidad (phishing)

El Phishing, también conocido como *Suplantación de marca* pretende sustraer datos de clientes que acceden a servicios bancarios, oficiales, proveedores de servicios, etc. en Internet.
La divulgación de la dirección de email en Internet, rellenar formularios en línea, darse de alta en grupos de noticias o páginas Web puede provocar que los denominados "Internet crawling spiders" puedan robar sus datos y utilizarlos sin su consentimiento en estafas u otros delitos.

Su programa AntiVir detecta la "suplantación de identidad (phishing)". Si se activa la opción **Phishing** enCategorías de riesgos, se recibirán alertas cuando su programa AntiVir detecte un comportamiento de este tipo.

Aplicación (APPL)

EL término APPL se refiera a una aplicación que implica riesgo al ser utilizada o tiene un origen dudoso.

Su programa AntiVir reconoce una "aplicación (APPL)". Si se activa la opción **Aplicación (APPL)** enCategorías de riesgos, se recibirá la alerta coprrespondiente cuando su programa AntiVir detecte un comportamiento de este tipo.

9.2 Virus y otro tipo de Malware

Adware

Adware es software que muestra banners (mensajes o anuncios) en ventanas emergentes que aparecen en la pantalla. Estos anuncios normalmente no pueden quitarse y por lo tanto siempre están visibles. Estos programas pueden ofrecer muchos datos del usuario y son problemáticos en términos de seguridad.

Backdoors (software de control de puerta trasera)

Los backdoors (castellano: puerta trasera) intentan coger el control del equipo, saltándose los mecanismos habituales de seguridad.

Un programa que se ejecute de manera oculta (una tarea invisible concurrente) en general concede al atacante derechos casi ilimitados. Con los backdoor se puede espiar, pero se utilizan normalmente para instalar otro tipo de virus o gusanos, creando un peligro adicional. Estos programas pueden ofrecer muchos datos del usuario y son problemáticos en términos de seguridad.

Virus del sector de arranque

El sector de arranque maestro de los discos duros se infecta mayormente con estos tipos de virus. Los cuales sobrescriben información importante necesaria para la ejecución del sistema. Una de las posibles consecuencias: que el equipo no se pueda reiniciar más...

Bot-Net (red de robots)

Una Bot-Net se define como una red remota de PC, la cual se compone de bots (robots de software) en comunicación entre sí. La red de robots se compone de una serie de equipo atacados que ejecutan programas (normalmente troyanos o gusanos) bajo una infraestructura de control común. Estas redes pueden usarse para propagar spam, realizar ataques DDoS (denegación de servicio distribuido), etc., en parte sin que el usuario del PC afectado lo descubra. El peligro principal de las redes de robots es que pueden componerse de miles de equipo y la suma de su tráfico generado puede agotar el ancho de banda de los accesos convencionales a Internet.

Exploit (vulnerabilidades)

Un exploit (agujero de seguridad) es un programa que aprovecha algún fallo o vulnerabilidad que permita controlar el sistema o crear una denegación de servicio en un equipo. Una caso de exploit, por ejemplo, son ataques desde Internet con las ayuda de paquetes de datos manipulados. Los programas pueden infiltrarse para obtener un acceso con mayores permisos.

Hoaxes (del inglés: hoax - bulo, engaño, broma de mal gusto)

Los usuarios reciben alertas de virus en Internet y en otras redes que se supone se han extendido vía email. Estas alertas se extienden por email de forma exponencial, ya que a los usuarios se les urge a que expandan la alerta para evitar el "peligro" sin ningún tipo de comprobación real.

Honeypot (foco de atracción, equipo trampa)

Un honeypot es un servicio (en forma de programa o para servidores) que se instala en una red. Tiene la función de monitorizar una red y desarrollar los protocolos de ataques. Este servicio está oculto al usuario legítimo, ya que nunca se hace notar. Si un atacante examina una red en busca de puntos débiles y usa los servicios ofrecidos por el honeypot, se protocoliza y se crea una alerta.

Macrovirus

Los macrovirus son programas que se escriben en lenguajes de macros de la aplicación (por ejemplo Word) y que normalmente sólo pueden propagarse dentro de los documentos de esa aplicación. Por ello, también se conocen como virus de documento. Para ser activos, necesitan de las aplicaciones correspondientes y que sean ejecutados en las mismas. A diferencia de los virus "normales", los macrovirus no atacan a archivos ejecutables sino a documentos de la aplicación anfitriona correspondiente.

Pharming (redirección de nombres de dominio)

El pharming es la manipulación del fichero host o los navegadores para que se hagan peticiones a sitios Web con pretensiones maliciosas. Es un desarrollo del clásico phishing. Los practicantes de pharming manipulan su conjunto de equipo infectados para almacenar datos con pretensiones maliciosas. El pharming se ha establecido como un término que abarca varios tipos de ataques DNS. En el caso de la manipulación del fichero host, un virus o troyano manipula de forma específica el sistema. El resultado es que el sistema sólo puede acceder a sitios Web predeterminados, incluso si se introducen direcciones correctas en el navegador.

Suplantación de identidad (phishing)

Se conoce como phishing la búsqueda no autorizada de datos personales del usuario en Internet. Los atacantes que utilizan phishing normalmente envían a sus víctimas emails aparentemente oficiales en los que inducen a desvelar datos personales tales como números de tarjeta o claves para acceder a servicios bancarios o comerciales. Con los datos sustraídos, los atacantes podrían asumir la identidad de sus víctimas y realizar transacciones en su nombre. Una cosa está clara: los bancos y las compañías de seguros nunca solicitan el envío de número de tarjetas de crédito, PIN, TAN u otros datos de acceso por email, SMS teléfono.

Virus polimórficos

Los virus polimórficos son auténticos maestros del disfraz. Cambian su propio código, por lo que son muy difíciles de detectar.

Virus de programas

Un virus de equipo es un programa que es capaz de anexarse a otro programa tras ejecutarse, creando así una infección. Los virus se multiplican a si mismos, a diferencia de las bombas lógicas y los troyanos. En contraste con un gusano (worm), un virus siempre requiere de un programa portador, en el cual el virus deposita su código. La ejecución normal del programa anfitrión original, en apariencia no cambia.

Rootkit

Un rootkit es una colección de herramientas de software que, tras penetrar en un sistema informático, se instalan para ocultar los inicios de sesión del intruso, ocultar procesos y espiar la información, es decir, actuar de forma invisible. Intentan actualizar programas espía ya instalados y volver a instalar el spyware eliminado.

Virus de script y gusanos

Tales virus son fáciles de programar y se pueden extender -con la tecnología adecuada- en sólo unas horas, vía email, por todo el globo.

Los virus de script y gusanos utilizan un lenguaje de script, como Javascript, VBScript etc., para infiltrarse en otros scripts nuevos o propagarse mediante la ejecución de funciones del sistema operativo. Este ocurre frecuentemente por email o mediante el intercambio de ficheros (documentos).

Un gusano es un programa que se multiplica por si mismo, sin infectar a otros. Los gusanos consecuentemente no forman parte de otros programas. Los gusanos son, a menudo, la única posibilidad de infiltrarse en sistemas con medidas de seguridad restrictivas.

Spyware

Se conoce por spyware a programas espías que interceptan o toman control parcial de un equipo, sin que el usuario se dé cuenta de ello. El spyware está diseñado para explotar los equipos en busca de un algún beneficio, normalmente fraudulento.

