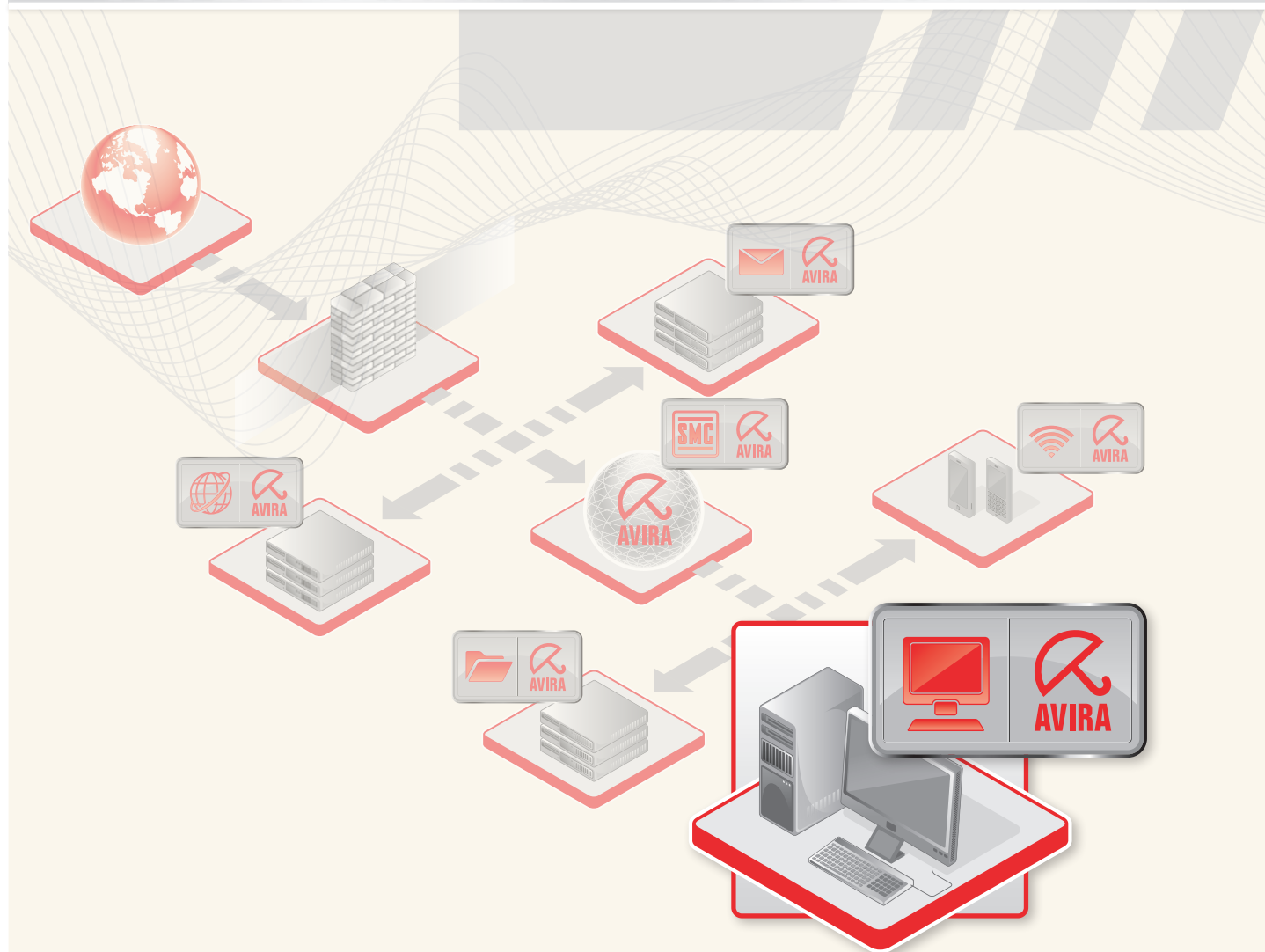


Manual para usuarios

Avira AntiVir Personal



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 propiedad 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 terceros de 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.....	5
4	Instalación y desinstalación.....	6
4.1	Instalación.....	6
4.2	Instalación diferencial	10
4.3	Módulos de instalación.....	10
4.4	Desinstalación.....	11
5	Información general de AntiVir Personal	12
5.1	Interfaz de usuario y uso	12
5.1.1	Centro de control	12
5.1.2	Configuración	14
5.1.3	Icono de bandeja	17
5.2	Procedimientos	18
5.2.1	Actualizar Avira AntiVir Personal de forma automática.....	18
5.2.2	Iniciar una actualización manualmente.....	19
5.2.3	Análisis directo: analizar la existencia de virus y malware con un perfil de análisis	20
5.2.4	Análisis directo: analizar la existencia de virus y malware mediante Arrastrar y soltar	21
5.2.5	Análisis directo: analizar la existencia de virus y malware mediante el menú contextual.....	21
5.2.6	Análisis directo: analizar la existencia de virus y malware de forma automática.....	21
5.2.7	Análisis directo: analizar directamente la existencia de rootkits activos.....	22
5.2.8	Reaccionar a virus y malware detectados.....	23
5.2.9	Cuarentena: tratar con ficheros (*.qua) en cuarentena.....	25
5.2.10	Cuarentena: restaurar los ficheros de cuarentena.....	26
5.2.11	Cuarentena: mover fichero sospechoso a cuarentena.....	27
5.2.12	Perfil de análisis: añadir o eliminar un tipo de fichero de un perfil de análisis ..	27
5.2.13	Perfil de análisis: crear acceso directo en el escritorio para el perfil de análisis .	28
5.2.14	Eventos: Filtrar eventos.....	28
6	Scanner.....	31
7	Actualizaciones	32
8	P+F, sugerencias	33
8.1	Ayuda en caso de problemas	33
8.2	Atajos.....	34
8.2.1	En los cuadros de diálogo.....	35
8.2.2	En la Ayuda.....	35
8.2.3	en Centro de control	36
8.3	Centro de Seguridad de Windows.....	37
8.3.1	General	37
8.3.2	El Centro de Seguridad y Avira AntiVir Personal	37

9	Virus y más	40
9.1	Extensión de las categorías de amenazas	40
9.2	Virus y otro tipo de Malware.....	42
10	Información y servicio	46
10.1	Dirección de contacto	46
10.2	Soporte Técnico	46
10.3	Archivos sospechosos	46
10.4	Informe falso positivo	47
11	Referencia: opciones de configuración.....	48
11.1	Scanner.....	48
11.1.1	Análisis	48
11.1.1.1.	Acción en caso de detección	51
11.1.1.2.	Heurística	54
11.1.1.3.	Heurística	54
11.1.2	Informe.....	55
11.2	Guard.....	56
11.2.1	Análisis	56
11.2.1.1.	Acción en caso de detección	58
11.2.1.2.	Excepciones	58
11.2.1.3.	Heurística	61
11.2.2	Informe.....	61
11.3	General.....	62
11.3.1	Configuración :: General.....	62
11.3.1.1.	Categorías de riesgos avanzadas	62
11.3.2	Seguridad.....	63
11.3.3	WMI.....	64
11.3.4	Directorios.....	65
11.3.5	Actualización	65
11.3.5.1.	Servidor web.....	66
11.3.6	Alertas.....	67
11.3.6.1.	Advertencias acústicas	67
11.3.7	Eventos	68
11.3.8	Límite de informes.....	68
11.3.9	Advertencias acústicas	69

1 Introducción

Avira AntiVir Personal de Avira GmbH protege su equipo frente a virus, malware, adware y spyware, así como frente a programas no deseados y otros riesgos. Para abreviar, en este manual se habla de virus y software malintencionado o malware.

El manual describe la instalación y el uso del programa.

En nuestra página web <http://www.free-av.es> puede descargarse el manual de Avira AntiVir Personal como PDF, actualizar Avira AntiVir Personal o informarse sobre la versión de Avira AntiVir Premium de pago, .

Además, en la página web encontrará otra información, como el número de teléfono del soporte técnico y nuestro boletín de noticias, al que puede suscribirse desde esa página.

El equipo de Avira GmbH

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 Avira AntiVir Personal.

Se usan los siguientes resaltados:

Resaltado	Explicación
<i>Cursiva</i>	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 Avira AntiVir Personal:

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

Avira AntiVir Personal es una herramienta completa y flexible para proteger el equipo con fiabilidad frente a virus, software malintencionado (malware) programas no solicitados 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 Avira AntiVir Personal mediante las actualizaciones automáticas. Configure el programa correspondientemente.

3.1 Gama de prestaciones

Avira AntiVir Personal ofrece 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
- Scanner (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
- Administración integrada de cuarentena para aislar y tratar los ficheros sospechosos
- Protección contra rootkits para detectar malware instalado de forma oculta en la máquina (denominado rootkit)
(Sólo para sistemas de 32 bits)
- 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


Para que Avira AntiVir Personal funcione correctamente, el sistema informático debe cumplir los siguientes requisitos:

- Ordenador Pentium o superior, de un mínimo de 266 MHz
- Sistema operativo
- Windows 2000, SP4 y el paquete acumulativo de actualizaciones 1 o
- Windows XP, SP2 (32 ó 64 bits) o
- Windows Vista (32 ó 64 bits, SP 1 recomendado)
- Al menos 100 MB de espacio libre en el disco duro (en caso de usar la cuarentena y para la memoria temporal, más)
- Al menos 192 MB de memoria RAM con Windows 2000/XP
- Al menos 512 MB de memoria RAM con Windows Vista
- Para la instalación de Avira AntiVir Personal: derechos de administrador
- Para todas las instalaciones: Windows Internet Explorer 6.0 o superior
- Si fuera necesario, conexión a Internet (consulte Instalación)

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.

