# Anti-Virus AVG 9 más Firewall

## Manual del usuario

**Revisión del documento 90.21 (3.2.2010)**

Copyright AVG Technologies CZ, s.r.o. Todos los derechos reservados.
Todas las demás marcas comerciales pertenecen a sus respectivos propietarios.

Este producto emplea el MD5 Message-Digest Algorithm de RSA Data Security, Inc., Copyright (C) 1991-2 de RSA Data Security, Inc. Creado en 1991.
Este producto emplea código de la biblioteca C-SaCzech, Copyright (c) 1996-2001 de Jaromir Dolecek (dolecek@ics.muni.cz).
Este producto emplea la biblioteca de compresión zlib, Copyright (C) 1995-2002 de Jean-loup Gailly y Mark Adler.
Este producto emplea la biblioteca de compresión libbzip2, Copyright (C) 1996-2002 de Julian R. Seward.

# Contenidos

**1. Introducción** ..... **7**

**2. Requisitos de instalación de AVG** ..... **8**

2.1 Sistemas de operación compatibles ..... 8
2.2 Requisitos mínimos y recomendados de hardware ..... 8

**3. Opciones de instalación de AVG** ..... **9**

**4. Administrador de descargas de AVG** ..... **10**

4.1 Selección de idioma ..... 10
4.2 Verificación de conectividad ..... 11
4.3 Configuración proxy ..... 12
4.4 Descargar archivos para instalar ..... 13

**5. Proceso de instalación de AVG** ..... **14**

5.1 Ejecución de la instalación ..... 14
5.2 Contrato de licencia ..... 15
5.3 Verificando el estado del sistema ..... 15
5.4 Seleccionar el tipo de instalación ..... 16
5.5 Activar su licencia AVG ..... 16
5.6 Instalación personalizada: carpeta de destino ..... 18
5.7 Instalación personalizada: selección del componente ..... 19
5.8 Barra de herramientas AVG Security ..... 20
5.9 Cierre las aplicaciones que estén abiertas ..... 21
5.10 Instalación de AVG ..... 22
5.11 Programar análisis y actualizaciones automáticas ..... 23
5.12 Selección de uso de equipo ..... 23
5.13 Conexión a Internet del equipo ..... 24
5.14 La configuración de la protección AVG ha finalizado ..... 25

**6. Después de la instalación** ..... **26**

6.1 Optimización del análisis ..... 26
6.2 Registro del producto ..... 26
6.3 Acceso a la interfaz de usuario ..... 26
6.4 Análisis de todo el equipo ..... 27
6.5 Análisis Eicar ..... 27

6.6 Configuración predeterminada de AVG ..... 28

**7. Interfaz del usuario de AVG ..... 29**

7.1 Menú del sistema ..... 30

*7.1.1 Archivo ..... 30*

*7.1.2 Componentes ..... 30*

*7.1.3 Historial ..... 30*

*7.1.4 Herramientas ..... 30*

*7.1.5 Ayuda ..... 30*

7.2 Información del estado de seguridad ..... 33

7.3 Vínculos rápidos ..... 34

7.4 Descripción general de los componentes ..... 35

7.5 Estadísticas ..... 36

7.6 Icono en la bandeja de sistema ..... 37

**8. Componentes de AVG ..... 38**

8.1 Antivirus ..... 38

*8.1.1 Antivirus Principios de ..... 38*

*8.1.2 Interfaz de Antivirus ..... 38*

8.2 Anti-Spyware ..... 40

*8.2.1 Anti-Spyware Principios de ..... 40*

*8.2.2 Interfaz de Anti-Spyware ..... 40*

8.3 Anti-Rootkit ..... 42

8.4 Firewall ..... 42

*8.4.1 Principios de Firewall ..... 42*

*8.4.2 Perfiles del Firewall ..... 42*

*8.4.3 Interfaz de Firewall ..... 42*

8.5 Analizador de correos electrónicos ..... 47

*8.5.1 Principios del analizador de correos electrónicos ..... 47*

*8.5.2 Interfaz del analizador de correos electrónicos ..... 47*

*8.5.3 Detección del analizador de correos electrónicos ..... 47*

8.6 Licencia ..... 52

8.7 Link Scanner ..... 53

*8.7.1 Principios de Link Scanner ..... 53*

*8.7.2 Interfaz de Link Scanner ..... 53*

*8.7.3 AVG Search-Shield ..... 53*

*8.7.4 Protección de navegación activa AVG ..... 53*

8.8 Online Shield ..... 57

*8.8.1 Principios de Online Shield* ..... *57*
*8.8.2 Interfaz de Online Shield* ..... *57*
*8.8.3 Detección de Online Shield* ..... *57*
8.9 Protección residente ..... 63
*8.9.1 Protección residente Principios de* ..... *63*
*8.9.2 Interfaz de protección residente* ..... *63*
*8.9.3 Detección de protección residente* ..... *63*
8.10 Administrador de actualización ..... 68
*8.10.1 Principios de administrador de actualización* ..... *68*
*8.10.2 Interfaz de administrador de actualización* ..... *68*

**9. Barra de herramientas AVG Security ..... 71**

9.1 Barra de herramientas AVG Security Interfaz ..... 71
9.2 Opciones de la Barra de herramientas AVG Security ..... 73
*9.2.1 Pestaña General* ..... *73*
*9.2.2 Pestaña Botones útiles* ..... *73*
*9.2.3 Pestaña Seguridad* ..... *73*
*9.2.4 Pestaña Opciones avanzadas* ..... *73*

**10. Configuración avanzada de AVG ..... 78**

10.1 Apariencia ..... 78
10.2 Sonidos ..... 81
10.3 Ignorar condiciones de falla ..... 82
10.4 Bóveda de Virus ..... 83
10.5 Excepciones de PUP ..... 84
10.6 Online Shield ..... 86
*10.6.1 Protección Web* ..... *86*
*10.6.2 Mensajería instantánea* ..... *86*
10.7 Link Scanner ..... 90
10.8 Análisis ..... 91
*10.8.1 Analizar todo el equipo* ..... *91*
*10.8.2 Análisis de extensión de la shell* ..... *91*
*10.8.3 Analizar carpetas o archivos específicos* ..... *91*
*10.8.4 Análisis de dispositivos extraíbles* ..... *91*
10.9 Programaciones ..... 98
*10.9.1 Análisis programado* ..... *98*
*10.9.2 Programación de actualización de la base de datos de virus* ..... *98*
10.10 Analizador de correos electrónicos ..... 109

*10.10.1 Certificación* ..... *109*
*10.10.2 Filtro de correos electrónicos* ..... *109*
*10.10.3 Registros y resultados* ..... *109*
*10.10.4 Servidores* ..... *109*
10.11 Protección residente ..... 119
*10.11.1 Configuración avanzada* ..... *119*
*10.11.2 Exclusiones de directorio* ..... *119*
*10.11.3 Archivos excluidos* ..... *119*
10.12 Servidor de caché ..... 124
10.13 Anti-Rootkit ..... 125
10.14 Actualización ..... 126
*10.14.1 Proxy* ..... *126*
*10.14.2 Conexión telefónica* ..... *126*
*10.14.3 URL* ..... *126*
*10.14.4 Administrar* ..... *126*
10.15 Administración remota ..... 133

**11. Configuración del Firewall ..... 135**

11.1 General ..... 135
11.2 Seguridad ..... 136
11.3 Perfiles de áreas y adaptadores ..... 137
11.4 Registros ..... 138
11.5 Perfiles ..... 140
*11.5.1 Información del perfil* ..... *140*
*11.5.2 Redes definidas* ..... *140*
*11.5.3 Aplicaciones* ..... *140*
*11.5.4 Servicios del sistema* ..... *140*