Troyanos

Los troyanos son muy comunes actualmente. Son programas que pretenden tener alguna función en particular pero que, al ejecutarse, desarrollan otra función, en el mayor de los casos, destructiva. Los troyanos no se multiplican ellos mismos, lo que los diferencia de los virus y gusanos. La mayoría de ellos tienen un nombre llamativo (SEX.EXE o leeme.EXE), con la intención de que el usuario lo ejecute. En cuanto se ejecutan pueden ejecutar cualquier acción, por ejemplo: formatear el disco duro. Un dropper es una forma especial de troyano que crea virus en el equipo atacado.

Zombie

Un PC zombie es un ordenador infectado con malware que permite a los hackers o piratas el abusar de otros ordenadores vía control remoto con propósitos criminales. El equipo infectado, inicia, por ejemplo, ataques por denegación de servicio o envía correo no solicitado (spam) o emails de suplantación de identidad (phishing).

10 Información y servicio

En este capítulo se ofrece información acerca de 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 una falsa alarma

10.1 Dirección de contacto

Si tiene cualquier pregunta o sugerencia acerca de cualquier producto AntiVir, estaremos encantados de ayudarle. Encontrará nuestras direcciones de contacto en el Centro de control en Ayuda :: Acerca de Avira AntiVir Personal.

10.2 Soporte Técnico

El soporte Avira está a su disposición para responder a sus preguntas o solucionar problemas técnicos con toda fiabilidad.

Toda la información necesaria sobre nuestro amplio servicio de soporte se puede obtener en nuestro sitio Web:

http://www.avira.es/classic-support

Para que podamos ofrecerte ayuda de forma rápida y eficiente, deberías tener preparada la siguiente información:

- **Información de versión**. La encontrará en la interfaz del programa en la opción de menú Ayuda:: Acerca de Avira AntiVir Personal :: Información de versión.
- **Versión de Sistema operativo**y los Service-Packs instalados.
- **Software instalado**, ej. antivirus de otras casas.
- **Mensaje exacto** del programa o del fichero de informe.

10.3 Archivos sospechosos

Los virus que no hayan sido detectados o eliminados por nuestros productos o archivos sospechosos se nos pueden enviar. Le ofrecemos varias vías para hacerlo.

- Seleccione el fichero en el Gestor de cuarentena del Centro de control y seleccione a través del menú contextual o el botón correspondiente el punto Enviar fichero.

– Envíe el fichero deseado comprimido (WinZIP, PKZip, Arj, etc.) adjunto en un email a la siguiente dirección:
virus-pe@avira.es
Como algunos servidores de correo trabajan con programas antivirus, también deberá poner una contraseña al archivo o archivos que desee enviar (por favor recuerde decirnos la contraseña).

10.4 Informe falso positivo

Si cree que su programa AntiVir notifica la detección de un fichero que muy probablemente esté "limpio", envíe ese fichero comprimido (WinZIP, PKZIP, Arj, etc.) adjunto en un email a la siguiente dirección:

– virus-pe@avira.es

Como algunos servidores de correo trabajan con programas antivirus, también deberá poner una contraseña al archivo o archivos que desee enviar (por favor recuerde decirnos la contraseña).

11 Referencia: opciones de configuración

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

11.1 Escáner

La sección Escáner de la configuración se encarga de la configuración del análisis directo, es decir del análisis a petición.

11.1.1 Análisis

Aquí se define el comportamiento básico de la rutina de búsqueda en caso de análisis directo. Si selecciona determinadas carpetas en un análisis directo, dependiendo de la configuración, el escáner analiza:

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

Ficheros

El escáner puede usar un filtro para analizar sólo ficheros con una determinad extensión (tipo).

Todos los ficheros

Con esta opción seleccionada se analizan todos los ficheros sin tener en cuenta su extensión ni contenido en busca de virus o programas no deseados. No se utilizará ningún filtro.

Nota
Si se activa Todos los ficheros , el botón **Extensiones de ficheros** no se puede seleccionar.

Extensiones inteligentes

Con esta opción activada, el programa selecciona de forma completamente automática los ficheros a analizar. Es decir, su programa AntiVir decide, dependiendo del contenido de un fichero, si éste se analizará o no en cuanto a virus y programas no deseados. Este procedimiento es algo más lento que usar la lista de extensiones de ficheros, pero más seguro, ya que no se analiza únicamente en base a la extensión del fichero. Esta configuración está activada de forma estándar y es la recomendada.

Nota
Si se activa las extensiones inteligentes el botón **Extensiones de fichero** no puede seleccionarse.

Usar lista de extensiones de fichero

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

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

Extensiones de fichero

Con la ayuda de este botón se abre una ventana de diálogo en la que aparecen todas las extensiones a analizar en el modo "**Usar lista de extensiones de fichero"**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota
La lista estándar puede variar entre versiones.

Configuración adicional

Analizar los sectores boot (de arranque) de los discos seleccionados

Con esta opción seleccionada el escáner sólo analiza los sectores de arranque de las unidades seleccionadas para al análisis directo. Este ajuste está activado de forma estándar.

Analizar sect. arranque maestros

Con esta opción activada, el escáner sólo analiza los sectores de arranque maestros de los discos duros usados en el sistema.

Omitir ficheros offline

Si se activa esta opción, el análisis directo omite por completo los llamados ficheros offline durante el análisis. Es decir, que no se analiza los mismos en busca de malware. 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.

Compr. integridad ficheros del sistema

Si está activada la opción, 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 ello, esta opción está desactivada de forma estándar.

Importante
Esta opción sólo está disponible a partir de Windows Vista.

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

Análisis optimizado

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

Nota
Esta opción sólo está disponible en equipos con multiprocesador.

Seguir enlaces simbólicos

Si la opción está activada, el escáner 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 existencia de virus y malware. Esta opción no es compatible con Windows 2000 y está desactivada de forma estándar.

Importante
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

Con esta opción activada, al inicio del análisis el escáner comprueba si hay rootkits activos en el directorio de sistema de Windows con el 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.

Importante
¡La búsqueda de rootkits no está disponible en Windows XP 64 Bit !

Analizar el registro

Con esta opción activada, se analiza el registro en búsqueda de indicios de software dañino.

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"** en la ventana del "Luke Filewalker". Si ha desactivado este ajuste, el botón **Detener** de la ventana del "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

Con el análisis directo, el escáner 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.

Bajo

El sistema operativo únicamente asigna tiempo de procesador al escáner si ningún otro proceso necesita tiempo de procesador, es decir, mientras sólo se esté ejecutando el escáner, 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 el escáner continúa ejecutándose en segundo plano. Esta configuración está activada de forma estándar y es la recomendada.

Medio

Al escáner se le asigna una prioridad normal. El sistema operativo asigna a todos los procesos la misma cantidad de tiempo de procesador. En ciertas circunstancias, puede afectarse el rendimiento de otras aplicaciones.

Alto

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

11.1.1.1. Acción en caso de detección

Acción en caso de detección

Puede definir las acciones que debe tomar el escáner cuando se detecta un virus o programa no deseado.

Interactiva

Si se activa esta opción, las detecciones del análisis del escáner se notifican en un cuadro de diálogo. Durante la búsqueda del escáner se recibe al finalizar el análisis un mensaje de advertencia con una lista de los ficheros afectados detectados. Tiene la posibilidad de seleccionar mediante el menú contextual la acción que se ejecutará para cada uno de los ficheros afectados. Puede ejecutar las acciones seleccionadas para todos los ficheros afectados o finalizar el escáner.