Avira AntiVir Personal requiere en Windows Vista privilegios de administrador para varias 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

Para utilizar Avira AntiVir Personal, es necesaria una licencia. Se deben aceptar las condiciones de licencia de Avira AntiVir Personal.

La licencia se asigna como clave de activación. La clave de activación es un código de letras y números que se recibe al adquirir Avira AntiVir Personal. 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 AntiVir Personal 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 Avira AntiVir Personal. La activación del producto puede llevarse a cabo durante la instalación. Pero también puede activar Avira AntiVir Personal después de la instalación, en el Centro de control en Ayuda::Activar licencia.

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

4 Instalación y desinstalación

Este capítulo proporciona información en torno a la instalación y desinstalación de Avira AntiVir Personal:

- 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 instalar Avira AntiVir Personal, comprueba que tu equipo cumple con todos los requerimientos mínimos. De ser así, puede instalar Avira AntiVir Personal.

Nota

Desde Windows XP, Avira AntiVir Personal crea un punto de restauración en el equipo previo a la instalación de Avira AntiVir Personal. Esto permite recuperar el sistema si se produce un error al instalar Avira AntiVir Personal. Para que esta función se active, la opción **Desactivar Restaurar sistema** en: "Inicio | Panel de Control | Sistema | Restaurar sistema " no debe de estar marcada.

Si desea recuperar su sistema anterior, puede hacerlo mediante "Inicio | Programas | Accesorios | Herramientas del Sistema | Restaurar Sistema". El punto de restauración generado por Avira AntiVir Personal se reconoce por la entrada AntiVir Personal.

Tipos de instalación

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

Completo

AntiVir Personal 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.

Personalizada

Tiene la posibilidad de elegir 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.

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 de Avira AntiVir Personal
- ▶ Si fuera necesario, ejecución de una actualización de AntiVir Personal tras finalizar la instalación
- ▶ Tenga la clave de licencia preparada para AntiVir Personal si desea activar AntiVir Personal.

Nota

Instalación basada en Internet:

Para la instalación basada en Internet de Avira AntiVir Personal, Avira GmbH 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 AntiVir Personal 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 AntiVir Personal. Se recomienda ejecutar una actualización al acabar la instalación para actualizar el fichero de firmas de virus.

Nota

Para registrar el producto, Avira AntiVir Personal 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.

Procedimiento para instalar AntiVir Personal:

- ▶ 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 AntiVir Personal 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

→ La instalación continúa con el cuadro de diálogo *Categorías de riesgos avanzadas*. El cuadro de diálogo informa sobre las funciones de protección de AntiVir Personal y ofrece indicaciones para ampliar las funciones de protección AntiVir Personal.

▶ Haga clic en **Continuar**.

→ 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 AntiVir Personal exclusivamente en el ámbito privado y no con fines industriales, y pulse **Continuar**.

→ Aparece el cuadro de diálogo *Crear 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*.

▶ Decida si va a ejecutar una instalación completa o una instalación personalizada.

▶ Active la opción **Completa** o **Personalizada** y confirme pulsando **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 de la instalación completa y la personalizada

→ Se abre el asistente de licencia.

El asistente de licencia ofrece la posibilidad de registrarse como cliente de AntiVir Personal y suscribirse al boletín de Avira GmbH. 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) una vez finalizada la instalación.
- ▶ Si fuera el caso, confírmelo y concluya la instalación con *Finalizar*.
- Se cierra el asistente de instalación.
- Si fuera el caso, se abre el fichero Léame (Readme).
- En el siguiente paso se abre el asistente de configuración. En el asistente de configuración puede establecer importantes valores predefinidos para AntiVir Personal. Si cancela la actualización, AntiVir Personal se inicia con la configuración predeterminada.

Valores predefinidos en el asistente de configuración

- El cuadro de diálogo *Configurar AHeAD* permite elegir un nivel de detección para la tecnología AHeAD. El nivel de detección seleccionado se aplica en la configuración de la tecnología AHead del Scanner (análisis directo) y del Guard (análisis en tiempo real) .
- ▶ Seleccione un nivel de detección y continúe con la configuración pulsando **Continuar**.
- En el siguiente cuadro de diálogo, *Seleccionar categorías de riesgos avanzadas*, puede adaptar las funciones de protección de AntiVir Personal seleccionando categorías de riesgos.
- ▶ Si fuera necesario, active más categorías de riesgos y prosiga con la configuración pulsando *Continuar*.
- ▶ 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 ordenador, 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 activó la opción *Análisis breve del sistema*, aparece la ventana Luke Filewalker. El Scanner lleva a cabo un breve análisis del sistema.
- Aparece el cuadro de diálogo *Finalizar la instalación*.
- Si instaló AntiVir Personal en Windows XP y desactivó el firewall de Windows, aparece una ventana informativa que le indica reiniciar el equipo.
- ▶ Concluya la instalación pulsando **Finalizar**.

Tras la instalación correcta se recomienda comprobar en el Centro de control, en *Información general :: Estado* la vigencia de AntiVir Personal.

- ▶ Si fuera necesario, lleve a cabo una actualización de AntiVir Personal 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 de Avira AntiVir Personal (consulte el capítulo Instalación y desinstalación::Módulos de instalación)

Si desea añadir o quitar módulos a la instalación actual de Avira AntiVir Personal, use la opción **Añadir o quitar programas** en el **panel de control de Windows** para **Cambiar/Eliminar** la instalación.

Seleccione Avira AntiVir Personal y haga clic sobre **Cambiar**. En la ventana de bienvenida de Avira AntiVir Personal seleccione la opción **Modificar**. Será guiado/a a través de la reinstalación.

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 Avira AntiVir Personal.
- **AntiVir Guard**
AntiVir Guard se ejecuta en segundo plano. Supervisa y repara, si fuera necesario, 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), Avira AntiVir Personal analiza automáticamente el fichero. En el caso de la operación de fichero Cambiar nombre, AntiVir Guard no realiza análisis alguno.
- **Protección contra rootkits de AntiVir**
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 software malintencionado.
- **Extensión del shell**
La extensión del shell de Avira AntiVir Personal crea en el menú contextual del Explorador de Windows (botón derecho del ratón) la entrada Analizar ficheros seleccionados con AntiVir. Esta entrada permite analizar directamente determinados ficheros o directorios.

4.4 Desinstalación

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

Procedimiento para desinstalar Avira AntiVir Personal (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 AntiVir Personal** y pulse **Quitar**.
- 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**.
- Avira AntiVir Personal se ha desinstalado. Si fuera necesario, el equipo se reiniciará. Al hacerlo, se eliminan todos los directorios, ficheros y entradas del registro de Avira AntiVir Personal.

5 Información general de AntiVir Personal

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

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

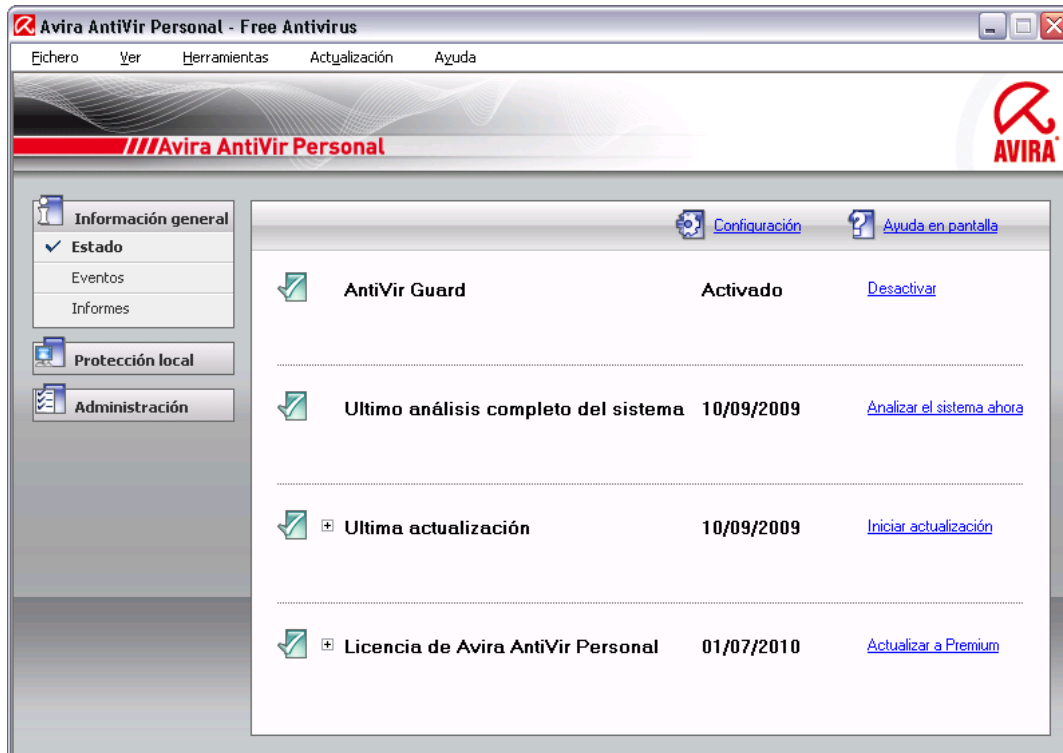
5.1 Interfaz de usuario y uso

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

- Centro de control: supervisión y control de AntiVir Personal
- Configuración de Avira AntiVir Personal: configuración de AntiVir Personal
- 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 AntiVir Personal.