**12. Análisis de AVG ..... 152**

12.1 Interfaz de análisis ..... 152
12.2 Análisis predefinidos ..... 153
*12.2.1 Analizar todo el equipo* ..... *153*
*12.2.2 Analizar carpetas o archivos específicos* ..... *153*
12.3 Análisis en el Explorador de Windows ..... 161
12.4 Análisis de línea de comandos ..... 162
*12.4.1 Parámetros del análisis de CMD* ..... *162*
12.5 Programación de análisis ..... 165
*12.5.1 Configuración de programación* ..... *165*

*12.5.2 Cómo analizar* ..... *165*
*12.5.3 Qué analizar* ..... *165*
12.6 Descripción general de los resultados del análisis ..... 176
12.7 Detalles de los resultados del análisis ..... 177
*12.7.1 Pestaña Descripción general de los resultados* ..... *177*
*12.7.2 Pestaña Infecciones* ..... *177*
*12.7.3 Pestaña Spyware* ..... *177*
*12.7.4 Pestaña Advertencias* ..... *177*
*12.7.5 Pestaña Rootkits* ..... *177*
*12.7.6 Pestaña Información* ..... *177*
12.8 Bóveda de virus ..... 186

**13. Actualizaciones de AVG ..... 188**

13.1 Niveles de actualización ..... 188
13.2 Tipos de actualización ..... 188
13.3 Proceso de actualización ..... 189

**14. Historial de eventos ..... 190**

**15. Preguntas frecuentes y soporte técnico ..... 192**

# 1. Introducción

Este manual del usuario proporciona documentación exhaustiva para **Anti-Virus AVG 9 más Firewall**.

**Felicidades por la compra de Anti-Virus AVG 9 más Firewall.**

**Anti-Virus AVG 9 más Firewall** es uno de los productos de una gama de productos galardonados de AVG, diseñados para proporcionarle tranquilidad y total seguridad para su equipo. Al igual que todos los productos de AVG, **Anti-Virus AVG 9 más Firewall** ha sido completamente rediseñado desde la base, para proporcionar la protección de seguridad renombrada y acreditada de AVG de una forma nueva, más agradable y eficiente para el usuario.

El nuevo producto **Anti-Virus AVG 9 más Firewall** tiene una interfaz simplificada combinada con un análisis más agresivo y rápido. Para su conveniencia se han automatizado más funciones de seguridad y se han incluido nuevas opciones inteligentes del usuario de manera que pueda adaptar las funciones de seguridad a su estilo de vida. No anteponga más la facilidad de uso a la seguridad.

AVG se ha diseñado y desarrollado para proteger su actividad de uso de equipos informáticos y de conexión en red. Disfrute la experiencia de la protección completa de AVG.

# 2. Requisitos de instalación de AVG

## 2.1. Sistemas de operación compatibles

**Anti-Virus AVG 9 más Firewall** tiene como propósito proteger las estaciones de trabajo con los siguientes sistemas operativos:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 y x64, todas las ediciones)
- Windows 7 (x 86 y x64, todas las ediciones)

(y posiblemente Service Packs superiores para determinados sistemas operativos)

## 2.2. Requisitos mínimos y recomendados de hardware

Requisitos mínimos de hardware para **Anti-Virus AVG 9 más Firewall**:

- Equipo Intel Pentium de 1,5 GHz
- 512 MB de memoria RAM
- 390 MB de espacio libre en el disco duro (para la instalación)

Requisitos recomendados de hardware para **Anti-Virus AVG 9 más Firewall**:

- Equipo Intel Pentium de 1,8 GHz
- 512 MB de memoria RAM
- 510 MB de espacio libre en el disco duro (para la instalación)

# 3. Opciones de instalación de AVG

AVG se puede instalar desde el archivo de instalación que incorpora el CD de instalación, o puede descargar el archivo de instalación más reciente del sitio Web de AVG (http://www.avg.com/).

**Antes de comenzar a instalar AVG, le recomendamos que visite el sitio Web de AVG (http://www.avg.com/) para comprobar si existe algún archivo de instalación nuevo. Así, puede asegurarse de instalar la última versión disponible de Anti-Virus AVG 9 más Firewall.**

**Le recomendamos probar nuestra nueva herramienta Administrador de descargas de AVG, que le ayudará a configurar el archivo de instalación en el idioma correspondiente.**

Durante el proceso de instalación, se le solicitará su número de venta o número de licencia. Por favor, téngalo a mano antes de comenzar con la instalación. El número de venta se encuentra en el paquete del CD. Si ha adquirido su copia de AVG en línea, se le ha enviado el número de licencia por correo electrónico.

# 4. Administrador de descargas de AVG

**Administrador de descargas de AVG** es una herramienta sencilla que le permite seleccionar el archivo de instalación adecuado para la versión de prueba de su producto AVG. Basándose en la información que usted ha proporcionado, el administrador seleccionará el producto específico, el tipo de licencia, los componentes deseados y el idioma. Finalmente, **Administrador de descargas de AVG** procederá a descargar e iniciar el proceso de instalación adecuado.

***Advertencia:*** *tenga en cuenta que el Administrador de descargas de AVG no es adecuado para descargar las ediciones para redes y para SBS, y que sólo los siguientes sistemas operativos son compatibles: Windows 2000 (SP4 + SRP roll-up), Windows XP, Windows Vista y Windows 7.*

**Administrador de descargas de AVG** se puede descargar en el sitio Web de AVG ( http://www.avg.com/). A continuación encontrará una breve descripción de cada paso que necesita realizar dentro del **Administrador de descargas de AVG**:

## 4.1. Selección de idioma

En este primer paso de **Administrador de descargas de AVG** seleccione el idioma de instalación en el menú desplegable. Observe que la selección de idioma se aplica solamente al proceso de instalación; después de la instalación podrá cambiar el idioma directamente desde la configuración del programa. A continuación presione el botón

***Siguiente*** para continuar.

## 4.2. Verificación de conectividad

En el siguiente paso, **Administrador de descargas de AVG** intentará conectarse a Internet para poder localizar las actualizaciones. No podrá continuar con el proceso de descarga hasta que **Administrador de descargas de AVG** pueda completar la prueba de conectividad.

- Si la prueba muestra que no hay conectividad, asegúrese de estar realmente conectado a Internet. A continuación haga clic en el botón ***Reintentar***.

- Si utiliza una conexión Proxy a Internet, haga clic en el botón ***Configuración Proxy*** para especificar la información del Proxy:

- Si la comprobación ha sido exitosa, presione el botón ***Siguiente*** para continuar.

## 4.3. Configuración proxy

Si **Administrador de descargas de AVG** no fue capaz de identificar la configuración de proxy, debe especificarla de forma manual. Rellene la información siguiente:

- ***Servidor***: introduzca un nombre de servidor Proxy o dirección IP válidos.
- ***Puerto***: proporcione el número de puerto respectivo
- ***Utilizar autenticación Proxy***: si su servidor Proxy requiere autenticación, seleccione esta casilla.
- ***Seleccionar autenticación***: seleccione el tipo de autenticación del menú desplegable. Recomendamos ampliamente mantener el valor predeterminado (*el servidor Proxy enviará los requisitos de forma automática*). No obstante, si usted tiene experiencia en este campo, también puede seleccionar la opción Básica (*requerido por algunos servidores*) o NTLM (*requerido por todos los servidores ISA*). A continuación, introduzca un ***Nombre de usuario*** y ***Contraseña*** válidos (opcional).

Confirme la configuración presionando el botón ***Aplicar*** para continuar con el siguiente paso de **Administrador de descargas de AVG**.