Nota
En el cuadro de diálogo para el tratamiento? de virus figura como acción predeterminada 'Mover a cuarentena'. A través de un menú contextual puede seleccionar otras acciones.

Encontrará más información aquí.

Automático

Si esta opción está activada, entonces no mostrará la ventana de acciones después de una detección de un virus o programa no deseado. El escáner reacciona de acuerdo a lo que configure en esta sección.

Copiar fichero a cuarentena antes de la acción

Si se activa esta opción, el escáner crea una copia de seguridad (backup) antes de llevar a cabo la acción principal o secundaria pertinente. La copia se guarda en cuarentena desde donde luego puede restaurarse si tienes algún valor informativo. Además puede enviar la copia al Avira Malware Research Center para que sea analizada a fondo.

Acción Primaria

La acción primaria es la que se ejecuta cuando el escáner detecta un virus o programa no deseado. Si seleccionó la opción "**reparar"** pero no es posible reparar el fichero afectado, se ejecuta la acción seleccionada en "**Acción secundaria"**.

Nota
La opción **Acción Secundaria** sólo puede seleccionarse si se ha configurado la **Opción primaria** como **Reparar**.

reparar

Con esta opción seleccionada el escáner repara los ficheros automáticamente. Si el escáner no puede reparar el fichero afectado, ejecuta alternativamente la opción seleccionada en Acción secundaria.

Nota
Se recomienda la reparación automática, pero eso significa que el escáner puede modificar los ficheros del equipo.

eliminar

Con esta opción activada, el fichero se borra.

cambiar el nombre

Con esta opción activada, el escáner renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Los ficheros pueden repararse posteriormente y renombrarse otra vez con su nombre original

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia
¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

Cuarentena

Con está opción activada el escáner mueve el fichero a cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse al Avira Malware Research Center.

Acción secundaria

La opción "**Acción Secundaria"** sólo puede seleccionarse si se ha seleccionado como "**Acción Principal"** el ajuste **Reparar**. Con esta opción se decide qué debe hacerse si el fichero afectado no puede repararse.

eliminar

Con esta opción activada, el fichero se borra.

cambiar el nombre

Con esta opción activada, el escáner renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Los ficheros pueden repararse posteriormente y renombrarse otra vez con su nombre original

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia
¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

Cuarentena

Con está opción activada el escáner mueve el fichero a cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse al Avira Malware Research Center.

Nota
Si ha seleccionado como acción principal o secundaria **Eliminar** o tenga en cuenta lo siguiente: en caso de detección mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a cuarentena.

Cuando el escáner 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 ficheros se analizan, descomprimen y vuelven a analizarse.

Analizar archivos comprimidos

Con esta opción activada, se analizan los archivos comprimidos seleccionados en la lista. Este ajuste está activado de forma estándar.

Todos los tipos de archivo comprimido

Con esta opción se seleccionan y analizan todos los archivos comprimidos en la lista.

Extensiones inteligentes

Con esta opción activa, el escáner detecta si un fichero tiene un formato de archivo comprimido, incluso si su extensión no lo refleja, y analiza el archivo. De todas formas, esto significa que se deben de abrir todos los ficheros, lo que reduce la velocidad de análisis. Ejemplo: si un archivo *.zip tiene la extensión de fichero *.xyz , el escáner descomprime también este archivo y lo analiza. Este ajuste está activado de forma estándar.

Nota
Sólo se soportan aquéllos tipos de archivos comprimidos marcados en la lista de archivos comprimidos.

Limitar la profundidad en la recursividad

El 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 archivos 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, el escáner 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 Límite de profundidad 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 introducción. Los valores permitidos van del 1 al 99. El valor predeterminado es 20 y es el recomendado.

Valores predeterminados

Este botón restableces los valores predefinidos cuando se analizan comprimidos.

Lista de archivos comprimidos

En este apartado puede establecer qué archivos comprimidos debe analizar el escáner. Para ello debe seleccionar las entradas relevantes.

11.1.1.2. Excepciones

Ficheros a excluir por el escáner

La lista en esta ventana contiene los ficheros y rutas que no deben ser incluidas en el análisis en busca de virus o programas no deseados por el escáner.

Introduzca las mínimas excepciones posibles que considere que 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 6 000 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 objeto fichero que no desee incluir en el análisis directo. No hay ningún fichero objeto fichero introducido de forma estándar.

El botón abre una ventana en la que puede seleccionar el fichero o la ruta pertinente. Cuando introduce un fichero con su ruta completa, sólo 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 de visualización el objeto fichero introducido en el campo de entrada.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Nota
Si añade toda una partición a la lista de los objetos fichero que deben excluirse, sólo se excluyen del análisis los ficheros guardados directamente debajo de la partición y no los ficheros que estén en directorios en esa partición.
Ejemplo: objeto fichero que se debe excluir: `D:\` = `D:\file.txt` se excluye del análisis del escáner, `D:\folder\file.txt` no se excluye del análisis.

11.1.1.3. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, se detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta configuración está activa por defecto si ha seleccionado el uso de esta heurística.

Nivel de detección alto

Si está activada la opción, se detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

11.1.2 Informe

El escáner tiene una completa funcionalidad sacando informes. Así puede obtener información muy precisa del resultado del análisis directo. El fichero de informe contiene todas las entradas del sistema, así como advertencias y mensajes del análisis directo.

Nota
Para que pueda establecer qué acciones ha tomado el escáner al detectar un virus o programa no deseado, debería crearse siempre un fichero de informe.

Protocolización

Desactivado

Si esta opción está activada, el escáner no informa de las acciones o resultados de un análisis directo.

Predeterminado

Si se selecciona esta opción, el escáner 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 licenciatario.

Ampliado

Con esta opción activada, el escáner informa de alertas e instrucciones, además de los nombres y rutas de los ficheros afectados.

Completo

Si se selecciona esta opción, el escáner 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.

11.2 Guard

La sección Guard es responsable de la configuración del análisis en tiempo real.

11.2.1 Análisis

Normalmente deseará monitorizar su sistema de forma constante. Para ello utiliza el Guard (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 existencia de virus y programas no deseados.

Modo de análisis

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

Analizar al leer

Si esta opción está activada, el Guard analiza los ficheros antes de que sean leídos o ejecutados por la aplicación o el sistema operativo.

Analizar al escribir

Si esta opción está activada, el Guard analiza el fichero al ser escrito. Sólo puede acceder al fichero de nuevo cuando se haya completado el proceso.

Analizar al leer y escribir

Si esta opción está activada, el Guard analiza los ficheros antes de ser abiertos, leídos, ejecutados y después de ser escritos. Este ajuste está activado de forma estándar y es el recomendado.

Ficheros

El Guard puede usar un filtro para analizar sólo ficheros de una cierta extensión (tipo).

Todos los ficheros

Si esta opción está activada, se analizan si hay virus o programas no deseados en todos los ficheros, independientemente de su contenido y su extensión.

Nota
Si se activa Todos los ficheros , el botón **Extensiones de ficheros** no se puede seleccionar.

Extensiones inteligentes

Con esta opción activada, el programa selecciona de forma completamente automática los ficheros a analizar. Esto significa que el programa decide, dependiendo del contenido, si se debe comprobar la existencia de virus y programas no deseados en los ficheros. Este procedimiento es algo más lento que usar la lista de extensiones de ficheros, pero más seguro, ya que no se analiza únicamente en base a la extensión del fichero.