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 AntiVir Personal.

- **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 de AntiVir Personal 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 del elemento de programa de AntiVir Personal en el menú Inicio | Programas.
- Por medio del icono de bandeja de Avira AntiVir Personal.

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.

Uso del Centro de control

Para explorar 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, pueda 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:

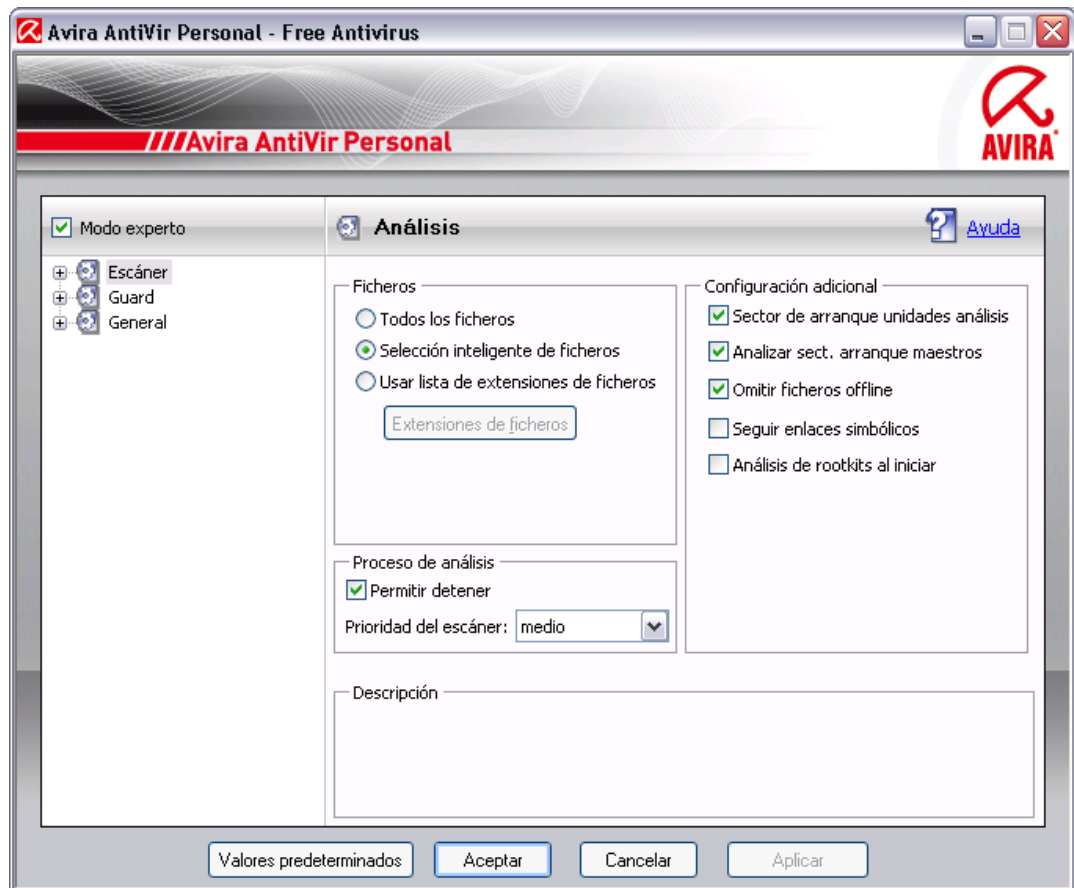
- ▶ Seleccione los datos u objetos que va a editar.
 - Para seleccionar varios elementos, mantenga pulsada la tecla Ctrl o la tecla Mayús (selección de elementos consecutivos) mientras elige los elementos.
- ▶ Pulse el botón que desee en la barra superior de la ventana de detalles para editar el objeto

Información general de Centro de control

- **Descripción general:** en **Descripción general** encontrará todas las secciones con las que puede supervisar la funcionalidad de Avira AntiVir Personal.
- La sección **Estado** ofrece la posibilidad de ver de una sola mirada qué módulos de Avira AntiVir Personal 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 Avira AntiVir Personal.
- La sección Informes ofrece la posibilidad de consultar los resultados de las acciones realizadas por Avira AntiVir Personal.
- **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. Prácticamente con sólo pulsar un botón, se obtiene información detallada sobre el último virus o programa no deseado que se detectó.
- **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 a Avira Malware Research Center.
- La sección Programador permite crear tareas de análisis y actualización, programadas, y adaptar o eliminar tareas existentes.

5.1.2 Configuración

En la Configuración de Avira AntiVir Personal puede establecer los parámetros de AntiVir Personal. Tras la instalación, AntiVir Personal 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 AntiVir Personal pueden presentar particularidades, de modo que querrá adaptar los componentes de protección de AntiVir Personal.



La Configuración de Avira AntiVir Personal 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.

Activación de la Configuración de Avira AntiVir Personal

Hay varias maneras de activar la configuración:

- Por medio del Panel de control de Windows .
- Por medio del Centro de seguridad de Windows: a partir de Windows XP Service Pack 2.
- Por medio del icono de bandeja de Avira AntiVir Personal.
- En el Centro de control de Avira AntiVir Personal, con la opción de menú Herramientas | Configuración.
- En el Centro de control de Avira AntiVir Personal, 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.

Uso de la Configuración de Avira AntiVir Personal

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 de Avira AntiVir Personal 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:

- **Scanner:** 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

- **General:**

Configuración del envío de email vía SMTP

Categorías de riesgo 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 AntiVir Personal 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 AntiVir Guard.

Por medio del menú contextual del icono de bandeja puede acceder rápidamente a las funciones principales de Avira AntiVir Personal. 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 Avira AntiVir Guard
- **Iniciar AntiVir:** abre el Centro de control de Avira AntiVir Personal .
- **Configurar AntiVir:** abre la Configuración de Avira AntiVir Personal.
- **Iniciar actualización:** inicia una actualización.
- **Ayuda:** Abre la ayuda online.
- **Avira en Internet:** abre el portal web del fabricante de AntiVir Personal en Internet. Debe de existir una conexión activa a Internet


5.2 Procedimientos

5.2.1 Actualizar Avira AntiVir Personal de forma automática

Nota

Existe una tarea de actualización preinstalada que actualiza Avira AntiVir Personal, si hay una conexión de Internet disponible, cada 24 horas, así como adicionalmente cada vez que se establece conexión con Internet.

Así se crea una tarea con el Programador de AntiVir con la que actualizar automáticamente Avira AntiVir Personal:

- ▶ En el Centro de control seleccione la sección **Administración :: Programador**.
- ▶ Haga clic en el icono  *Crear tarea nueva con el asistente*.
- Aparece el cuadro de diálogo *Nombre y descripción de la tarea*.
- ▶ Asigne nombre a la tarea y descríbalas 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 actualizar Avira AntiVir Personal de forma frecuente y regular, por ejemplo, cada 24 horas.

- ▶ Según lo que seleccione, indique la fecha si fuera necesario.
- ▶ Si fuera el caso, seleccione opciones adicionales (sólo disponible en algunos tipos de tarea):
 - **Repetir la tarea si el tiempo ya transcurrió**

Los trabajos en el pasado se relanzan por si no pudieron realizarse en su momento, por ejemplo, porque el ordenador 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

5.2.2 Iniciar una actualización manualmente

Dispone de varias posibilidades de iniciar manualmente una actualización de Avira AntiVir Personal: 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 Avira AntiVir Personal:

- ▶ Haga clic con el botón derecho del ratón en el icono de bandeja de Avira AntiVir Personal en la barra de tareas.
- Aparece un menú contextual.
- ▶ Seleccione **Se inició la actualización**.
- Aparece el cuadro de diálogo *Avira AntiVir Personal Updater*.
 - O BIEN -
- ▶ En el Centro de control, seleccione la sección **Descripción general :: Estado**.
- ▶ En el área *Ultima actualización* haga clic en el enlace **Iniciar actualización**.
- Aparece el cuadro de diálogo Avira AntiVir Personal Updater.
 - O BIEN -
- ▶ En el Centro de control, en el menú **Actualización**, seleccione el comando de menú *Iniciar actualización*.
- Aparece el cuadro de diálogo Avira AntiVir Personal Updater.

Nota

Recomendamos encarecidamente actualizar Avira AntiVir Personal de forma automática y regular, por ejemplo, cada 24 horas.

Nota

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

5.2.3 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 la sección **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 y las unidades que va a analizar:
- ▶ Seleccione los nodos y que desea analizar mediante un clic en la casilla de :

5.2.4 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 Avira AntiVir Personal.
- ▶ 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.


5.2.5 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.
- ▶ En el menú contextual seleccione **Analizar 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.

5.2.6 Análisis directo: analizar la existencia de virus y malware de forma automática

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 descríbalas 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.
- ▶ Si fuera el caso, seleccione la siguiente opción adicional (sólo disponible en algunos tipos de tarea):
 - **Repetir la tarea si el tiempo ya transcurrió**
Los trabajos en el pasado se relanzan por si no pudieron realizarse en su momento, por ejemplo, porque el ordenador 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 :: Programador* como activada (marca de verificación).
- ▶ Si es el caso, desactive las tareas que no deban ejecutarse.

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



Ver las propiedades de una tarea



Modificar tarea



Eliminar tarea



Iniciar tarea





Detener tarea

5.2.7 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*.