## 4.4. Descargar archivos para instalar

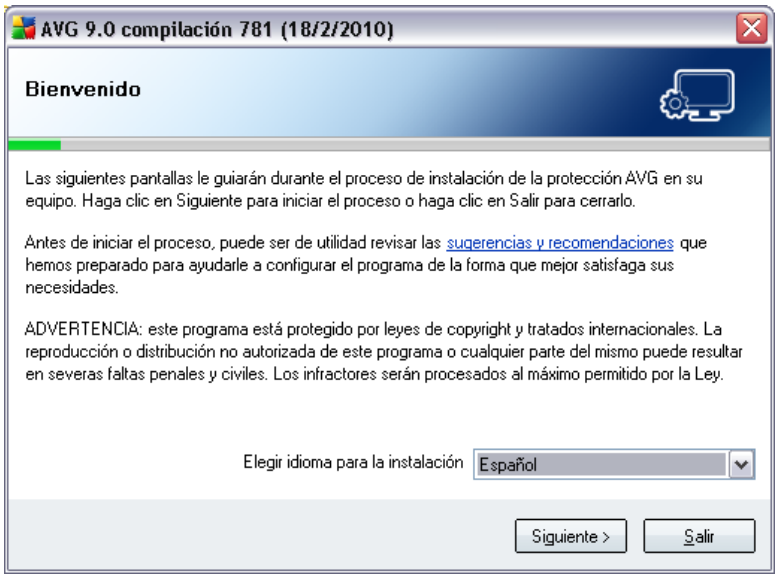
Ahora ha proporcionado toda la información necesaria para que **Administrador de descargas de AVG** inicie la descarga del paquete de instalación y el proceso de instalación. A continuación, avance hacia el proceso de instalación de AVG.

# 5. Proceso de instalación de AVG

Para instalar **Anti-Virus AVG 9 más Firewall** en su equipo debe obtener el archivo de instalación más reciente. Puede utilizar el CD de instalación que forma parte de su edición en caja, pero este archivo puede no estar actualizado. Por lo tanto, recomendamos obtener el archivo de instalación más reciente en línea. Puede descargar el archivo desde el sitio Web de AVG (http://www.avg.com/), en la sección ***Centro de soporte/Descarga***. O bien, puede utilizar nuestra nueva herramienta ***Administrador de descargas de AVG*** que le ayuda a crear y descargar el paquete de instalación que usted necesita e iniciar el proceso de instalación.

La instalación consta de una secuencia de ventanas de diálogo que contienen una breve descripción de lo que se debe hacer en cada paso. A continuación, ofrecemos una explicación para cada ventana de diálogo:

## 5.1. Ejecución de la instalación

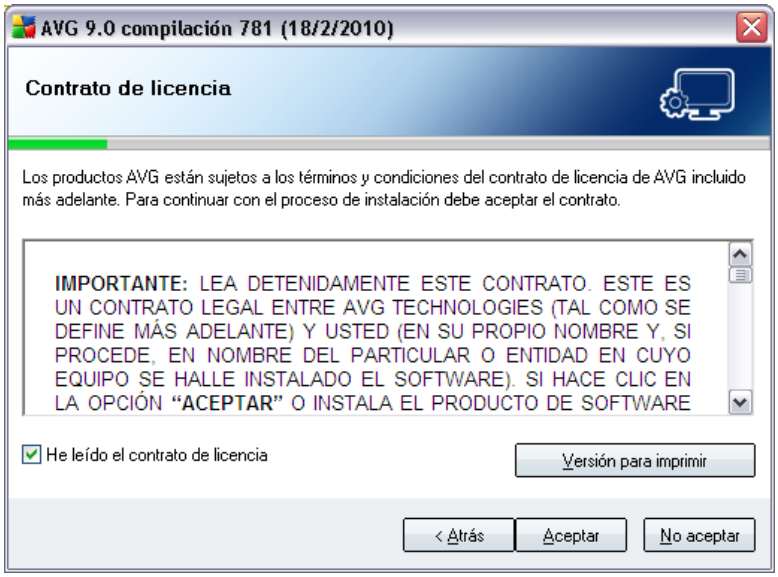



El proceso de instalación se inicia con la ventana ***Bienvenido al programa de instalación de AVG***. Aquí se selecciona el idioma empleado para el proceso de instalación. En la parte inferior de la ventana del diálogo, busque el elemento ***Elegir idioma para la instalación*** y seleccione el idioma deseado en el menú desplegable. A continuación, presione el botón ***Siguiente*** para confirmar la selección y pasar al diálogo siguiente.

***Atención:*** *Aquí se selecciona únicamente el idioma del proceso de instalación. No se selecciona el idioma de la aplicación AVG, que se puede especificar más adelante en el*

*proceso de instalación.*

## 5.2. Contrato de licencia



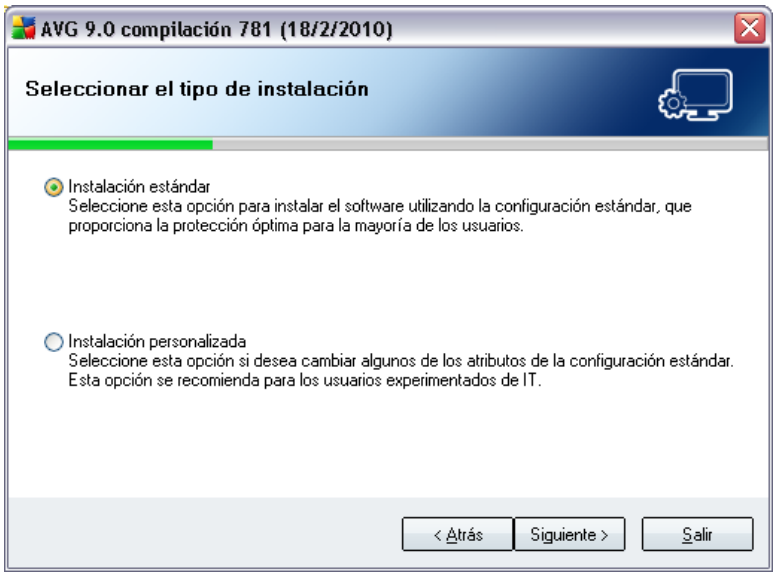

El cuadro de diálogo ***Contrato de licencia*** muestra íntegramente el contrato de licencia de AVG. Léalo detenidamente y confirme que lo ha leído y entendido. A continuación, acéptelo seleccionando la casilla de verificación ***He leído el contrato de licencia*** y presionando el botón ***Aceptar***.

Si no está conforme con el contrato de licencia, presione el botón ***No aceptar*** y el proceso de instalación se terminará de inmediato.

## 5.3. Verificando el estado del sistema

Una vez confirmado el contrato de licencia se le enviará al diálogo ***Verificando el estado del sistema*** . Este diálogo no requiere de ninguna intervención; su sistema se está verificando antes de que se pueda iniciar la instalación del AVG. Espere hasta que el proceso haya finalizado, después continúe automáticamente al siguiente diálogo.

## 5.4. Seleccionar el tipo de instalación




El diálogo ***Seleccionar el tipo de instalación*** ofrece dos opciones de instalación: ***estándar*** y ***personalizada.***

Para la mayoría de los usuarios, se recomienda mantener la ***instalación estándar*** que instala el programa AVG en modo totalmente automático con la configuración predefinida por el proveedor del programa. Esta configuración proporciona la máxima seguridad combinada con el uso óptimo de los recursos. En el futuro, si es necesario cambiar la configuración, siempre se puede hacer directamente en la aplicación AVG.