Nota
Si se activa las extensiones inteligentes el botón **Extensiones de fichero** no puede seleccionarse.

Usar lista de extensiones de fichero

Con esta opción activada, sólo se analizan ficheros de la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están preseleccionados. Esta lista puede editarse manualmente con el botón "**Extensiones de ficheros"**. Esta configuración está activada de forma estándar y es la recomendada.

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

Extensiones de fichero

Con la ayuda de este botón se abre una ventana de diálogo en la que aparecen todas las extensiones a analizar en el modo "**Usar extensiones de la lista de ficheros"**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota
La lista de extensiones de ficheros puede variar entre versiones.

Archivos

Analizar archivos

Si está activa esta opción, se analizarán los archivos comprimidos. Los archivos comprimidos se analizan, se descomprimen y se analizan de nuevo. Esta opción no está activa 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 analizarán y el tamaño máximo del archivo comprimido.

Nota
Esta opción no está activa de forma estándar, ya que sobrecarga mucho al procesador. En general se recomienda que los archivos comprimidos se comprueben con el análisis directo.

Nivel máximo de recursividad

Al realizar análisis de archivos el Guard usa 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 archivos que se encuentren directamente en el archivo principal.

Máximo número de ficheros

Al analizar archivos comprimidos 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)

Al analizar archivos el análisis se limita a un tamaño máximo del archivo que se descomprimirá. Se recomienda el valor estándar de 1 000 KB.

11.2.1.1. Acción en caso de detección

Notificaciones

Usa el registro de eventos

Si esta opción esta activada, se añade una entrada en el registro de eventos de Windows con cada detección. Los eventos pueden abrirse en el visor de eventos de Windows. Este ajuste está activado de forma estándar.

Inicio automático

Bloquear función de inicio automático

Con esta opción activada, se bloquea la ejecución de la función de inicio automático de Windows en todas las unidades conectadas tales como lápices USB, unidades de CD y DVD, unidades de red. Con la función de inicio automático de Windows se leen inmediatamente los ficheros al insertar portadatos o conectar unidades de red, permitiendo así el inicio y ejecución automática de los ficheros. Sin embargo, esta funcionalidad conlleva un elevado riesgo de seguridad ya que el inicio automático de ficheros permite la instalación de malware y programas no deseados. La función de inicio automático es especialmente crítica para lápices USB, ya que los datos de un lápiz pueden cambiar constantemente.

Excluir CD y DVD

Con esta opción activada, se permite la función de inicio automático en las unidades de CD y DVD.

Advertencia

Desactive la función de inicio automático para unidades de CD y DVD sólo si está seguro de utilizar únicamente portadatos de confianza.

11.2.1.2. Excepciones

Estas opciones permiten configurar los objetos de excepción para el Guard (análisis en tiempo real). Los objetos en cuestión no se considerarán en el análisis en tiempo real. Mediante la lista de procesos omitidos, el Guard puede omitir sus accesos a ficheros durante el análisis en tiempo real. Esto resulta útil en el caso de bases de datos o de soluciones de copia de seguridad.
Tenga en cuenta lo siguiente al indicar los procesos y los objetos de fichero que deben omitirse: La lista se procesa de arriba a abajo. Cuanto más larga es la lista, más tiempo de procesador se requiere para procesar la lista en cada acceso. Por lo tanto se recomienda que las listas sean lo más cortas posible.

Procesos omitidos por Guard

Todos los accesos a ficheros de los procesos que constan en esta lista se excluyen de la supervisión por parte del Guard.

Campo de entrada

En este campo se introduce el nombre del proceso que no debe considerarse durante el análisis en tiempo real. De forma estándar no hay ningún proceso indicado.

Nota

Puede introducir un máximo de 128 procesos.

Nota
Al indicar el proceso se aceptan caracteres Unicode. Por ello, puede indicar nombres de procesos o directorios que contienen caracteres especiales.

Nota
Tiene la posibilidad de excluir procesos sin la indicación completa de la ruta de monitorización del Guard:
aplicación.exe
No obstante, esto es válido exclusivamente para procesos cuyos ficheros ejecutables se encuentren en unidades del disco duro.
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 lápiz de memoria USB.

Nota
Las unidades de deben indicar de la siguiente forma: [letra de la unidad]:\
El carácter de dos puntos (:) sólo puede utilizarse para indicar unidades.

Nota
Al indicar el proceso puede utilizar los comodines * (sin límite de caracteres) e ? (un solo 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 monitorización del Guard, se consideran no válidos los datos formados exclusivamente por los siguientes caracteres: * (asterisco), ? (interrogante), / (barra), \ (barra invertida), . (punto), : (dos puntos).

Nota
La ruta y el nombre de fichero del proceso no deben superar un máximo de 255 caracteres. La suma de las entradas de la lista no puede superar el máximo de 6 000 caracteres.

Advertencia
¡Tenga en cuenta que todos los accesos a ficheros por procesos anotados en la lista son excluidos del análisis en busca de virus y programas no deseados! Windows Explorer y el sistema operativo en sí no pueden excluirse. La entrada correspondiente de la lista se ignorará.

Al pulsar el botón se abre una ventana en la que puede seleccionar un fichero ejecutable.

Procesos

El botón "**Procesos"** abre la ventana "*Selección de proceso"*, donde se indican los procesos activos.

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 a excluir por Guard

Todos los accesos a objetos de esta lista son excluidos del análisis realizado por Guard.

Campo de entrada

En este campo puede introducir el nombre del objeto fichero que no debe incluirse en el análisis en tiempo real. No hay ningún fichero objeto fichero introducido de forma estándar.

Nota
Al indicar los objetos de fichero que deben omitirse, puede utilizar los comodines * (sin límite de caracteres) e ? (un solo carácter). También se pueden excluir distintas extensiones de fichero (incluidos los comodines):
C:\Directorio*.mdb
*.mdb
*.md?
.xls
C:\Directorio*.log

Nota
Los nombres de directorio deben acabar con una barra diagonal inversa \; de no ser así, se supone que se trata de un nombre de fichero.

Nota
La suma de las entradas de la lista no puede superar el máximo de 6 000 caracteres.

Nota
Si se excluye un directorio, todos sus subdirectorios se excluyen automáticamente.

Nota
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

Nota
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 del Guard permite determinar el nombre de alias del sistema operativo que se debe usar.

El botón abre una ventana en la que puede seleccionar el objeto a excluir.

Añadir

Este botón permite incluir en la ventana de visualización el objeto fichero introducido en el campo de entrada.

Eliminar

Con este botón, puede borrar el objeto seleccionado que aparece en la ventana.

Al indicar excepciones, tenga en cuenta lo siguiente:

Nota
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 excepción!

Nota
Mediante el fichero de informe del Guard puede determinar las rutas que usará el Guard 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 del Guard en la configuración, en Guard :: informe, en **Completo**. Con el Guard activado, acceda a los ficheros, directorios, unidades incorporadas . Ahora puede leer la ruta que debe usarse en el fichero de informe del Guard . El fichero de informe se activa en el Centro de control en Protección local :: Guard.

Ejemplos de procesos que deben excluirse:

- aplicación.exe

  El proceso de aplicación.exe queda excluido del análisis del Guard, independientemente de en qué unidad del disco duro y en qué directorio se encuentre anwendung.exe.

- C:\Archivos de programa1\aplicación.exe

  El proceso del fichero aplicación.exe, que se encuentra en la ruta C:\Archivos de programa1, queda excluido del análisis del Guard.