Así se analiza directamente la existencia de rootkits activos:

- ▶ En el Centro de control seleccione la sección **Protección local :: Analizar**.
- Aparecen perfiles de análisis predefinidos.
- ▶ Seleccione el perfil de análisis predefinido **Análisis de rootkits**.
- ▶ 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.

5.2.8 Reaccionar a virus y malware detectados

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

Opciones del Scanner:

– **Interactivo**

En el modo de acción interactivo, las detecciones del análisis del Scanner se notifican en un cuadro de diálogo. Esta opción está activada de forma predeterminada.

Cuando se analiza la existencia de **rootkits**, **virus del sector de arranque** y **procesos activos**, aparece un cuadro de diálogo en el que puede seleccionar lo que debe hacerse con el objeto afectado.

Durante el **análisis de ficheros**, la notificación y la posibilidad de selección del tratamiento de los ficheros afectados dependen del modo de notificación seleccionado:

Modo de notificación: Combinado

En el modo de notificación combinado se recibe al finalizar el análisis de ficheros un mensaje de advertencia con una lista de los ficheros afectados detectados. No hay posibilidades de seleccionar el tratamiento de los ficheros afectados. Puede ejecutar la acción predeterminada del Scanner para todos los ficheros afectados o cancelar el Scanner.

Modo de notificación: Combinado (experto)

En el modo de notificación experto se recibe al finalizar el análisis de ficheros 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 seleccionada para todos los ficheros afectados o finalizar el Scanner.

Modo de notificación: Personalizado

En el modo de notificación personalizado, cada detección de virus durante el análisis de ficheros se notifica en una ventana aparte. En el cuadro de diálogo puede seleccionar lo que debe hacerse con el fichero afectado.

– **Automático**

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

Opciones del Guard:

– **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. Esta opción está activada de forma predeterminada.

– Automático

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

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) que notifica la detección y del malware detectado.

Acciones del Scanner 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 pero puede restaurarse con las herramientas correspondientes (p. ej., *Avira UnErase*). Así se puede volver a encontrar la firma de virus. 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

Avira AntiVir Personal no ejecuta ninguna acción más. El fichero afectado permanece activo en el ordenador.

Advertencia

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

– Denegar acceso

Opción de acción en las detecciones de Guard: se bloquea el acceso al fichero afectado. La detección sólo se registra en el fichero de informe (si está activada la función de informe).

– Copiar a cuarentena

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

– Finalizar programa

Opción de acción al detectar un proceso sospechoso: el proceso finaliza. Aparece otro cuadro de diálogo en el que puede seleccionar lo que debe ocurrir con el fichero ejecutable.

Nota


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

5.2.9 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 ordenador 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 Avira AntiVir Personal ha actualizado el fichero de firmas de virus 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

Se recomienda el análisis por parte del Avira Malware Research Center en los siguientes casos

Detección mediante heurística (fichero sospechoso): Durante un análisis, AntiVir Personal 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.

Los ficheros que están en la cuarentena se pueden restaurar:

- consulte el capítulo: Cuarentena: restaurar los ficheros de cuarentena

5.2.10 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. Use la función *Restaurar el objeto seleccionado* sólo en casos excepcionales justificados. Restablezca 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 datos adjuntos sólo pueden restaurarse 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 datos adjuntos sólo pueden restaurarse 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.

5.2.11 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 AntiVir Scanner:

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

5.2.12 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.


5.2.13 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 Avira AntiVir Personal.

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.

5.2.14 Eventos: Filtrar eventos

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

- Updater
- Guard
- Scanner
- Programador

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 **Descripción 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 Scanner

El componente Scanner 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 mediante menú contextual (botón secundario del ratón **Analizar ficheros seleccionados con AntiVir**) se recomienda cuando se desea analizar ficheros o directorios individuales. Otra ventaja es que no es necesario arrancar primero Avira AntiVir Personal Centro de control para realizar un análisis directo.

- **Análisis directo con Arrastrar y soltar**

Al arrastrar un fichero o directorio en la ventana de Avira AntiVir Personal Centro de control, Scanner analiza el fichero o el directorio y su contenido. Esto se recomienda 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 por medio del Programador**

Programador le permite programar los 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 rootkits*
- 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, el componente AntiVir Updater se ha integrado en AntiVir Personal. AntiVir Updater se encarga de que Avira AntiVir Personal funcione siempre con la vigencia más reciente y pueda así detectar los virus que aparecen a diario. AntiVir 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 AntiVir Personal en los análisis de virus y malware, así como en la reparación de los objetos infectados.

- Motor de análisis:

El motor de análisis contiene los métodos que usa AntiVir Personal 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, AntiVir Updater ejecuta, además, una actualización de producto o bien le informa sobre la disponibilidad de ésta. Tras la actualización no es necesario reiniciar AntiVir Personal.

Nota

Por razones de seguridad, Avira AntiVir Personal Updater comprueba si el fichero host de Windows del equipo se modificó en lo que se refiere, por ejemplo, a manipulación por parte de malware de la URL de actualización de Avira AntiVir Personal con el fin de que Avira AntiVir Personal 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 Avira AntiVir Personal Updater.

En el Centro de control, en el Programador puede configurar las tareas de actualización que ejecutará AntiVir Updater con los intervalos indicados. De forma predeterminada, tras la instalación de AntiVir Personal se crea una tarea de actualización. 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 fabricante. De forma predeterminada 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 de Avira AntiVir Personal, en General :: Actualización.

8 P+F, sugerencias

En este capítulo encontrará una recopilación de preguntas frecuentes sobre Avira AntiVir Personal, ayuda en caso de problemas, así como sugerencias y trucos para el uso de Avira AntiVir Personal.

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

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. Esa es la razón de que Avira AntiVir Personal no pueda encontrar el servidor de 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 Configuración de Avira AntiVir Personal (Modo experto) en General :: Actualización.

Los virus y malware no se pueden mover ni borrar.

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

- Actualizar Avira AntiVir Personal.
- Si usa los sistemas operativos Windows XP, desactive la Restauración del Sistema.
- Arranque el PC en modo seguro
- Inicie Avira AntiVir Personal y Configuración de Avira AntiVir Personal (Modo experto).
- Seleccione Scanner :: Análisis :: Ficheros :: Todos los ficheros y pulse **Aceptar**.
- Inicie un análisis de todos los discos locales
- Arranque el PC 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 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 PC 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 copiado.

- ▶ En la Configuración de Avira AntiVir Personal (modo experto) seleccione Guard :: Análisis :: Excepciones e introduzca el nombre de proceso del software de backup.

Mi Firewall informa de AntiVir Guard, en cuanto se activa.

Causa: La Comunicación con AntiVir Guard se realiza vía TCP/IP. Un firewall monitoriza todas las conexiones con este protocolo.

- ▶ Habilite de forma general 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.

8.2 Atajos

Los comandos de teclado -conocidos como atajos - ofrecen una rápida posibilidad de encontrar módulos individuales y ejecutar acciones con Avira AntiVir Personal.

A continuación hacemos un repaso de los comando de teclado disponibles en Avira AntiVir Personal. Por favor 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	Cambiar a la sección siguiente.
Ctrl + Mayús + Tab Ctrl + Retroceder Página	Cambiar a la sección anterior.
Tab	Cambiar a la siguiente acción u opciones de grupo.
Mayús + 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	Muestra el menú del sistema
Alt + Tab	Conmuta entre la ayuda y otras posibles ventanas abiertas.
Alt + F4	Cerrar ayuda
Mayús + F10	Muestra el menú de contexto de la ayuda.
Ctrl + Tab	Cambiar a la sección siguiente en la ventana de exploración.
Ctrl + Mayús + 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.

F6	Cambiar entre las ventanas de exploración y de temas.
Retr. Pág. Av. Pág.	Avanza en el pantalla

8.2.3 en Centro de control

General

Comando de teclado	Descripción
F1	Muestra la Ayuda
Alt + F4	Cierra Centro de control
F5	Refresca la pantalla
F8	Abre la configuración
F9	Iniciar actualización

Sección Analizar

Comando de teclado	Descripción
F3	Iniciar análisis con el perfil seleccionado
F4	Crea 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...
Intro	Propiedades
Ins	Añadir fichero
Supr	Eliminar objeto

Sección Programador

Comando de teclado	Descripción
F2	Modificar tarea
Intro	Propiedades
Ins	Insertar nueva tarea
Supr	Eliminar tarea

Sección Informes

Comando de teclado	Descripción
F3	Mostrar fichero de informe
F4	Imprimir fichero de informe
Intro	Mostrar informe
Supr	Borrar informes

Sección Eventos

Comando de teclado	Descripción
F3	Exportar eventos
Intro	Mostrar evento
Supr	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 ordenador 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 y Avira AntiVir Personal

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

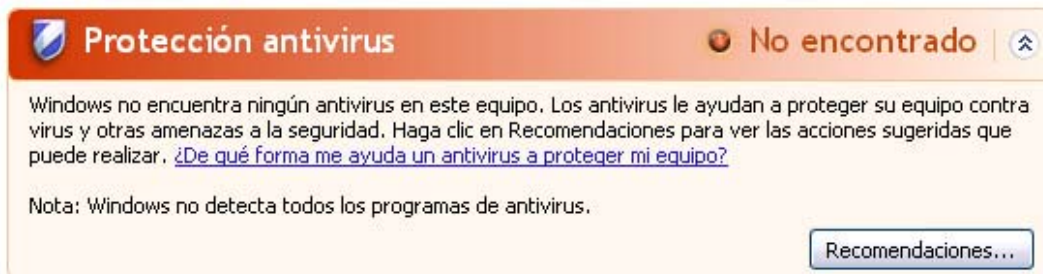
Antivirus ACTIVO

Antivirus INACTIVO

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.