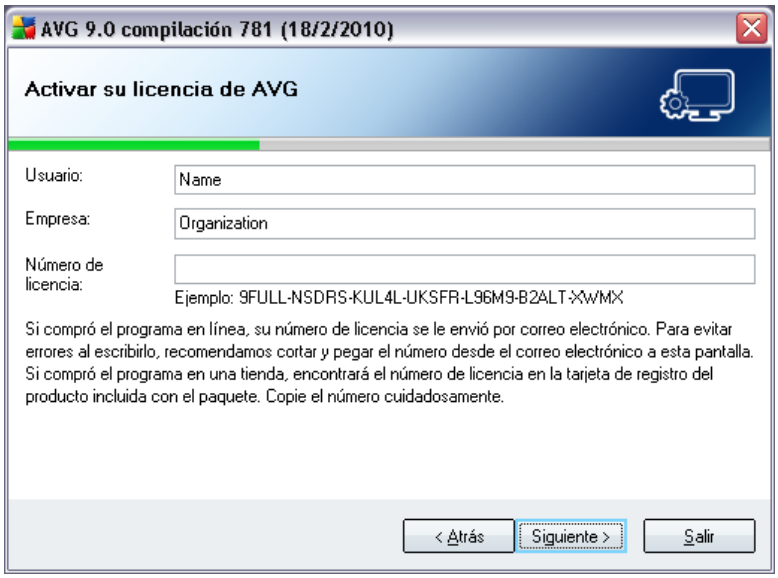
***La instalación personalizada*** sólo deben utilizarla los usuarios con experiencia que tienen un motivo importante para instalar AVG con una configuración distinta de la estándar (por ejemplo, para ajustarse a necesidades específicas del sistema).

## 5.5. Activar su licencia AVG

En el diálogo ***Activar su licencia AVG*** tiene que escribir sus datos de registro. Escriba su nombre (campo ***Nombre de usuario***) y el nombre de su organización (campo ***Nombre de empresa).***

Después, introduzca el número de licencia o número de venta en el campo de texto ***Número de licencia***. El número de venta se puede encontrar en el paquete del CD en la caja de **Anti-Virus AVG 9 más Firewall** . El número de licencia se encuentra en el correo electrónico de confirmación que recibió después de la compra en línea de **Anti-**

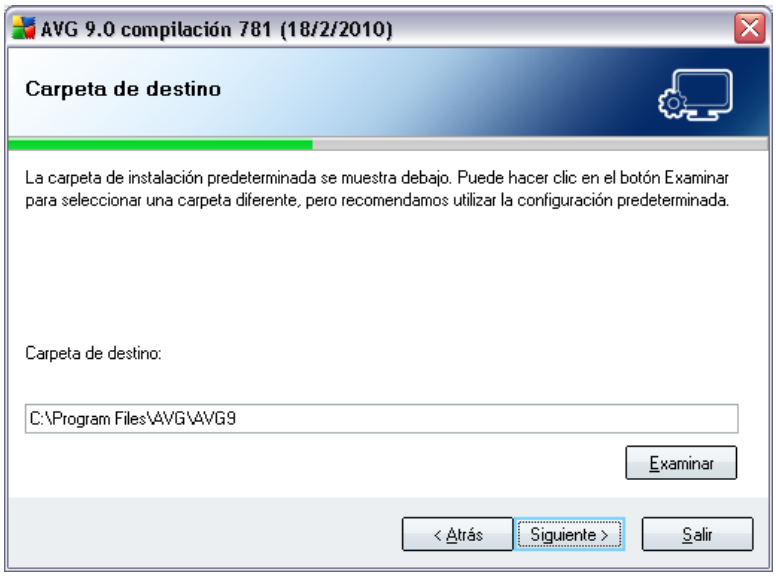
**Virus AVG 9 más Firewall**. Debe escribir el número exactamente como se muestra. Si está disponible el formulario digital del número de licencia (*en el correo electrónico*), se recomienda utilizar el método de copiar y pegar para insertarlo.




Presione el botón ***Siguiente*** para continuar con el proceso de instalación.

Si en el paso anterior ha seleccionado la instalación estándar, se le redirigirá directamente al cuadro de diálogo ***Barra de herramientas AVG Security***. Si seleccionó la instalación personalizada, continuará con el cuadro de diálogo ***Carpeta de destino***.

## 5.6. Instalación personalizada: carpeta de destino

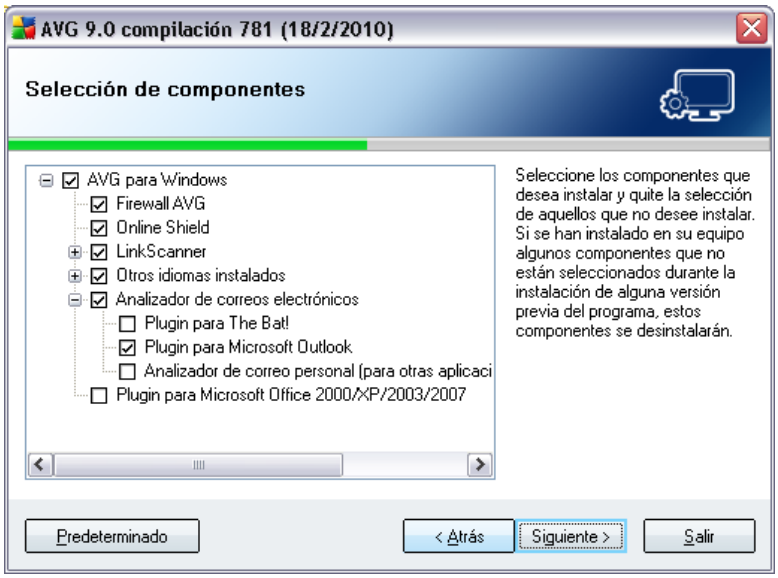



El cuadro de diálogo ***Carpeta de destino*** permite especificar la ubicación donde debe instalarse **Anti-Virus AVG 9 más Firewall**. De modo predeterminado, AVG se instalará en la carpeta de archivos de programa de la unidad C:. Si la carpeta no existe, un nuevo cuadro de diálogo le pedirá que confirme que está de acuerdo en que AVG cree esta carpeta en este momento.

Si desea cambiar esta ubicación, utilice el botón ***Examinar*** para ver la estructura de la unidad y seleccione la carpeta correspondiente.

Presione el botón ***Siguiente*** para confirmar la selección.

## 5.7. Instalación personalizada: selección del componente




El cuadro de diálogo ***Selección de componentes*** muestra una descripción general de todos los componentes de **Anti-Virus AVG 9 más Firewall** que pueden instalarse. Si la configuración predeterminada no se adecua a sus necesidades, puede quitar/agregar componentes específicos.

***Sin embargo, sólo puede seleccionar de entre los componentes incluidos en la edición del AVG que compró. Sólo se ofrecerá instalar estos componentes en el diálogo Selección de componentes.***

- ***Selección de idioma***

  Dentro de la lista de componentes a instalar, puede definir el idioma o idiomas en que se instalará AVG. Seleccione el elemento ***Otros idiomas instalados*** y, a continuación, elija los idiomas deseados del menú correspondiente.

- ***Complementos del analizador de correos electrónicos***

  Haga clic en el elemento ***Analizador de correos electrónicos*** para abrirlo y decidir los complementos a instalar para garantizar la seguridad de su correo electrónico. De forma predeterminada se instalará el ***Complemento para Microsoft Outlook***.Otra opción específica es el ***Complemento para The Bat!*** Si utiliza cualquier otro cliente de correo electrónico (*MS Exchange, Qualcomm Eurora, etc.*), seleccione la opción ***Analizador de correo electrónico personal*** para asegurar de forma automática la comunicación por correo electrónico, sin

importar el programa de correo electrónico que use.

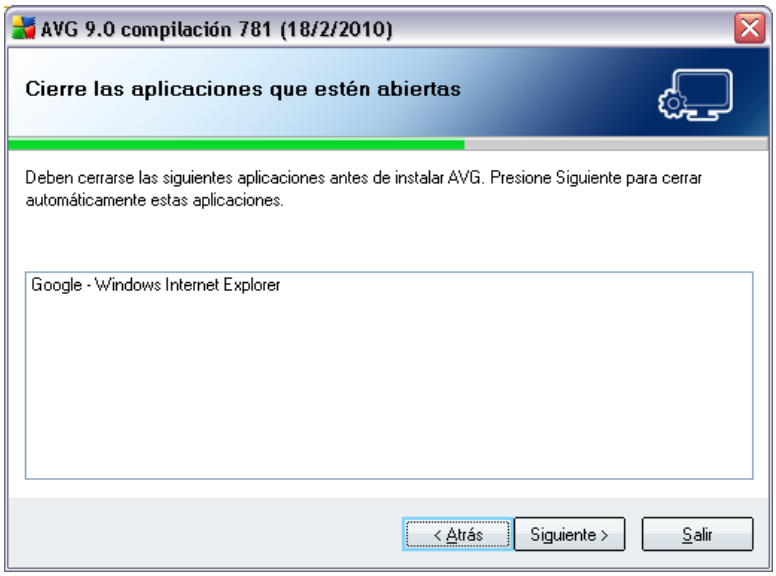
Para continuar, presione el botón ***Siguiente***.