- C:\Archivos de programa1*.exe

  Todos los procesos de ficheros ejecutables que se encuentran en la ruta C:\Archivs de programa1, quedan excluidos del análisis del Guard.

Ejemplos de ficheros que deben excluirse:

- *.mdb

  Todos los ficheros con la extensión de fichero "mdb" quedan excluidos del análisis del Guard.

- *.xls*

  Todos los ficheros cuya extensión de fichero comience por "xls" quedan excluidos del análisis del Guard, p. ej. ficheros con las extensiones de fichero .xls y xlsx.

- C:\Directorio*.log

  Todos los ficheros log con la extensión de fichero "log" que se encuentran en la ruta C:\Directorio, quedan excluidos del análisis del Guard.

11.2.1.3. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta configuración está activa por defecto si ha seleccionado el uso de esta heurística.

Nivel de detección alto

Si está activada la opción, detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

11.2.2 Informe

El Guard incluye una completa función de registro que puede ayudar al administrador en la identificación de una detección.

Protocolización

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

Desactivado

Con esta opción el Guard no crea ningún protocolo.
Desactive la protocolización sólo en casos excepcionales, p. ej. sólo cuando realice una prueba con muchos virus o programas no deseados.

Predeterminado

Si la opción está activada, el Guard 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.

Ampliado

Con esta opción activada, el Guard registra también información secundaria.

Completo

Si la opción está activada, el Guard registra toda la información en el fichero de informe, incluso la correspondiente al tamaño de fichero, tipo de fichero, fecha, etc.

Limitar fichero de informe

Limitar tamaño a n MB

Si la opción está activada, el fichero de registro se puede limitar a un determinado tamaño; posibles valores: 1 a 100 MB. En la limitación del fichero de informe se concede un margen de unos 50 kilobytes para mantener reducida la carga del equipo. Si el tamaño del fichero de informe supera la magnitud indicada en 50 kilobytes, se eliminan automáticamente tantas entradas antiguas como sea necesario para alcanzar la magnitud indicada menos 50 kilobytes.

Guardar fichero de informe antes de reducir

Si está activada esta opción, se hace una copia del fichero de informe antes de reducirlo.

Escribir configuración en fichero de informe

Al activar esta opción, la configuración del análisis directo se guarda en el fichero de informe.

Nota

Si no ha indicado ninguna limitación del fichero de informe, se creará de forma automática un nuevo fichero de informe cuando el fichero de informe haya alcanzado un tamaño de 100 MB. Se creará una copia de seguridad del antiguo fichero de informe. Se preservarán hasta tres copias de seguridad de los antiguos ficheros de informe. Las copias de seguridad más antiguas son las que primero se borran.

11.3 WebGuard

La sección WebGuard se utiliza para la configuración del WebGuard.

11.3.1 Análisis

Con el WebGuard puede protegerse frente a virus y malware que acceden a su sistema a través de las páginas Web que se cargan desde Internet en el explorador Web. En la sección *Análisis* puede configurar el comportamiento de WebGuard.

Análisis

Activar WebGuard

Si está activada la opción, las páginas Web que se solicitan a través del explorador de Internet se analizan en cuanto a virus y malware. El WebGuard supervisa los datos de Internet transmitidos con el protocolo HTTP en los puertos 80, 8080 y 3128. En caso de detectar páginas Web afectadas, se bloquea su carga. Si la opción está desactivada, el servicio WebGuard sigue ejecutándose pero el análisis de virus y malware se desactiva.

Protección sobre la marcha

Con la protección sobre la marcha dispone de la posibilidad de realizar configuraciones para bloquear I-Frames, también denominados marcos incorporados. I-Frames son elementos HTML, es decir elementos de páginas de Internet que limitan un área de una página Web. Los I-Frames permiten cargar y mostrar otros contenidos Web (normalmente, otras direcciones URL) como documentos independientes en una subventana del explorador. La mayoría de las veces los I-Frames se usan para banners, un formato publicitario en Internet. En algunos casos los I-Frames sirven para ocultar malware, es decir, software malintencionado. El área del I-Frame es, en esos casos, apenas visible en el explorador. La opción *Bloquear I-Frames sospechosos* permite controlar y bloquear la carga de I-Frames sospechosos.

Bloquear I-Frames sospechosos

Si la opción está activada, los I-Frames de las páginas Web solicitadas se analizan según determinados criterios. En caso de que existan I-Frames sospechosos en una página Web solicitada, éstos se bloquean. En la ventana del I-Frame aparece un mensaje de error.

Predeterminado

Si está activada esta opción, se bloquean los I-Frames de contenido sospechoso.

Ampliado

Con esta opción activada, los I-Frames de contenido sospechoso y los que se usan de forma sospechosa se bloquean. Se habla de uso sospechoso de I-Frames si el I-Frame es muy pequeño por lo que apenas o ni tan siquiera se ve, o si el I-Frame está colocado en una posición poco habitual en la página Web.

11.3.1.1. Acción en caso de detección

Acción en caso de detección

Puede definir las acciones que tomar el WebGuard cuando se detecta un virus o programa no deseado.

Interactiva

Con esta opción activada, durante un análisis directo aparece una ventana con opciones sobre qué hacer con el fichero concerniente. Este ajuste está activado de forma estándar.

Encontrará más información aquí.

Mostrar barra de progreso

Si la opción está activada, aparece una notificación en el escritorio con una barra de progreso de la descarga cuando una descarga o la descarga de contenidos de páginas Web supera un tiempo de espera de 20 segundos. Esta notificación en el escritorio sirve especialmente de control al descargar páginas Web con gran volumen de datos: al navegar con el WebGuard los contenidos de las páginas Web en el explorador de Internet no se cargan sucesivamente, ya que antes de presentarlos en el explorador de Internet se analizan acerca de la existencia de virus y malware. Esta opción está desactivada de forma estándar.

Automático

Si esta opción está activada, entonces no mostrará la ventana de acciones después de una detección de un virus o programa no deseado. El WebGuard reacciona de acuerdo a lo que configure en esta sección.

Acción Primaria

La acción principal es la que se ejecuta cuando el WebGuard detecta un virus o 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 sobre acceso denegado ha sido mostrado en su navegador Web. El WebGuard registra la detección en el fichero de informe si está activada la función de informe.

aislar

En el caso de una detección, la página Web solicitada por el servidor Web y/o los datos transferidos se mueven a la cuarentena. Desde el gestor de cuarentena puede volver a restaurar el fichero afectado si éste tiene valor informativo o, si fuera necesario, puede enviarlo al Avira Malware Research Center.

omitir

La página Web solicitada por el servidor Web o los datos y archivos transmitidos son pasados por el WebGuard a su navegador. Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

11.3.1.2. Accesos bloqueados

Con el filtro Web puede bloquear direcciones URL conocidas no deseadas, p. ej., URL de suplantación de identidad (phishing) y de software malintencionado (malware). El WebGuard impide la transmisión de datos de Internet a su sistema informático.

Filtro Web

El filtro Web dispone de una base de datos interna, que se actualiza a diario, en la que se clasifican las URL por criterios de contenido.

Activar filtro Web

Si está activada esta opción se bloquean todas las direcciones URL pertenecientes a las categorías seleccionadas en la lista de filtros Web.

Lista de filtros Web

En la lista de filtros Web puede seleccionar las categorías de contenido cuyas URL debe bloquear el WebGuard.

Nota

El filtro Web se omite en caso de existir entradas en la lista de direcciones URL omitidas en WebGuard::Análisis::Excepciones.