Protección antivirus No encontrado

Windows no encuentra ningún antivirus en este equipo. Los antivirus le ayudan a proteger su equipo contra virus y otras amenazas a la seguridad. Haga clic en Recomendaciones para ver las acciones sugeridas que puede realizar. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Nota: Windows no detecta todos los programas de antivirus.

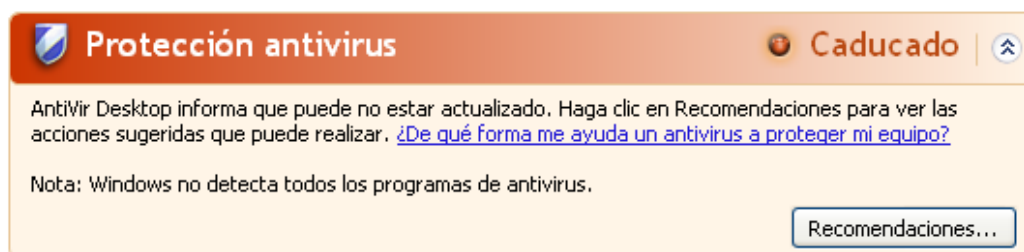
Recomendaciones...

Nota

Instale Avira AntiVir Personal en su ordenador para protegerlo contra ¡virus o programas no deseados!.

Protección Antivirus Caducada

Si ya ha instalado Windows XP Service Pack 2 o Vista y Avira AntiVir Personal, o si instala Windows XP Service Pack 2 o Vista sobre un sistema que ya tenga Avira AntiVir Personal instalado, recibirá el siguiente mensaje:



Protección antivirus Caducado

AntiVir Desktop informa que puede no estar actualizado. Haga clic en Recomendaciones para ver las acciones sugeridas que puede realizar. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Nota: Windows no detecta todos los programas de antivirus.

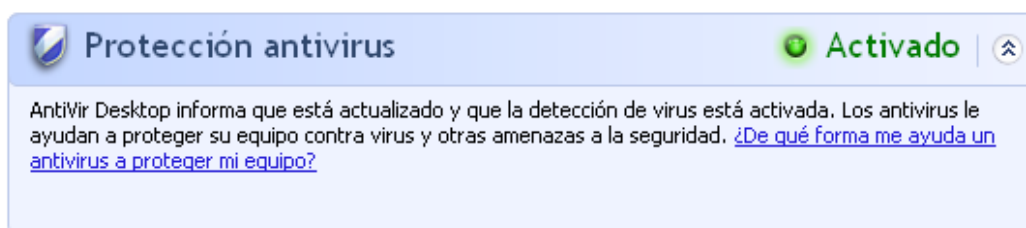
Recomendaciones...

Nota

Para que el centro de seguridad de Windows reconozca a Avira AntiVir Personal como un producto actualizado, debe de llevarse a cabo una actualización. Actualice su sistema mediante una Actualización de Avira AntiVir Personal .

Protección Virus Activa

Tras la instalación de Avira AntiVir Personal y la actualización subsecuente, recibe el siguiente mensaje:



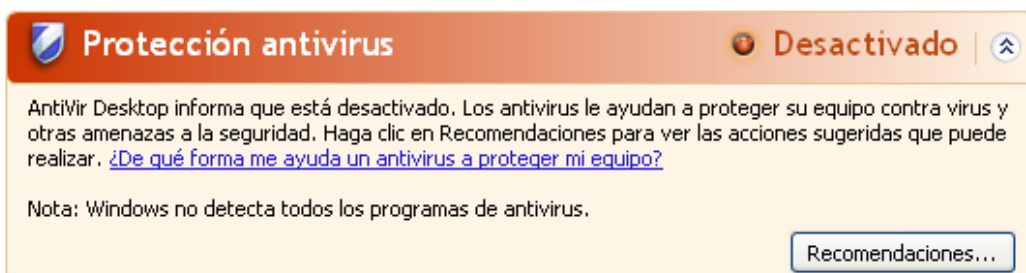
Protección antivirus Activado

AntiVir Desktop informa que está actualizado y que la detección de virus está activada. Los antivirus le ayudan a proteger su equipo contra virus y otras amenazas a la seguridad. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Avira AntiVir Personal está ahora actualizado y AntiVir Guard está activo.

Protección Antivirus Apagada

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



Protección antivirus Desactivado

AntiVir Desktop informa que está desactivado. Los antivirus le ayudan a proteger su equipo contra virus y otras amenazas a la seguridad. Haga clic en Recomendaciones para ver las acciones sugeridas que puede realizar. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Nota: Windows no detecta todos los programas de antivirus.

Recomendaciones...

Nota

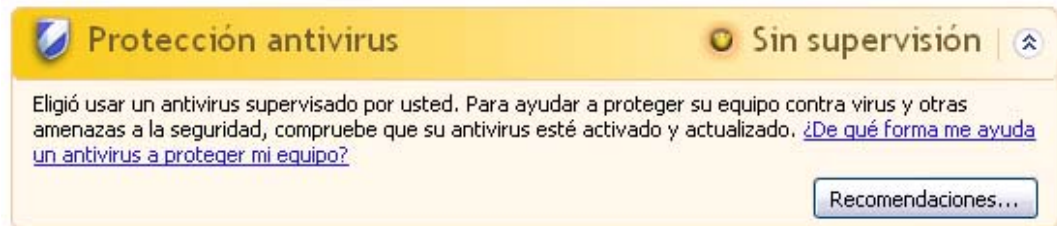
Puede activar o desactivar AntiVir Guard en la sección Descripción general :: Estado de Avira AntiVir Personal Centro de control. Además, puede ver que AntiVir Guard está activado si el paraguas rojo en la barra de tareas está abierto.

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**

Avira AntiVir Personal 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 Vista, necesita una solución Antivirus, por ejemplo: Avira AntiVir Personal. 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 Extensión de las categorías de amenazas

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 ordenador, 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 ordenadores 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.

Avira AntiVir Personal puede detectar los dialers por defecto.

Si la opción **Dialers** se activa en Extensión de Categorías de Amenazas ,recibirá una alerta al detectarse estos programas. Así puede eliminar el potencial peligro de los dialers. De todas formas si hay algún dialer excepcional que le interese, puede 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, pueden 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 ordenador en horario laboral alcanza ya magnitudes económicamente importantes. Así que no sorprende que las empresas se tomen en serio este tipo de posibles problemas.

Avira AntiVir Personal detecta juegos de ordenador. Al seleccionar **Games** con una marca en Extensión de Categorías de Amenazas recibirá una alerta de Avira AntiVir Personal si se detecta un juego. El juego ha terminado en el sentido literal, porque tiene la posibilidad de eliminarlo fácilmente.

Chistes (JOKES)

Los programas de broma sólo deben estar destinados a poner un toque de humor sin llegar a ocasionar perjuicios ni multiplicarse a sí mismos. El ordenador 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 disquete) o BUGSRES.COM(come pantallas).

Pero ¡tenga cuidado! 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.

Avira AntiVir Personal detecta estos programas y los elimina, tratándolos como programas indeseados, si fuera necesario. Si se configura **Jokes** en Extensión de Categorías de Amenazas se recibirán alertas al detectarse.

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

Software que puede comprometer la seguridad del sistema, iniciar actividades no deseadas, violar su privacidad o espiar datos y/o comportamientos.

Avira AntiVir Personal detecta el software que "Viola la privacidad". Si se elige **Riesgo de seguridad-confidencialidad** en Extensión de Categorías de Amenazas se recibirán alertas al detectar Avira AntiVir Personal software de este tipo.

Software de control de puerta trasera (BDC)

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

Avira AntiVir Personal detecta este tipo de "software de control de puerta trasera". Si se configura **Software de control de puerta trasera (BDC)** en Categorías de riesgos avanzadas, se recibirán advertencias al detectar Avira AntiVir Personal este tipo de software.

Adware/Spyware (ADSPY)

Software que muestra anuncios, mensajes o envía datos del usuario sin el conocimiento de éste.

Avira AntiVir Personal detecta este tipo de software "Adware/Spyware". Si en la configuración, en Categorías de riesgos avanzadas, está activada la opción **Adware/Spyware (ADSPY)** con una marca de verificación, recibirá la correspondiente advertencia cuando Avira AntiVir Personal realiza una detección.

Utilidades de compresión poco habituales

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

Avira AntiVir Personal detecta las "utilidades de compresión poco habituales". Si se configura **Utilidades de compresión poco habituales** en Categorías de riesgos avanzadas, recibirá una advertencia al realizar Avira AntiVir Personal una detección.

Ficheros de doble extensión (HEUR-DBLEXT)

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

Avira AntiVir Personal detecta "Los ficheros de doble extensión". Si se configura **Ficheros con extensión oculta (HEUR-DBLEXT)** en Categorías de riesgos avanzadas, se recibirán alertas al detectarse por parte de Avira AntiVir Personal.

Phishing (Pesca)

El Phishing, también conocido como *Suplantación de marca* pretende sustraer datos de clientes que acceden a servicios de banking, oficiales, proveedores de servicios, etc. en Internet.

La divulgación de la dirección de email en Internet, el rellenar formularios en línea, el 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.

Avira AntiVir Personal detecta el "Phishing". Si se configura **Phishing** en Extensión de Categorías de Amenazas, se recibirán alertas al detectar Avira AntiVir Personal el mismo.