## 5.8. Barra de herramientas AVG Security

En el cuadro de diálogo ***Barra de herramientas AVG Security***, decida si desea instalar la ***barra de herramientas AVG Security*** (*comprobación de resultados de la búsqueda de los motores de búsqueda en Internet compatibles*). Si no cambia la configuración predeterminada, este componente se instalará automáticamente en el navegador de Internet (*los navegadores compatibles actualmente son Microsoft Internet Explorer 6.0 o superior y Mozilla Firefox 2.0 o superior*) para proporcionarle una protección exhaustiva en línea mientras navega por la red.

Asimismo, puede decidir si desea utilizar Yahoo! como su proveedor de búsqueda predeterminado. Si lo desea, marque la casilla de verificación correspondiente.

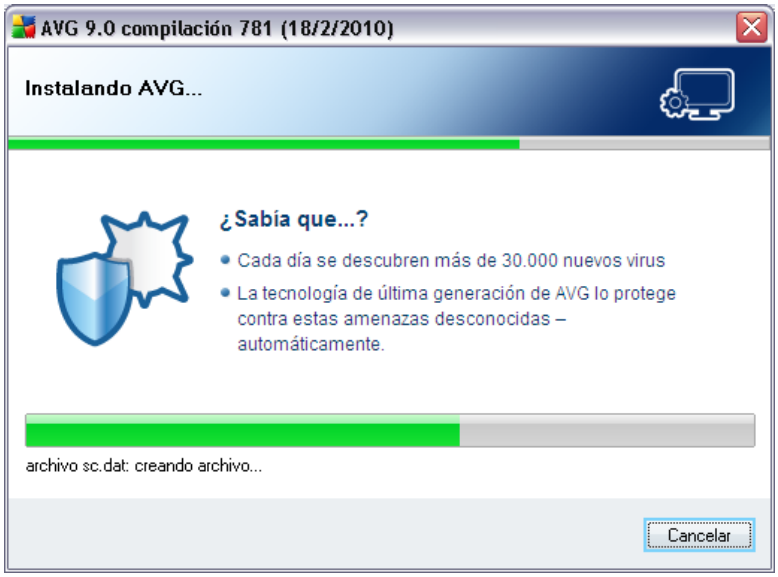
## 5.9. Cierre las aplicaciones que estén abiertas




El cuadro de diálogo ***Cierre las aplicaciones que estén abiertas*** sólo aparecerá durante el proceso de instalación si en su equipo se produjera un conflicto con otros programas en ejecución. A continuación, se proporcionará una lista con los programas que deben cerrarse para finalizar correctamente el proceso de instalación. Presione el botón ***Siguiente*** para confirmar que acepta cerrar las aplicaciones correspondientes y para continuar con el paso siguiente.

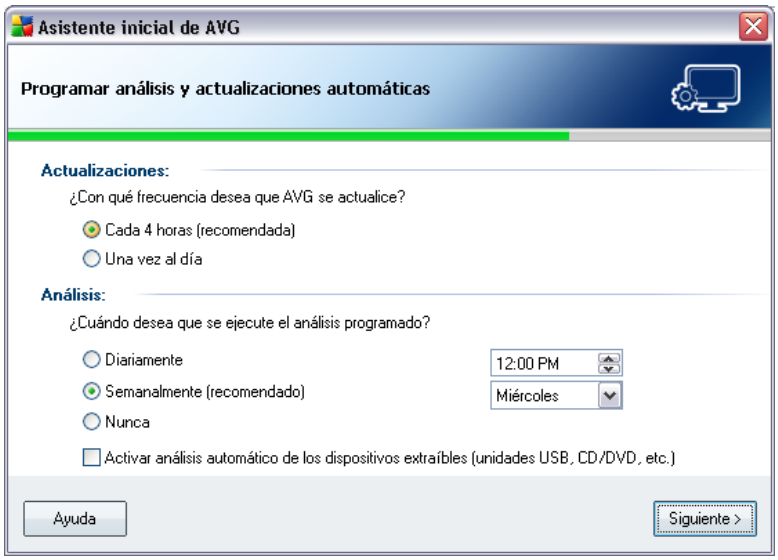
## 5.10. Instalación de AVG

El cuadro de diálogo ***Instalando AVG*** muestra el progreso del proceso de instalación y no precisa la intervención del usuario:




Después de finalizar el proceso de instalación, pasará al siguiente cuadro de diálogo automáticamente.

## 5.11. Programar análisis y actualizaciones automáticas




En el diálogo ***Programar análisis y actualizaciones automáticas*** configure el intervalo para comprobar la accesibilidad de los nuevos archivos de actualización, y defina la hora en que debe iniciarse el análisis programado. Se recomienda mantener los valores predeterminados. Presione el botón ***Siguiente*** para continuar.

## 5.12. Selección de uso de equipo

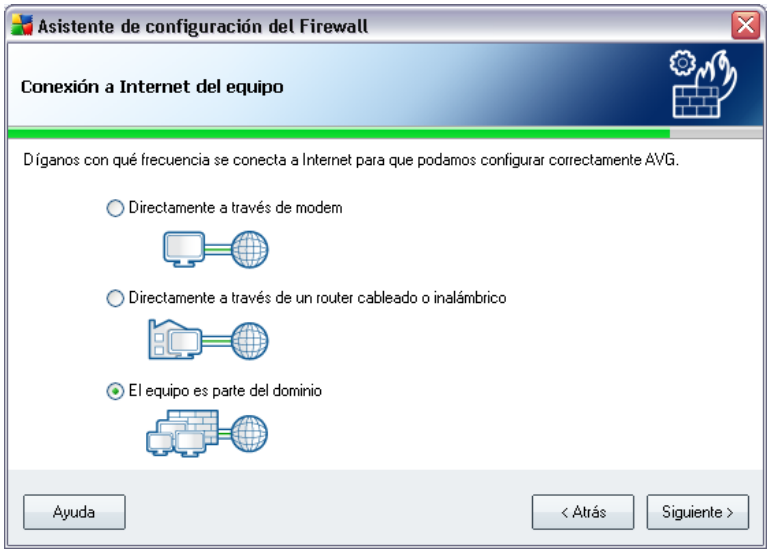
En este cuadro de diálogo, el ***Asistente de configuración del Firewall*** pregunta qué tipo de equipo utiliza. Por ejemplo, un equipo portátil, que se conecta a Internet desde varios lugares diferentes (*aeropuertos, habitaciones de hotel, etc.*) necesita reglas de seguridad más estrictas que las que requiere un equipo en un dominio (*red de empresa, etc.*). Según el tipo de uso del equipo seleccionado, se definirán las reglas predeterminadas del ***Firewall*** con diferente nivel de seguridad.

Puede elegir entre dos opciones alternativas:

- ***Un equipo de escritorio***
- ***Un equipo portátil***

Confirme la selección que hizo presionando el botón ***Siguiente*** y pase al siguiente cuadro de diálogo.

## 5.13. Conexión a Internet del equipo




En este cuadro de diálogo, el ***Asistente de configuración del Firewall*** le preguntará cómo está conectado su equipo a Internet. Según el tipo de conexión seleccionado, se definirán las reglas predeterminadas del ***Firewall*** con diferente nivel de seguridad.