Nota

Se consideran direcciones URL de spam o correo no solicitado las URL que se propagan con emails de correo no solicitado. La categoría de fraudes y engaños incluye páginas Web con 'trampas de suscripción y otras ofertas de servicios, cuyos costes oculta el proveedor.

11.3.1.3. Excepciones

Estas opciones permiten excluir tipos MIME (tipos de contenidos de los datos transmitidos) y tipos de ficheros para URL (direcciones de Internet) del análisis del WebGuard. El WebGuard omite los tipos MIME y las URL indicadas, es decir, estos datos no se analizan en cuanto a virus y malware al transmitirse a su equipo.

Tipos MIME omitidos por WebGuard

En este campo puede seleccionar los tipos MIME que serán ignorados por el WebGuard durante el análisis.

Tipos de fichero y tipos MIME (definidos por el usuario) omitidos por WebGuard

Todos los tipos de fichero y MIME (tipos de contenido de los datos transmitidos) de la lista serán ignorados por el WebGuard durante el análisis.

Campo de entrada

En este campo puede escribir los tipos MIME y tipos de fichero que serán ignorados por el WebGuard durante el análisis. Para los tipos de fichero, debe indicar la extensión de fichero, p. ej. **.htm**. Para los tipos MIME, se indica el tipo de medio y, si es necesario, el subtipo. Ambas indicaciones se separan mediante una barra inclinada simple, p. ej., **video/mpeg** o **audio/x-wav**.

Nota
Cuando indique los tipos de fichero y tipos MIME, no puede utilizar comodines (comodín * para tantos caracteres como desee o comodín ? para un único carácter).

Advertencia
Todos los tipos de fichero y tipos de contenido de la lista de exclusión se cargan en el explorador de Internet sin más análisis de del WebGuard: No se ejecuta análisis alguno de virus y malware.

Tipos MIME: ejemplos de tipos de medio:

- `text` = para ficheros de texto
- `image` = para ficheros de imagen
- `video` = para ficheros de vídeo
- `audio` = para ficheros de sonido
- `application` = para ficheros vinculados a un determinado programa

Ejemplos: Tipos de fichero y tipos MIME que se omitirán

- `audio/` = todos los ficheros del tipo audio se excluyen del análisis del WebGuard
- `video/quicktime` = todos los ficheros de vídeo del subtipo Quicktime (*.qt, *.mov) se excluyen del análisis del WebGuard
- `.pdf` = todos los ficheros PDF de Adobe quedan excluidos del análisis del WebGuard.

Añadir

Este botón permite incluir en la ventana de visualización el tipo MIME o tipo de fichero introducido 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.

Direcciones URL omitidas por WebGuard

Todas las URL que constan en esta lista se excluyen del análisis del WebGuard.

Campo de entrada

En este campo se indican las URL (direcciones de Internet) que deben excluirse del análisis del WebGuard, p. ej., **www.nombrededominio.com**. Puede introducir partes de la URL, identificando con puntos al principio o al final el nivel de dominio: .nombrededominio.es para todas las páginas y todos los subdominios del dominio. Para escribir una página Web con cualquier dominio de nivel superior (.com o .net) debe indicarlo con un punto final: **nombrededominio.**. Si escribe una secuencia de caracteres sin punto inicial o final, dicha secuencia se interpreta como 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. Combine los comodines con puntos finales o iniciales para identificar los niveles de dominio:
.nombrededominio.*
*.nombrededominio.com
.*nombre*.com (es válido pero no se recomienda)
Las indicaciones sin puntos, como *nombre* se interpretan como parte de un dominio de nivel superior y no son útiles.

Advertencia

Todas las páginas Web de la lista de URL omitidas se cargan en el explorador de Internet sin más análisis por parte del filtro Web o del WebGuard: para todas las entradas de la lista de URL omitidas se pasan por alto las entradas del filtro Web (consulte WebGuard::Análisis::Accesos bloqueados). No se ejecuta análisis alguno de virus y malware. Por lo tanto, únicamente excluya direcciones URL de confianza del análisis del WebGuard.

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 BIEN- `www.avira.com/*`

  = todas las URL con el dominio 'www.avira.com' se excluyen del análisis del WebGuard: www.avira.com/es/pages/index.php, www.avira.com/es/support/index.html, www.avira.com/es/download/index.html,.. Las URL con el dominio www.avira.es no se excluyen del análisis del WebGuard.

- `avira.com` -O BIEN- `*.avira.com`

  = todas las URL con el dominio de segundo nivel y el dominio de nivel superior 'avira.com' se excluyen del análisis del WebGuard. La indicación incluye todos los subdominios existentes para '.avira.com': www.avira.com, forum.avira.com,...

- `avira.` -O BIEN- `*.avira.*`

= todas las URL con el dominio de segundo nivel 'avira' se excluyen del análisis del WebGuard. La indicación incluye todos los dominios de nivel superior o subdominios existentes para '.avira.': www.avira.com, www.avira.es, forum.avira.com,...

– `.*dominio*.*`

Todas las URL que contienen un dominio de segundo nivel con la cadena de caracteres 'dominio' se excluyen del análisis del WebGuard: www.dominio.com, www.nuevo-dominio.es, www.ejemplo-dominio1.es, ...

– `net` -O BIEN- `*.net`

= todas las URL con el dominio de nivel superior 'net' se excluyen del análisis del WebGuard: www.nombre1.net, www.nombre2.net,...

Advertencia
Indique con tanta precisión como sea posible las URL que desea excluir del análisis del WebGuard. Evite indicar dominios de nivel superior completos o partes de un nombre de dominio de segundo nivel, ya que existe el riesgo de que las páginas de Internet que propagan malware y programas no deseados queden excluidas del análisis del WebGuard debido a especificaciones demasiado globales. Se recomienda indicar por lo menos el dominio de segundo nivel completo y el dominio de nivel superior: nombrededominio.com

11.3.1.4. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta configuración está activa por defecto si ha seleccionado el uso de esta heurística.

Nivel de detección alto

Si está activada la opción, se detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

11.3.2 Informe

El WebGuard incluye una completa función de registro que puede ayudar al administrador en la identificación de una detección.

Protocolización

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

Desactivado

Con esta opción activada, el WebGuard no crea ningún protocolo.
Desactive la protocolización sólo en casos excepcionales, p. ej. sólo cuando realice una prueba con muchos virus o programas no deseados.

Predeterminado

Con esta opción activada, el WebGuard registra información importante (detecciones, alertas y errores) en el fichero de informe, obviando información secundaria para ganar en claridad. Este ajuste está activado de forma estándar.

Ampliado

Con esta opción activada, el WebGuard registra también información secundaria.

Completo

Si la opción está activada, el WebGuard registra toda la información en el fichero de informe, incluso la correspondiente al tamaño de fichero, tipo de fichero, fecha, etc.

Limitar fichero de informe

Limitar tamaño a n MB

Si la opción está activada, el fichero de registro se puede limitar a un determinado tamaño; posibles valores: 1 a 100 MB. En la limitación del fichero de informe se concede un margen de unos 50 kilobytes para mantener reducida la carga del equipo. Si el tamaño del fichero de informe supera la magnitud indicada en 50 kilobytes, se eliminan automáticamente tantas entradas antiguas como sea necesario para alcanzar la magnitud indicada menos un 20% .

Guardar fichero de informe antes de reducir

Si está activada esta opción, se hace una copia del fichero de informe antes de reducirlo.