Aplicación (APPL)

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

Avira AntiVir Personal detecta "Aplicaciones (APPL)". Si se configura **Aplicación (APPL)** en Extensión de Categorías de Amenazas, se recibirán alertas al detectar Avira AntiVir Personal la misma.

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 ordenador, 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 ordenador 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 PC atacados que ejecutan programas (normalmente troyanos o gusanos) bajo una infraestructura de control común. Estas redes pueden usarse para propagar spam, realizar ataques DDoS (ataques de denegación de servicio), etc., incluso sin que el usuario del PC tenga conocimiento de ello. El peligro principal de las redes de robots es que pueden componerse de miles de PC 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 ordenador. 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 "peligro" sin ningún tipo de comprobación real.

Honeypot (foco de atracción, ordenador 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 normalmente atacan los documentos de la aplicación, no a los ejecutables.

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 PC 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 de banking en línea 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 ordenador 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 ordenador 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 consulta acerca de cualquier producto Avira AntiVir Personal, 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

Avira AntiVir Personal ofrece soporte y asistencia para la resolución de preguntas y problemas técnicos.

Toda la información necesaria sobre nuestro soporte técnico se puede obtener en nuestra 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 el Centro de control de Avira AntiVir Personal en la opción de menú Ayuda :: Acerca de 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 la opción Enviar fichero por medio del menú contextual o el botón correspondiente.

- Envíe el fichero en cuestión comprimido (WinZIP, PKZip, Arj, etc.) adjunto en un email a virus-classic@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 Avira AntiVir Personal notifica la detección de un fichero que muy probablemente esté "limpio", envíe ese fichero comprimido (WinZIP, PKZIP, Arj, etc.) adjunto en un email a virus-classic@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 en Avira AntiVir Personal.

11.1 Scanner

La sección Scanner de la Configuración de Avira AntiVir Personal se encarga de la configuración del análisis directo, es decir del análisis a petición.

11.1.1 Análisis

Aquí se define el comportamiento básico al proceder con un análisis directo. Si seleccionas ciertas carpetas en un análisis directo, dependiendo de la configuración, Scanner 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

Scanner puede usar un filtro para analizar sólo ficheros de una cierta extensión.

Todos los ficheros

Al seleccionar esta opción, se analizan todos los ficheros sin tener en cuenta su extensión ni contenido, en busca de malware. No se utilizó ningún filtro.

Nota

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

Extensiones inteligentes

Si se activa esta opción, Avira AntiVir Personal elige automáticamente los ficheros seleccionados para analizarlos. Es decir que Avira AntiVir Personal decide sobre la base del contenido de un fichero si éste se analizará o no en cuanto a virus y programas no deseados. Esto es algo más lento que Usar la lista de extensiones de fichero, pero más seguro, ya que no se analiza únicamente en base a la extensión del fichero. Esta configuración está por defecto 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

Si se activa esta opción, sólo se analizan ficheros de la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están establecidos. Esta lista puede editarse manualmente con el botón **Extensiones de ficheros**

Nota

Si se activa esta opción y has eliminado todas las entradas de la lista, esto se indica como "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**. Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota

La lista por defecto puede variar entre versiones.

Configuración avanzada

Analizar los sectores de arranque de los discos seleccionados

Al seleccionar esta opción, Scanner sólo analiza los sectores de arranque de las unidades seleccionadas para al análisis directo. Esta opción está activada de forma predeterminada.

Analizar sectores de arranque maestros

Si se activa esta opción, el Scanner sólo analiza los sectores de arranque maestros de los discos duros usados en el sistema.

Omitir ficheros online

Si está activada esta opción, el análisis directo omite por completo los así llamados ficheros offline durante el análisis. Es decir, que no se analiza los mismos en busca de malware. Los ficheros offline son aquéllos que se han movido físicamente del disco duro a otro medio, p. ej., una cinta, en un sistema jerárquico de administración de almacenamientos (HSMS, del inglés Hierarchical Storage Management System). Esta opción está activada de forma predeterminada.

Comprobación de integridad de 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 predeterminada.

Análisis optimizado

Si la opción está activada, durante el análisis del Scanner 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 ordenadores con multiprocesador. Si AntiVir Personal se administra con SMC, la opción se muestra en todos los casos y se puede activar: Si el equipo administrado no dispone de varios procesadores, el Scanner no usa la opción.

Seguir enlaces simbólicos

Si la opción está activada, Scanner sigue durante el análisis todos los accesos directos simbólicos del perfil de análisis o del directorio seleccionado con el fin de analizar los ficheros vinculados acerca de la existencia de virus y malware. Esta opción no es compatible con Windows 2000 y está desactivada de forma predeterminada.

Importante

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

Análisis de rootkits al iniciar

Si se activa esta opción, al inicio del análisis el Scanner comprueba si hay rootkits en el directorio del sistema Windows con un así llamado procedimiento rápido. Este procedimiento no analiza la existencia de rootkits activos en el equipo tan exhaustivamente como lo hace el perfil de análisis **Búsqueda de rootkits**, pero su ejecución es considerablemente más rápida.

Importante

El análisis de rootkit no está disponible en los sistemas de 64 bits!

Proceso de análisis

Permitir detención

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 de "Luke Filewalker". Si has desactivado esta configuración, el botón **Detener** en la ventana de "Luke Filewalker" aparece en gris. Con lo cual el análisis ¡no se puede detener de forma prematura! Esta opción está activada de forma predeterminada.

Prioridad del escáner

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

Bajo

El sistema operativo únicamente asigna tiempo de procesador al Scanner si ningún otro proceso necesita tiempo de procesador, es decir, mientras sólo se esté ejecutando el Scanner, la velocidad es la máxima. Globalmente, así se facilita el trabajo con otros programas: el equipo reacciona más rápidamente cuando otros programas precisan tiempo de cálculo y en esos casos el Scanner continúa ejecutándose en segundo plano. Esta configuración está por defecto y es la recomendada.

Medio

A Scanner se le asigna una prioridad normal. El sistema operativo da a todos los procesos la misma cantidad de proceso en teoría. En ciertas circunstancias, puede afectarse el rendimiento de otras aplicaciones.

Alto

A Scanner se le asigna una prioridad máxima. El trabajo simultáneo con otras aplicaciones es casi imposible. Scanner analiza con la mayor velocidad posible.

11.1.1.1. Acción en caso de detección

Acción en caso de detección

Puede definir las acciones a tomar de Scanner, cuando se detecta un virus o programa no deseado.

Interactiva

Si se activa esta opción, las detecciones del análisis del Scanner se notifican en un cuadro de diálogo. Cuando se analiza la existencia de rootkits, virus del sector de arranque y procesos activos, aparece un cuadro de diálogo en el que puede seleccionar lo que debe hacerse con el objeto afectado. Durante el análisis de ficheros, la notificación y la posibilidad de selección del tratamiento de los ficheros afectados dependen del modo de notificación seleccionado. Esta opción está activada de forma predeterminada.

Encontrará más información aquí.

Modo de notificación

El modo de notificación permite definir la manera con la que se notificarán las detecciones de virus durante el análisis de ficheros del Scanner. Con el modo de notificación se especifica si habrá posibilidades de selección del tratamiento de los ficheros afectados.

Combinado

En el modo de notificación combinado se recibe al finalizar el análisis de ficheros un mensaje de advertencia con una lista de los ficheros afectados detectados. No hay posibilidades de seleccionar el tratamiento de los ficheros afectados. Puede ejecutar la acción predeterminada del Scanner para todos los ficheros afectados o cancelar el Scanner.

Combinado (experto)

En el modo de notificación experto se recibe al finalizar el análisis de ficheros 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 Scanner.

Personalizado

En el modo de notificación personalizado, cada detección de virus durante el análisis de ficheros se notifica en una ventana aparte. En el cuadro de diálogo puede seleccionar lo que debe hacerse con el fichero afectado.

Automático

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

Copiar fichero a cuarentena antes de la acción

Si se activa esta opción, Scanner 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 a Avira Malware Research Center para ser analizado a fondo.

Acción Primaria

La acción Primaria es la que se ejecuta cuando Scanner encuentra 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 configuró **La opción Primaria** como **Reparar**.

reparar

Si se selecciona esta opción Scanner repara los ficheros automáticamente. Si Scanner no puede reparar el fichero afectado, ejecuta la acción Acción Secundaria.

Nota

Se recomienda la reparación automática, pero eso significa que Scanner puede modificar los ficheros en el PC.

eliminar

Al seleccionar esta opción el fichero se elimina, pero puede recuperarse con las herramientas adecuadas (ej. Avira UnErase). Esto significa que el patrón de virus podrá ser detectado nuevamente.

cambiar nombre

Si se activa esta opción, Scanner 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

Al elegir esta opción, se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el PC! ¡Podría causar daños graves en el PC!

cuarentena

Al habilitar esta opción, Scanner mueve el fichero a cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse a Avira Malware Research Center.

Acción secundaria

La opción **Acción secundaria** sólo puede seleccionarse si en **Acción principal** se seleccionó el parámetro reparar. Con esta opción se decide qué hacer si el fichero afectado no puede repararse.

eliminar

Al seleccionar esta opción el fichero se elimina, pero puede recuperarse con las herramientas adecuadas (ej. Avira UnErase). Esto significa que el patrón de virus podrá ser detectado nuevamente.

cambiar nombre

Si se activa esta opción, Scanner 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

Al elegir esta opción, se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el PC! ¡Podría causar daños graves en el PC!

cuarentena

Al habilitar esta opción, Scanner mueve el fichero a Cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse a Avira Malware Research Center.