Puede elegir entre tres opciones alternativas:

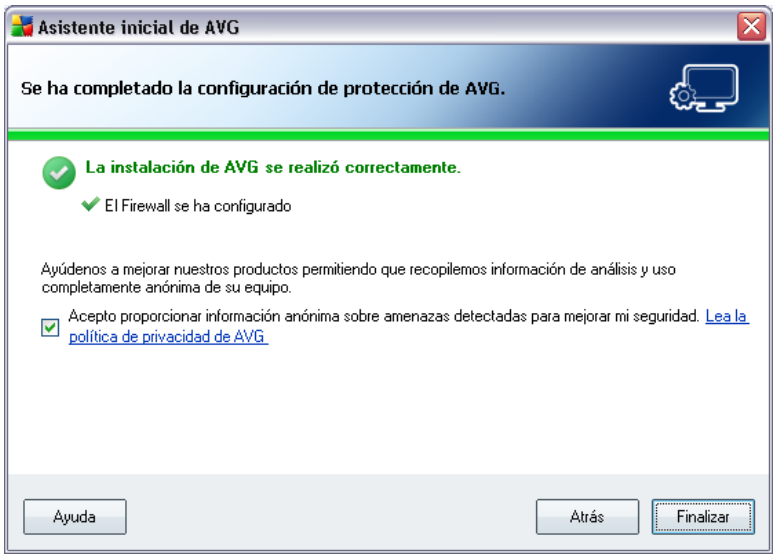
- ***Directamente a través de modem***

- ***Directamente a través de un router cableado o inalámbrico***
- ***El equipo es parte del dominio***

Seleccione el tipo de conexión que mejor describa su conexión a Internet.

Confirme la selección que hizo presionando el botón ***Siguiente*** y pase al siguiente cuadro de diálogo.

## 5.14. La configuración de la protección AVG ha finalizado




Se ha configurado su **Anti-Virus AVG 9 más Firewall**.

En este cuadro de diálogo decide si desea activar la opción de generación de reportes anónimos de sitios vulnerables y peligrosos para el laboratorio de virus de AVG. Si desea hacerlo, seleccione la opción ***Acepto proporcionar información ANÓNIMA sobre amenazas detectadas para mejorar mi seguridad***.

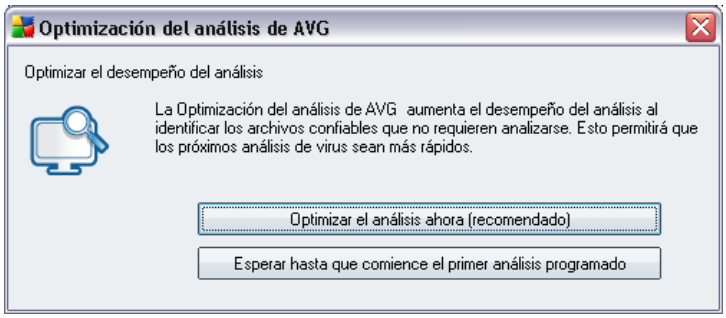
Finalmente, presione el botón ***Finalizar.*** Puede ser necesario reiniciar el equipo para que pueda empezar a trabajar con AVG.

# 6. Después de la instalación

## 6.1. Optimización del análisis

La optimización del análisis busca en las carpetas *Windows* y *Archivos de programa* donde detecta archivos adecuados (*por el momento son los archivos *.exe, *.dll y *.sys*) y guarda la información sobre estos archivos. En el próximo acceso no se volverán a analizar estos archivos, con lo que se reduce significativamente el tiempo de análisis.

Una vez finalizado el proceso de instalación, un nuevo cuadro de diálogo le invitará a optimizar el análisis:




Le recomendamos que utilice esta opción y ejecute el proceso de optimización del análisis presionando el botón ***Optimizar análisis ahora***.

## 6.2. Registro del producto

Al terminar la instalación de **Anti-Virus AVG 9 más Firewall**, registre su producto en línea en el sitio Web de AVG (http://www.avg.com/), en la página ***Registro*** (*siga las instrucciones indicadas directamente en la página*). Tras el registro, dispondrá de pleno acceso a la cuenta de usuario AVG, el boletín de actualizaciones de AVG y otros servicios que se ofrecen exclusivamente para los usuarios registrados.

## 6.3. Acceso a la interfaz de usuario

Se puede tener acceso a la ***Interfaz de usuario de AVG*** de varios modos:

- haga doble clic en el icono AVG de la bandeja del sistema
- haga doble clic en el icono AVG del escritorio

- desde el menú ***Inicio/Programas/AVG 9.0/Interfaz del usuario de AVG***

## 6.4. Análisis de todo el equipo

Existe el riesgo potencial de que un virus informático se transmitiera a su equipo antes de la instalación de **Anti-Virus AVG 9 más Firewall**. Por esta razón debe ejecutar un ***Análisis de todo el equipo*** para estar seguro de que no hay infecciones en su equipo.

Para obtener instrucciones sobre la ejecución de un ***Análisis de todo el equipo*** consulte el capítulo ***Análisis de AVG***.

## 6.5. Análisis Eicar

Para confirmar que **Anti-Virus AVG 9 más Firewall** se ha instalado correctamente, puede realizar el análisis EICAR.

El Análisis EICAR es un método estándar y absolutamente seguro que se utiliza para comprobar el funcionamiento de un sistema anti-virus. Es seguro emplearlo porque no se trata de un virus real y no incluye ningún fragmento de código viral. La mayoría de los productos reaccionan ante él como si fuera un virus (*aunque suelen notificarlo con un nombre obvio, tal como "EICAR-AV-Test" [análisis anti-virus EICAR]*). Puede descargar el virus EICAR del sitio web www.eicar.com. Allí también encontrará toda la información necesaria relacionada con el análisis EICAR.

Intente descargar el archivo ***eicar.com*** y guárdelo en el disco local. Inmediatamente después de que confirme que desea descargar el archivo de análisis, ***Online Shield*** reaccionará con una advertencia. Esta notificación demuestra que AVG se ha instalado correctamente en su equipo.

Desde el sitio Web http://www.eicar.com también puede descargar la versión comprimida del "virus" EICAR (*por ejemplo, con el formato eicar_com.zip*). ***Online Shield*** permite descargar este archivo y guardarlo en el disco local, pero ***Protección residente*** detectará el "virus" cuando intente descomprimirlo. **Si AVG no identifica el archivo de análisis EICAR como un virus, deberá verificar otra vez la configuración del programa.**