Escribir configuración en fichero de informe

Al activar esta opción, la configuración del análisis directo se guarda en el fichero de informe.

Nota
Si no ha indicado ninguna limitación del fichero de informe, se borrarán de forma automática las entradas más antiguas cuando el fichero de informe haya alcanzado un tamaño de 100 MB. Se borrarán las entradas suficientes hasta que el fichero de informe alcance un tamaño de 80 MB.

11.4 Actualización

En la sección *Actualización* se configura la ejecución automática de actualizaciones. Se pueden configurar distintos intervalos de actualización y activar y desactivar la actualización automática.

Actualización automática

Activar

Si esta opción está activada, se ejecutan actualizaciones automáticas en el intervalo de tiempo indicado y para los eventos activados.

Actualización automática cada n días / horas / minutos

En este campo se puede indicar el intervalo con el que deberán ejecutarse las actualizaciones automáticas. Para modificar el intervalo de actualización, seleccionar una de las entradas de datos en el campo y cambiarla mediante los botones de flecha a la derecha del campo de introducción.

Repetir la tarea si el tiempo ya transcurrió

Con esta opción activada, se relanzan las tareas de actualización pasadas que no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.

11.4.1 Actualización de producto

En **Actualización del producto** se configura la ejecución de actualizaciones del producto o la notificación sobre actualizaciones de producto disponibles.

Actualizaciones de producto

Descargar actualizaciones de producto e instalar automáticamente

Si está activada esta opción, se descargan las actualizaciones de producto y el componente de actualización las instala automáticamente en cuanto estén disponibles. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración. Los requisitos para esta opción son: la configuración completa de la actualización y una conexión establecida con un servidor de descargas.

Descargar actualizaciones de producto. Si fuera necesario un reinicio, instalar la actualización después del siguiente reinicio del sistema; si no, instalarla inmediatamente.

Con esta opción activada, las actualizaciones de producto se descargan en cuanto estén disponibles. La actualización se instala automáticamente después de la descarga de los ficheros de actualización si no se precisa el reinicio del equipo. Si se trata de una actualización del producto que precisa el reinicio del equipo, la actualización del producto no se ejecuta inmediatamente después de la descarga de los ficheros de actualización, sino sólo después del siguiente reinicio del sistema ejecutado por el usuario. La ventaja es que el reinicio no se produce en un momento en el que el usuario trabaja en el equipo. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración. Los requisitos para esta opción son: la configuración completa de la actualización y una conexión establecida con un servidor de descargas.

Notificar cuando haya nuevas actualizaciones de producto disponibles

Si está activada esta opción, sólo recibirá notificación si hay nuevas actualizaciones de producto disponibles. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración. Los requisitos para esta opción son: la configuración completa de la actualización y una conexión establecida con un servidor de descargas. La notificación se produce mediante un mensaje en el escritorio en forma de ventana emergente y mediante un mensaje de advertencia del Updater en el Centro de control en Información general::Eventos.

Notificar nuevamente después de n día(s)

Indique en este campo después de cuántos días se debe efectuar una nueva notificación sobre actualizaciones de producto disponibles si la actualización del producto no se efectuó después de la primera notificación.

No descargar actualizaciones de producto

Si está activada la opción, no se llevan a cabo actualizaciones automáticas del producto ni notificaciones sobre la disponibilidad de dichas actualizaciones a través de Updater. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración.

Importante
Las actualizaciones del fichero de firmas de virus y del motor de análisis se llevan a cabo con cada actualización que se ejecute, independientemente de la configuración de la actualización de producto (consulte al respecto el cap. Actualizaciones).

Nota
Si ha activado una opción para una actualización automática del producto, bajo Configuración del reinicio puede configurar otras opciones para la notificación y posibilidades de cancelación del reinicio.

11.4.2 Configuración del reinicio

Si se ejecuta una actualización de producto de su programa AntiVir, puede ser necesario reiniciar el equipo. Si ha configurado la ejecución automática de actualizaciones del producto en Actualización::Actualización del producto, puede seleccionar en **Configuración del reinicio** entre diferentes opciones para la comunicación y la cancelación del reinicio.

Nota
Cuando configure el reinicio tenga en cuenta que puede seleccionar durante la configuración en Actualización::Actualización del producto entre dos opciones para la ejecución de una actualización del producto con necesidad de reinicio del equipo:

Ejecución automática de la actualización del producto con necesidad de reinicio del equipo cuando esté disponible la actualización: La actualización y el reinicio se ejecutarán mientras esté trabajando un usuario en el equipo. Si tiene activada esta opción, pueden ser útiles las rutinas de reinicio con posibilidad de cancelación o con función de recordatorio.

Ejecución de la actualización del producto con necesidad de reinicio del equipo tras el siguiente inicio del sistema: la actualización y el reinicio se ejecutan cuando un usuario haya arrancado el equipo e iniciado la sesión. Para esta opción son recomendables las rutinas automáticas de reinicio.

Configuración del reinicio

Reiniciar el equipo después de n segundos

Con esta opción activada, se ejecuta en caso necesario **automáticamente** un reinicio una vez realizada la actualización del producto y transcurrido el intervalo de tiempo indicado. Aparece un mensaje de cuenta atrás sin la posibilidad de cancelar el reinicio del equipo.

Mensaje de recordatorio para el reinicio cada n segundos

Con esta opción activada, **no se ejecuta automáticamente** un reinicio necesario tras la actualización del producto. En el intervalo de tiempo indicado recibirá mensajes sin posibilidad de cancelación del reinicio. Los mensajes permiten confirmar el reinicio del equipo o seleccionar la opción "**Recordar en otro momento"**.

Consulta si desea realizar el reinicio del equipo

Con esta opción activada, **no se ejecuta automáticamente** un reinicio necesario tras la actualización del producto. Aparecerá un único mensaje donde puede confirmar el reinicio o cancelar la rutina de reinicio.

Reiniciar el equipo sin consulta

Con esta opción activada, se ejecuta **automáticamente** un reinicio necesario tras la actualización del producto. No aparece ningún mensaje.

La actualización puede realizarse desde un servidor Web en Internet.

Conexión al servidor Web

Utilizar la conexión existente (red)

Este parámetro se muestra cuando su conexión se utiliza a través de una red.

Utilizar la siguiente conexión:

Este parámetro se muestra si define su conexión de forma individual.

El Updater detecta automáticamente las conexiones disponibles. Las conexiones que no están disponibles están en 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 aquí el nombre de usuario de la cuenta seleccionada.
- **Contraseña:** Indique la contraseña de esa cuenta. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Nota
Si ha olvidado los datos para conectar a Internet, contacte con su proveedor de servicios de Internet.

Nota
La marcación telefónica automática del Updater por medio de herramientas de marcación telefónica (p. ej., SmartSurfer, Oleco...) todavía no está disponible en.

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 no está disponible en Vista. En Vista, la conexión de acceso telefónico a redes abierta para la actualización siempre finaliza en cuanto la descarga se haya ejecutado.

11.5 General

11.5.1 Categorías de riesgos

Selección de categorías de riesgos

Su producto AntiVir le protege contra virus informáticos.

Además, puede ejecutar un análisis de acuerdo con las siguientes categorías de amenazas.