Nota

Si seleccionó 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 Scanner analiza ficheros utiliza un análisis recursivo: también se descomprimen los archivos dentro de otros archivos y se analizan en busca de virus y programas no deseados. Los ficheros se analizan, descomprimen y vuelven a analizarse.

Analiza ficheros comprimidos

Con esta opción se analizan los archivos comprimidos seleccionados en la lista. Esta opción está activada de forma predeterminada.

Todos los tipos de archivo

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

Extensiones inteligentes

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

Nota

Sólo se soportan aquéllos tipos de ficheros comprimidos, marcados en la lista.

Límite de profundidad en la recursión

El descomprimir y analizar ficheros profundamente entrelazados puede requerir gran cantidad de tiempo y recursos. Al activar esta opción, limitas la profundidad del análisis en ficheros comprimidos múltiples veces (máximo nivel de recursión). Esto ahorra tiempo y recursos del PC.

Nota

Para encontrar un virus o programa no deseado, Scanner debe de analizar hasta el nivel donde se encuentre el código dañino.

Nivel máximo de recursividad

Para introducir el máximo nivel de recursión, se debe activar la opción Límite de profundidad de recursión.

Puede introducir directamente el nivel de recursividad pertinente o cambiarlo con las teclas de flecha que hay a la derecha del campo de entrada. Los valores permitidos 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

En este apartado, puede establecer qué ficheros comprimidos debiera analizar Scanner. Para ello, debe seleccionar las entradas relevantes.

11.1.1.2. Heurística

Scanner omite estos ficheros.

La lista en esta ventana contiene los ficheros y rutas que no deben de incluirse en el análisis en busca de virus o programa no deseados por parte de Scanner

Por favor, introduce las mínimas excepciones posibles que consideres que no debieran incluirse en un análisis de rutina. Le recomendamos que los ficheros incluidos en esta lista hayan sido analizados antes.

Nota

La suma de las entradas de la lista no puede superar el máximo de 6.000 caracteres.

Advertencia

Estos ficheros no se incluyen en el análisis.

Nota

Los ficheros incluidos en esta lista se anotan en el fichero de informe. Por favor, comprueba el informe de análisis de vez en cuando, ya que los ficheros excluidos pudiera ser necesario analizarlos de nuevo. En este caso, debieras retirarlo(s) de esta lista.

Campo de entrada

En esta ventana, puede introducir el nombre del fichero que no deseas incluir en el análisis directo. No hay objeto introducido por defecto.



El botón abre una ventana en la que puede seleccionar el fichero o la ruta pertinente. Cuando introduces un fichero con su ruta completa, sólo este fichero se excluye del análisis. Si has introducido 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 la entrada no está 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 de Scanner, 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 de Avira AntiVir Personal.

Avira AntiVir Personal dispone 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 software malintencionado. 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, basado en su conocimiento o experiencia previa.

Heurística de macrovirus

Heurística de macrovirus

Avira AntiVir Personal contiene una potente herramienta de heurística para macro virus. Si se activa esta opción, se eliminan todas la 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. Esta opción está activada de forma predeterminada y es la recomendada.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Avira AntiVir Personal dispone con la tecnología AntiVir AHeAD de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Al activar esta opción, puede definir el nivel de "tolerancia " de la heurística. Esta opción está activada de forma predeterminada.

Nivel de detección bajo

Si está activada la opción, Avira AntiVir Personal detecta menos malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es 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, Avira AntiVir Personal detecta bastante más malware desconocido pero hay que contar con detecciones erróneas.

11.1.2 Informe

Scanner 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 puedas establecer qué acciones debe tomar Scanner al encontrar un virus o programa no deseado, debe de crearse siempre un fichero de informe.

Informes

Desactivado

Al activar esta opción, Scanner no informa de las acciones o resultados de un análisis directo.

Predeterminado

Si se selecciona esta opción Scanner informa del nombre y ruta de los ficheros afectados. Además, en el fichero de informe aparece la configuración del análisis, información de la versión y del propietario de la licencia.

Avanzado

Al activar esta opción Scanner informa de alertas e instrucciones, además de los nombres y rutas de los ficheros afectados.

Completo

Si se selecciona esta opción, Scanner informa de todos los ficheros analizados. Además se incluyen en el informe todos los ficheros, así como alertas y mensajes .

Nota

Si tienes que enviarnos algún informe para resolver algún problema, hazlo en este modo.

11.2 Guard

La sección Guard de Configuración de Avira AntiVir Personal es responsable de la configuración del análisis en tiempo real.

11.2.1 Análisis

Normalmente desearás monitorizar tu sistema de forma constante. En este momento utiliza 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

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

Analizar al escribir

Al activar esta opción, Guard analiza el fichero al ser escrito. Sólo puede acceder al fichero de nuevo cuando se ha completado el proceso.

Analiza en lectura y escritura

Al activar esta opción, Guard analiza los ficheros antes de ser abiertos, leídos, ejecutados y después de ser escritos. Esta opción está activada de forma predeterminada y es la recomendada.

Ficheros

Guard puede usar un filtro para analizar sólo ficheros de una cierta extensión.

Todos los ficheros

Si esta opción está activada, se analizan todos los ficheros independientemente de su extensión.

Nota

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

Extensiones inteligentes

Si se activa esta opción, Avira AntiVir Personal elige automáticamente los ficheros seleccionados para analizarlos. Esto significa que Avira AntiVir Personal decide, dependiendo del contenido, si los ficheros se analizan o no. 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

Si se activa esta opción, sólo se analizan ficheros de la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están establecidos. Esta lista puede editarse manualmente con el botón **Extensiones de ficheros** Esta configuración está por defecto y es la recomendada.

Nota

Si se activa esta opción y has eliminado todas las entradas de la lista, esto se indica como "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**. 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 comprimidos. Al utilizar esta opción se analizan los ficheros, se descomprimen y se analizan de nuevo. Esta opción no está activa por defecto. Se limitan el análisis de archivos mediante el nivel de recursividad, la cantidad de ficheros que se analizarán y el tamaño del archivo. Puede establecer el nivel de recursividad, la cantidad de ficheros que se analizarán y el tamaño máximo del archivo.

Nota

Esta opción no está activa por defecto, ya que sobrecarga mucho al procesador. En general se recomienda que los 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 dentro de otros archivos 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 se recomienda. Se descomprimen y analizan todos los archivos que se encuentren directamente en el archivo principal.

Máximo número de ficheros

Al analizar archivos el análisis se limita a una cantidad máxima de ficheros. El valor predeterminado para la cantidad máxima de ficheros que se analizarán es 10 y se recomienda.

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

Esta opción está activada y se añadirá una entrada en el registro de eventos. El administrador puede identificar las detecciones y reaccionar de acuerdo a las mismas. Esta opción está activada de forma predeterminada.

Advertencia acústica

Si la opción está activada, Guard reproduce una secuencia de sonidos al producirse una detección. Esta opción está activada de forma predeterminada.

11.2.1.2. Excepciones

Estas opciones permiten configurar los objetos de excepción para Guard (análisis en tiempo real). Los objetos en cuestión no se considerarán en el análisis en tiempo real. Mediante la lista de procesos omitidos, 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.

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 se considerará durante el análisis en tiempo real. De forma predeterminada no hay ningún proceso indicado. La manera más fácil de saber el nombre del proceso pertinente es mediante el Administrador de tareas. En la pestaña "Procesos" (inglés: "Processes") del Administrador de tareas encontrará los nombres de todos los procesos activos actualmente. Busque "su" proceso e indique ese nombre en "Nombre" (inglés: "Image Name").

Nota

Puede introducir un máximo de 20 procesos.

Atención:

Sólo se tienen en cuenta los primeros 15 caracteres del nombre del proceso (incluida la extensión de fichero). Si hay 2 procesos cuyos nombres coinciden en los primeros 15 caracteres, ambos procesos se excluyen de la supervisión de Guard.

Advertencia

Tenga en cuenta que todos los ficheros accedidos por los procesos en la lista ¡son excluidos del análisis en busca de virus y programas no deseados! El explorador de Windows y el sistema operativo en sí no pueden excluirse. La entrada correspondiente en la lista se ignora.

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.

Guard omite estos ficheros.

Todos los objetos accedidos en esta lista son excluidos del análisis realizado por Guard.

Nota

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

Campo de entrada

En esta ventana, puede introducir el nombre del fichero que no deseas incluir en el análisis en tiempo real. No hay objeto introducido por defecto.



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.

Por favor, ten en cuenta los siguientes puntos:

- Los comodines * (sin límite de caracteres) e ? (un solo carácter) sólo están permitidos en el nombre de fichero.
- 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.
- La lista se procesa de arriba a abajo.
- También se pueden excluir extensiones de fichero por separado (incluidos los comodines).
- Si se excluye un directorio, todos sus subdirectorios se excluyen automáticamente.
- Cuanto más larga es la lista, más tiempo de procesador se requiere para procesar la lista en cada acceso. Por lo tanto se recomienda una lista corta.
- Para excluir objetos a los que se tiene acceso con nombres de fichero DOS cortos (convención de nombres 8.3), el nombre de fichero en cuestión también debe introducirse 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

En el caso de unidades dinámicas que se integran (montan) como directorio en otra unidad, debe usar el alias del sistema operativo para la unidad integrada en la lista de excepciones:

p. ej., \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\

Si usa el punto de montaje (mount point) propiamente dicho, p. ej., C:\DynDrive, la unidad dinámica se analiza de todos modos. El fichero de informe de Guard permite determinar el nombre de alias del sistema operativo que se debe usar.