## 6.6. Configuración predeterminada de AVG

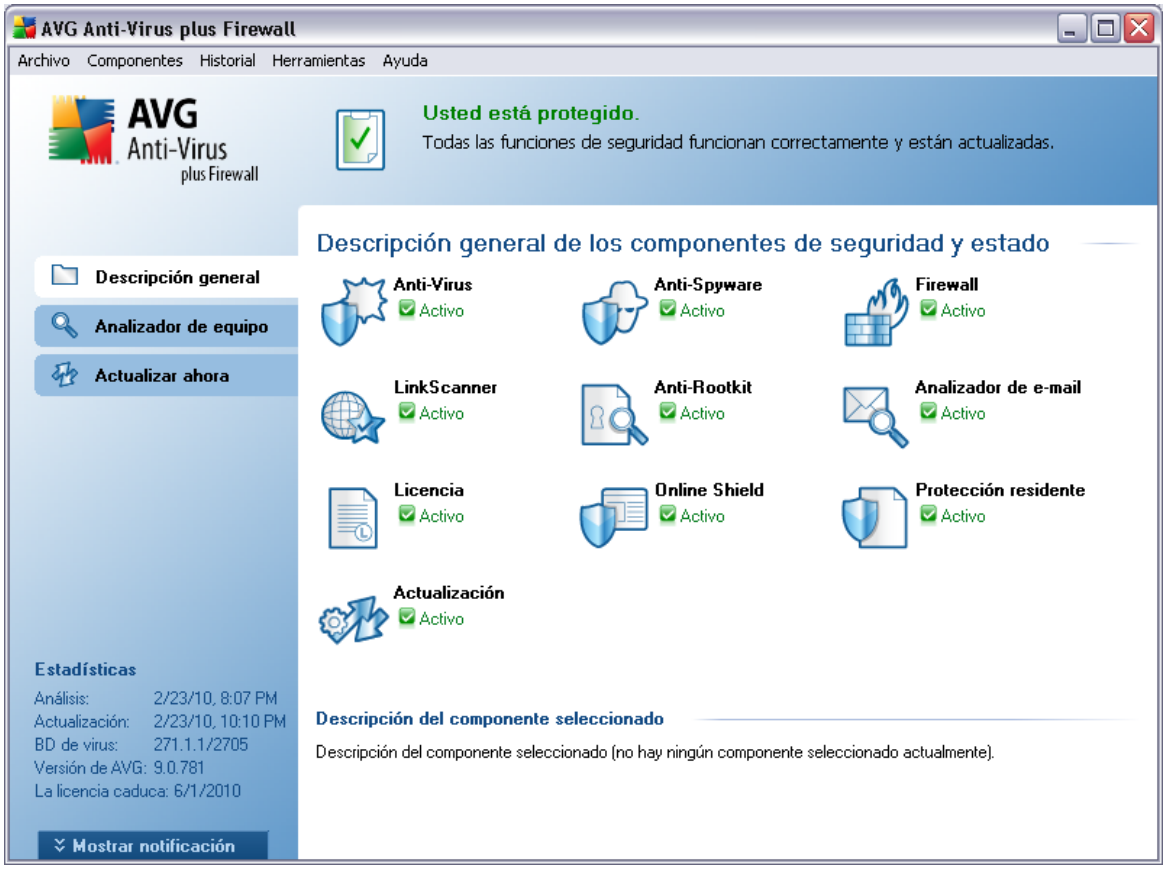
La configuración predeterminada (*es decir, la configuración de la aplicación inmediatamente después de la instalación*) de **Anti-Virus AVG 9 más Firewall** está definida por el proveedor de software para que todos los componentes y funciones proporcionen un rendimiento óptimo.

***No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración.***

Se puede efectuar alguna pequeña modificación de la configuración de los componentes de AVG directamente desde la interfaz de usuario del componente concreto. Si considera que debe cambiar la configuración de AVG para adaptarla mejor a sus necesidades, vaya a ***Configuración avanzada de AVG***, seleccione el elemento del menú del sistema ***Herramientas/Configuración avanzada*** y modifique la configuración de AVG en el diálogo ***Configuración avanzada de AVG*** que se abre.

# 7. Interfaz del usuario de AVG

**Anti-Virus AVG 9 más Firewall** se abre con la ventana principal:




La ventana principal se divide en varias secciones:

- ***Menú del sistema*** *(línea del sistema superior en la ventana)* es la navegación estándar que le permite tener acceso a todos los componentes, servicios y funciones de AVG - detalles >>

- ***Información del estado de seguridad*** *(sección superior de la ventana)* le proporciona información acerca del estado actual de su programa AVG - detalles >>

- ***Vínculos rápidos*** *(sección izquierda de la ventana)* le permite tener acceso rápidamente a las tareas de AVG más importantes y que se utilizan con mayor frecuencia - detalles >>

- ***Vista general de componentes*** *(sección central de la ventana* ofrece una descripción general de todos los componentes de AVG instalados - detalles >>

- ***Estadística*** *(sección inferior izquierda de la ventana)* le proporciona todos los datos estadísticos relacionados con la operación de los programas - detalles >>

- ***Icono de la bandeja del sistema*** *(esquina inferior derecha del monitor, en la bandeja del sistema)* indica el estado actual del AVG - detalles >>

## 7.1. Menú del sistema

El ***menú del sistema*** es el método de navegación estándar que se utiliza en todas las aplicaciones Windows. Está situado horizontalmente en la parte superior de la ventana principal de **Anti-Virus AVG 9 más Firewall**. Utilice el menú del sistema para acceder a componentes, funciones y servicios específicos de AVG.

El menú del sistema está dividido en cinco secciones principales:

### 7.1.1. Archivo

- ***Salir***: cierra la interfaz del usuario de **Anti-Virus AVG 9 más Firewall**. Sin embargo, la aplicación de AVG continuará funcionando en segundo plano y su equipo seguirá estando protegido.

### 7.1.2. Componentes

El elemento ***Componentes*** del menú del sistema incluye vínculos a todos los componentes AVG instalados, y abre su página de diálogo predeterminada en la interfaz de usuario:

- ***Vista general del sistema***: permite ir al diálogo predeterminado de la interfaz de usuario con la vista general de todos los componentes instalados y su estado.

- ***Anti-Virus***: abre la página predeterminada del componente ***Anti-Virus***.

- ***Anti-Rootkit***: abre la página predeterminada del componente ***Anti-Rootkit***.

- ***Anti-Spyware***: abre la página predeterminada del componente ***Anti-Spyware***.

- ***Firewall***: abre la página predeterminada del componente ***Firewall***.

- ***LinkScanner***: abre la página predeterminada del componente ***LinkScanner***.

- ***Analizador de correos electrónicos***: abre la página predeterminada del componente ***Analizador de correos electrónicos***.

- ***Licencia***: abre la página predeterminada del componente ***Licencia***.

- ***Online Shield***: abre la página predeterminada del componente ***Online Shield***.

- ***Protección residente***: abre la página predeterminada del componente ***Protección residente***.

- ***Administrador de actualizaciones***: abre la página predeterminada del componente ***Administrador de actualizaciones***.

### 7.1.3. Historial

- ***Resultados del análisis***: cambia a la interfaz de análisis de AVG, específicamente al diálogo de ***Descripción general de los resultados del análisis***

- ***Detección de protección residente***: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por la ***Protección residente***

- ***Detección del Analizador de correos electrónicos***: abre un cuadro de diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente ***Analizador de correos electrónicos***

- ***Hallazgos de Online Shield***: abre un cuadro de diálogo con una descripción general de las amenazas detectadas por ***Online Shield***

- ***Bóveda de Virus***: abre la interfaz del espacio de cuarentena (***Bóveda de Virus***) en el cual AVG elimina todas las infecciones detectadas que no pueden repararse automáticamente por alguna razón. Los archivos infectados se aíslan dentro de esta cuarentena, garantizando la seguridad de su equipo, y al mismo tiempo se guardan los archivos infectados para repararlos en el futuro si existe la posibilidad.

- ***Registro de historial de eventos***: abre la interfaz del registro de historial de todas las acciones **Anti-Virus AVG 9 más Firewall** registradas.

- ***Firewall***: abre la interfaz de configuración del Firewall en la pestaña ***Registros*** con una descripción general detallada de todas las acciones del Firewall.

### 7.1.4. Herramientas

- ***Analizar el equipo***: cambia a la interfaz de análisis de AVGy ejecuta un análisis del equipo completo

- ***Analizar la carpeta seleccionada***: cambia a la interfaz de análisis de AVGy permite definir qué archivos y carpetas se analizarán dentro de la estructura de árbol de su equipo

- ***Analizar archivo***: permite ejecutar un análisis bajo petición en un archivo seleccionado de la estructura de árbol de su disco

- ***Actualizar***: ejecuta automáticamente el proceso de actualización de **Anti-Virus AVG 9 más Firewall**

- ***Actualizar desde el directorio***: ejecuta el proceso de actualización desde los archivos de actualización ubicados en una carpeta específica en el disco local. Sin embargo, esta opción sólo se recomienda en casos de emergencia, por ejemplo, en situaciones en que no existe una conexión a Internet disponible *por ejemplo, su equipo se encuentra infectado y está desconectado de Internet, su equipo está conectado a una red sin acceso a Internet, etc.*). En la nueva ventana abierta, seleccione la carpeta donde guardó el archivo de actualización anteriormente, y ejecute el proceso de actualización.