- Software de control de puerta trasera (BDC)
- Marcador (DIALER)
- Juegos (GAMES)
- Chistes (JOKES)
- Riesgo de seguridad-confidencialidad (Security privacy risk, SPR)
- Adware/Spyware (ADSPY)
- Utilidades de compresión no estándar (PCK)
- Ficheros con doble extensión (HEUR-DBLEXT)
- Suplantación de identidad (phishing)
- Aplicación (APPL)

Hacer clic sobre las marcas correspondientes para activar o desactivar

Activar todas

Con esta opción, se activan todos los tipos

Valores predeterminados

Este botón restablece los valores estándar predefinidos.

Nota
Si no se activa un tipo, los ficheros que se reconocen como pertenecientes al mismo, no se siguen indicando. No se anota en el fichero de informe.

11.5.2 Seguridad

Update/Actualización

Alertar si la última actualización se produjo hace más de n días

Aquí puede introducir el máximo número de días permitidos sin actualizar. Si se sobrepasa este periodo de tiempo, se muestra un icono rojo en el Centro de control en el estado para el estado de actualización.

Mostrar nota si el fichero de firmas de virus está obsoleto

Si esta opción está activada, se mostrará un mensaje si los ficheros de firmas no están al día. Con la ayuda de la opción de alerta, puede configurar el intervalo para recibir el aviso si la última actualización no se ha producido desde hace más de cierto número de días.

Protección del producto

Nota
Las opciones de protección del producto no están disponibles si no se ha instalado el Guard durante una instalación personalizada.

Previene la finalización no deseada de procesos

Con esta opción 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

Con esta opción 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. La opción está activada de forma estándar. Para desactivar la opción se debe reiniciar el equipo.

Importante
¡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 esos casos, desactive la protección de procesos.

Proteger los ficheros y las entradas del registro contra manipulaciones

Con esta opción 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 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 fracasar la reparación de ordenadores infectados con determinados tipos de malware.

Nota
Con esta opción activada, la modificación de la configuración y también la modificación de tareas de análisis o actualización sólo es posible por medio de la interfaz de usuario.

Importante
¡La protección de ficheros y entradas de registro no está disponible en Windows XP 64 Bit !

11.5.3 WMI

Compatibilidad con Windows Management Instrumentation (Instrumental de Administración de Windows - WMI)

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 programa AntiVir es compatible con WMI y proporciona los 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 está opción está activada, puede consultar los datos operativos del programa por medio de WMI.

11.5.4 Directorios

Ruta temporal

En este campo puede introducir la ruta en la que deben guardarse los ficheros temporales del programa.

Usar configuración del sistema

Al activar esta opción, se usa la configuración del sistema para la gestión de los ficheros temporales.

Nota
Puede ver dónde se guardan los ficheros temporales de Windows XP - en: Inicio | Panel de Control | Sistema | Pestaña Opciones Avanzadas | Botón Variables de entorno. Aquí se muestran las variables temporales (TEMP, TMP) (TEMP, TMP) del usuario registrado, con su valor.

Usar el directorio siguiente

Al usar esta opción, se utiliza la ruta contenida en el campo.

...

El botón abre una ventana en la que puede seleccionar la ruta temporal.

Predeterminado

El botón restablece el directorio por defecto como directorio temporal.

11.5.5 Proxy

Servidor proxy

No usar servidor proxy

Al activar esta opción, su conexión al servidor Web no se realiza a través de un servidor proxy.

Utilizar la configuración del sistema de Windows

Al activar esta opción se utiliza la configuración del sistema de Windows actual para la conexión al servidor Web a través de un servidor proxy. Se configura el sistema de Windows para utilizar un servidor proxy en el **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* sólo 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 clave para el registro en el servidor proxy. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Ejemplos:

Dirección:	proxy.dominio.com	Puerto:	8080
Dirección:	192.168.1.100	Puerto:	3128

11.5.6 Eventos

Limitar tamaño de base de datos de eventos

Limita el máximo número de eventos a n entradas

Si se selecciona esta opción el máximo número de entradas listadas en la base de datos puede limitarse a cierto tamaño; valores posibles: de 100 a 10 000 entradas. Si se sobrepasa el número de entradas, las más antiguas se eliminan.

Elimina eventos con antigüedad superior a n días

Si se selecciona esta opción, los eventos listados en la base de datos se borran después de un cierto período de tiempo: Los valores permisibles están en 1 y 90 días. Esta opción se habilita de forma estándar con un valor de 30 días

No limitar el tamaño de la base de datos (eliminar eventos manualmente)

Si la opción está activada, el tamaño de la base de datos de eventos no está limitado. No obstante, en la interfaz del programa en eventos se muestran como máximo 20 000 entradas.

11.5.7 Limitar informes

Limitar el número de informes

Limitar el número a n unidades

Con esta opción activada, se puede limitar la cantidad máxima de informes; los valores permitidos son: 1 a 300. Al superar la cantidad indicada se eliminan los informes más antiguos.

Borrar todos los informes de más de n días

Si esta opción está activada, los informes se eliminan automáticamente tras un número específico de días. Los valores permisibles están en 1 y 90 días. Esta opción se habilita de forma estándar con un valor de 30 días

No limitar el número de informes (eliminar informes manualmente)

Si esta opción está activada, la cantidad de informes no está limitada.

11.5.8 Advertencias acústicas

Advertencia acústica

Cuando el escáner o el Guard detectan virus o malware, en el modo de acción interactivo suena 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 del escáner se establece en la configuración, en Escáner::Análisis::Acción en caso de detección.

Sin advertencia

Si la opción está activada, en caso de que el escáner o el Guard detecten virus, no tiene lugar ninguna advertencia acústica.

Reproducir a través de altavoces del PC (sólo en modo interactivo)

Si la opción está activada, en caso de que el escáner o el Guard detecten virus, tiene lugar una advertencia acústica con el sonido de advertencia predeterminado. El sonido de advertencia se reproduce a través del altavoz interno del equipo.

Usar el siguiente fichero Wave (sólo en modo interactivo)

Si la opción está activada, en caso de que el escáner o el Guard detecten virus, tiene lugar 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. Por defecto se introduce el sonido de advertencia estándar del programa.

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.

11.5.9 Advertencias

En caso de eventos determinados, su programa AntiVir genera notificaciones en el escritorio, las denominadas Slide-Ups, para informarle sobre peligros y ejecuciones correctas o erróneas del programa, como por ejemplo la ejecución de una actualización. En *Advertencias* se puede activar o desactivar la notificación en caso de eventos determinados.

Las notificaciones de escritorio ofrecen la posibilidad de desactivar la notificación directamente en el Slide-Up. Puede deshacer la desactivación de la notificación en *Advertencias*.

Advertencias

sobre las conexiones de marcación telefónica utilizadas

Con la opción activada se le alerta con una notificación en el escritorio cuando un programa de marcación telefónica establece una conexión a través de la red de teléfono o RDSI en su equipo. Existe el peligro de que el programa de marcación sea un Dialer desconocido y no deseado que establece una conexión no gratuita. (ver Virus y más::Categorías de riesgos avanzadas: Dialers).

sobre ficheros actualizados correctamente

Con la opción activada recibe una notificación de escritorio cuando una actualización ha sido completada correctamente y se actualizaron ficheros.

sobre error de actualización

Con la opción activada recibe una notificación de escritorio en caso de una actualización errónea: no se pudo establecer una conexión con el servidor de descargas o los ficheros de actualización no se pudieron instalar.

informando de que no hace falta actualizar

Con la opción activada recibe una notificación de escritorio cuando se inició una actualización, pero la instalación de ficheros no ha sido necesaria al encontrarse su programa actualizado.

Versión 3er trimestre de 2011.

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