Nota

Mediante el fichero de informe de Guard puede determinar las rutas que usará Guard al analizar la existencia de ficheros afectados. Use por principio las mismas rutas en la lista de excepciones. Proceda del modo siguiente: establezca la función de registro de Guard en la configuración, en Guard :: informe, en **Completo**. Con Guard activado, acceda a los ficheros, directorios unidades incorporadas . Ahora puede leer la ruta que debe usarse en el fichero de informe de Guard. El fichero de informe se activa en el Centro de control, en Protección local :: Guard.

Ejemplos:

C:

C:\

C:*.*

C:*

*.exe

*.xl?

.

C:\Archivos de programa\Aplicación\aplicación.exe\

C:\Archivos de programa\Aplicación\aplic*.exe\

C:\Archivos de programa\Aplicación\aplic*

C:\Archivos de programa\Aplicación\aplic????.e*

C:\Archivos de programa\

C:\Archivos de programa

C:\Archivos de programa\Aplicación*.mdb

11.2.1.3. Heurística

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

Avira AntiVir Personal dispone 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 software malintencionado. 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, basado en su conocimiento o experiencia previa.

Heurística de macrovirus

Heurística de macrovirus

Avira AntiVir Personal contiene una potente herramienta de heurística para macro virus. Si se activa esta opción, se eliminan todas la 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. Esta opción está activada de forma predeterminada y es la recomendada.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Avira AntiVir Personal dispone con la tecnología AntiVir AHeAD de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Al activar esta opción, puede definir el nivel de "tolerancia " de la heurística. Esta opción está activada de forma predeterminada.

Nivel de detección bajo

Si está activada la opción, Avira AntiVir Personal detecta menos malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es 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, Avira AntiVir Personal detecta bastante más malware desconocido pero hay que contar con detecciones erróneas.

11.2.2 Informe

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

Informes

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

Desactivado

Con esta opción Guard no crea ningún registro/informe.
Es recomendable que desactives la generación de registro sólo en casos excepcionales.

Predeterminado

Si la opción está activada, Guard incluye información importante (sobre la detección, advertencias y errores) en el fichero de registro; la información de menor importancia se omite para mayor claridad. Esta opción está activada de forma predeterminada.

Avanzado

Al activar esta opción Guard registra también información secundaria.

Completo

Si la opción está activada, 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. Esta opción está activada por defecto con 1 MB.

Guardar fichero de informe antes de reducir

Si está activada esta opción, se hace una copia del 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.

11.3 General

11.3.1 Configuración :: General

11.3.1.1. Categorías de riesgos avanzadas

Selección de categorías de riesgos avanzadas

Avira AntiVir Personal le protege ante virus y programas mal intencionados.

Además, puede ejecutar un análisis de acuerdo a 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.

11.3.2 Seguridad

Actualización

Alertar si la última actualización se produjo hace más de n día(s)

Aquí puede introducir el máximo número de días permitidos sin que Avira AntiVir Personal se actualice. Si se supera ese tiempo, en el Programador se muestra un mensaje de advertencia.

Mostrar nota si el fichero de firmas de virus está obsoleto

Al activar esta opción, 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 actualización no se ha producido desde hace más de cierto número de días.

Análisis completo del sistema

En esta área puede configurar el indicador de estado del análisis completo del sistema en el Centro de control, en Información general:: Estado.

Estado 'amarillo' si anterior a n días

Introduzca en este campo un intervalo de tiempo en días desde el último análisis completo del sistema para que, si se supera, el indicador de estado cambie a amarillo. El intervalo de tiempo indicado debe ser menor que el que consta en el estado rojo. El valor predeterminado es de siete días y se recomienda.

Estado 'rojo' si anterior a n días

Introduzca en este campo un intervalo de tiempo en días desde el último análisis completo del sistema para que, si se supera, el indicador de estado cambie a rojo. El intervalo de tiempo indicado debe ser mayor que el que consta en el estado amarillo. El valor predeterminado es de 30 días y se recomienda.

Nota

Si indica 0 en estos intervalos de tiempo, la supervisión de estado del análisis completo del sistema queda desactivada. Se muestra siempre un icono verde. Este parámetro sólo debe configurarse en casos excepcionales justificados. Si sólo se establece uno de los intervalos de tiempo en 0, la indicación se descarta como no válida.

Protección del producto

Previene la finalización del proceso

Si se activa esta opción, los procesos de AntiVir quedan protegidos contra finalización no deseada por virus y malware o bien contra la finalización 'sin control' por parte de un usuario, p. ej., a través del Administrador de tareas. Esta opción está establecida por defecto.

Importante

La protección de procesos todavía no está disponible para sistemas de 64 bits.

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

Si se activa esta opción, todas las entradas en el registro de AntiVir Personal, 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.

Nota

Al activar esta opción 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 del registro todavía no está disponible para sistemas de 64 bits.

11.3.3 WMI

Compatibilidad con Instrumental de administración de Windows

El Instrumental de administración de Windows 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. AntiVir Personal 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 de AntiVir Personal .

Activar compatibilidad con WMI

Si esta opción está activada, puede consultar los datos operativos de AntiVir Personal por medio de WMI.

11.3.4 Directorios

Ruta temporal

En este campo puede introducir la ruta para los ficheros temporales de Avira AntiVir Personal.

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.

11.3.5 Actualización

La sección **Actualización** de la Configuración de Avira AntiVir Personal se encarga de configurar el Updater .

Actualizaciones de producto

Descargar actualizaciones de producto e instalar automáticamente

Si está activada esta opción, AntiVir Updater descarga las actualizaciones de producto y las instala automáticamente en cuanto están 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.

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 de AntiVir Updater en el Centro de control, en Información general ::Eventos.

No descargar actualizaciones de producto

Si está activada la opción, AntiVir Updater no lleva a cabo actualizaciones automáticas del producto ni notificaciones sobre la disponibilidad de dichas actualizaciones. 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).

11.3.5.1. Servidor web

La actualización puede realizarse desde un servidor de 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.

Avira AntiVir Personal 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 teclees será 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 Avira AntiVir Personal.

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.

Proxy

Servidor proxy

No utilizar servidor proxy

Al activar esta opción, su conexión a Internet no se lleva a través de un Proxyserver.

Utilizar configuración del sistema de Windows

Al activar esta opción un servidor proxy establece su conexión al servidor web, con la configuración de sistema de Windows.

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

Por favor, introduzca la URL o IP del servidor Proxy que desea usar para conectar al servidor web.

Puerto

Introduzca el puerto del servidor proxy por el que se conecta a Internet.

Nombre de inicio de sesión

Introduzca el nombre de inicio de sesión en el 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

11.3.6 Alertas

11.3.6.1. Advertencias acústicas

Advertencia acústica

Cuando el Scanner 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 Scanner se establece en la configuración, en Scanner::Análisis::Acción en caso de detección.

Sin advertencia

Si la opción está activada, en caso de que el Scanner 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 Scanner 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 PC.

Usar el siguiente fichero WAV (sólo en modo interactivo)

Si la opción está activada, en caso de que el Scanner 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 Wav

En este campo, puede introducir el nombre y ruta del fichero de audio deseado. De forma predeterminada consta el sonido de advertencia estándar de AntiVir Personal.



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 wav

11.3.7 Eventos

Limitar tamaño de base de datos de eventos

Limita el máximo número de eventos a n entradas

Si se elige esta opción el máximo número de eventos listados 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 elige 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 por defecto 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. Sin embargo, en el Centro de control, en Eventos, se muestra un máximo de 20.000 entradas.

11.3.8 Límite de informes

Límite de informes

Limitado el número a n unidades

Si se activa esta opción, 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 día(s)

Al activar esta opción, los informes se eliminan automáticamente tras un número específico de días. Los valores permisibles están en 1 y 90 días. Esta opción está habilitada por defecto con un valor de 30 días.

No limitar el número de informes (eliminar informes manualmente)

Al activar esta opción, la cantidad de informes no se limitará.

11.3.9 Advertencias acústicas

Advertencia acústica

Cuando el Scanner 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 Scanner se establece en la configuración, en Scanner::Análisis::Acción en caso de detección.

Sin advertencia

Si la opción está activada, en caso de que el Scanner 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 Scanner 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 PC.

Usar el siguiente fichero WAV (sólo en modo interactivo)

Si la opción está activada, en caso de que el Scanner 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 Wav

En este campo, puede introducir el nombre y ruta del fichero de audio deseado. De forma predeterminada consta el sonido de advertencia estándar de AntiVir Personal.



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 wav

//// Avira AntiVir Personal – Free Antivirus

Avira GmbH

Lindauer Str. 21
88069 Tett nang
Alemania
Teléfono: +49 7542-500 0
Fax: +49 7542-525 10
Internet: <http://www.avira.es>

© Avira GmbH. Reservados todos los derechos.

Este manual se ha elaborado con sumo cuidado. No obstante, no se descartan errores de forma o de contenido. No se permite reproducir esta publicación o parte de ella por ningún medio sin la previa autorización por escrito de Avira GmbH.

Salvo errores y modificaciones técnicas.

Versión del cuarto trimestre de 2009

AntiVir[®] es una marca registrada de Avira GmbH, Alemania. Todos los demás nombres de marcas y productos son marcas o marcas registradas de sus respectivos propietarios. Las marcas protegidas no se indican como tales en este manual. Esto no significa, de todas formas, que pueden usarse libremente.