- ***Configuración avanzada***: abre el cuadro de diálogo ***Configuración avanzada de AVG*** en el cual es posible editar la configuración de **Anti-Virus AVG 9 más Firewall**. Generalmente, se recomienda mantener la configuración predeterminada de la aplicación como se encuentra definida por el distribuidor del software.

- ***Configuración del Firewall***: abre un diálogo independiente para la configuración avanzada del componente ***Firewall***

### 7.1.5. Ayuda

- ***Contenido***: abre los archivos de ayuda AVG

- ***Obtener ayuda en línea***: abre el sitio Web de AVG (http://www.avg.com/) en la página del centro de soporte al cliente

- ***Su Web AVG***: abre el sitio Web de AVG (http://www.avg.com/)

- ***Acerca de virus y amenazas***: abre la ***Enciclopedia de virus*** en línea donde puede buscar información detallada acerca del virus identificado

- ***Reactivar***: abre el cuadro de diálogo ***Activar AVG*** con la información introducida en el cuadro de diálogo ***Personalizar AVG*** del proceso de instalación. Dentro de este cuadro de diálogo puede introducir el número de licencia para reemplazar el número de venta (*el número con el que instaló AVG*) o el número de licencia antiguo (*como al actualizar a un nuevo producto AVG*).

- ***Registrar ahora***: permite conectarse a la página de registro del sitio Web de AVG (http://www.avg.com/). Introduzca su información de registro; sólo los clientes con productos AVG registrados pueden recibir soporte técnico gratuito.

***Nota****: si utiliza la versión de prueba de* **Anti-Virus AVG 9 más Firewall***, los dos últimos elementos aparecen como* ***Compre ahora*** *y* ***Activar****, con lo que puede comprar la versión completa del programa inmediatamente. Para* **Anti-Virus AVG 9 más Firewall** *instalado con un número de venta, los elementos aparecen como* ***Registrar*** *y* ***Activar****. Para obtener más información, consulte la sección Licencia de esta documentación.*

- ***Acerca de AVG***: abre el cuadro de diálogo ***Información*** con cinco pestañas que proporcionan información acerca del nombre del programa, la versión del programa y la base de datos de virus, información del sistema, el contrato de licencia e información de contacto de ***AVG Technologies CZ***.

## 7.2. Información del estado de seguridad

La sección ***Información del estado de seguridad*** está situada en la parte superior de la ventana principal de AVG. En esta sección siempre encontrará información sobre el estado de seguridad actual de su **Anti-Virus AVG 9 más Firewall**. Consulte la descripción general de los iconos que posiblemente se muestran en esta sección, y su significado:

El icono verde indica que AVG funciona completamente. Su equipo está totalmente protegido, actualizado y todos los componentes instalados funcionan correctamente.

El icono naranja indica que uno o más componentes están configurados de manera incorrecta y debería prestar atención a su configuración/propiedades. No hay problemas críticos en AVG y probablemente ha optado por desactivar algunos componentes por alguna razón. Aún está protegido por AVG. Sin embargo, preste atención a la configuración de los componentes con problemas. Se podrá ver su nombre en la sección ***Información del estado de seguridad***

Este icono también aparece si por alguna razón ha decidido ignorar el estado de error de un componente (*la opción "Ignorar el estado del componente" está disponible desde el menú contextual haciendo clic con el botón secundario sobre el icono del componente respectivo en la descripción general del componente de la ventana principal de AVG*). Puede ser necesario utilizar esta opción en una situación específica, pero es muy recomendable desactivar la opción "***Ignorar el estado del componente***" a la mayor brevedad.

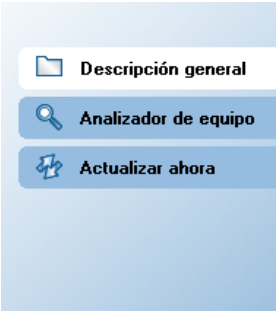
El icono rojo indica que AVG se encuentra en estado crítico  Uno o más componentes no funcionan correctamente y AVG no puede proteger su equipo. Preste atención de inmediato para corregir el problema notificado. Si no puede corregir el error sin ayuda, póngase en contacto con el equipo de soporte técnico de AVG.

Se recomienda encarecidamente que preste atención a la información del estado de seguridad y en caso de que el informe indique algún problema, siga adelante y trate de solucionarlo de inmediato.  Su equipo está en peligro.

***Nota:*** *la información de estado de AVG también se puede obtener en cualquier momento del icono de la bandeja del sistema.*

## 7.3. Vínculos rápidos

***Vínculos rápidos*** *(en la sección izquierda de la Interfaz del usuario de AVG)* que le permiten el acceso inmediato a las funciones más importantes y de uso más frecuente de AVG:




- ***Descripción general*** : utilice este vínculo para cambiar de cualquier interfaz de AVG abierta actualmente a la interfaz predeterminada con una descripción general de todos los componentes instalados (consulte el capítulo ***Descripción general de los componentes*** >>)

- ***Analizador del equipo***: utilice este vínculo para abrir la interfaz de análisis de AVG donde puede ejecutar los análisis directamente, programar los análisis o editar sus parámetros; consulte el capítulo ***Análisis de AVG >>***

- ***Actualizar ahora*** : este vínculo abre la interfaz de actualización, e inicia el proceso de actualización de AVG inmediatamente (consulte el capítulo ***Actualizaciones de AVG >>***)

Estos vínculos están disponibles desde la interfaz de usuario en todo momento. Una vez que emplea un vínculo rápido para ejecutar un proceso específico, la interfaz gráfica del usuario (GUI) cambiará a un nuevo diálogo pero los vínculos rápidos aún están disponibles. Más aún, el proceso de ejecución se ve más gráficamente.

## 7.4. Descripción general de los componentes

La sección ***Vista general de componentes*** se encuentra en la parte central de la Interfaz del usuario de AVG. La sección se divide en dos partes:

- Vista general de todos los componentes instalados con un panel que muestra el icono del componente y la información referida al estado activo o inactivo del componente en cuestión.

- Descripción de un componente seleccionado.

En **Anti-Virus AVG 9 más Firewall,** la sección ***Descripción general de los componentes*** contiene información sobre los siguientes componentes:

- ***Anti-Virus*** garantiza la protección del equipo frente a los virus que intenten introducirse en él. Detalles >>

- ***Anti-Spyware*** analiza las aplicaciones en segundo plano mientras se ejecutan. Detalles >>

- ***Firewall*** controla cómo el equipo intercambia datos con otros equipos en Internet o la red local. Detalles >>

- ***Link Scanner*** verifica los resultados de búsqueda visualizados en el navegador de Internet. Detalles >>

- ***Anti-Rootkit*** detecta los programas y las tecnologías que intentan camuflar malware. Detalles >>

- ***Analizador de correos electrónicos*** verifica todo el correo entrante y saliente para ver si contiene virus. Detalles >>

- ***Licencia*** muestra el número de licencia, el tipo de licencia y la fecha de vencimiento. Detalles >>

- ***Online Shield*** analiza todos los datos que descarga un navegador Web. Detalles >>

- ***Protección residente*** se ejecuta en segundo plano y analiza los archivos mientras éstos se copian, abren o guardan. Detalles >>

- ***Administrador de actualizaciones*** controla todas las actualizaciones de AVG . Detalles >>

Haga un solo clic en el icono de cualquier componente para resaltarlo en la vista general de componentes. Simultáneamente aparece una descripción de las funciones básicas del componente en la parte inferior de la interfaz de usuario. Haga doble clic en el icono para abrir la interfaz propia del componente con una lista de datos estadísticos básicos.

Haga clic con el botón secundario del ratón sobre el icono de un componente para expandir un menú de contexto: además al abrir la interfaz gráfica del componente también puede seleccionar ***Ignorar el estado del componente***. Seleccione esta opción para expresar que es consciente del estado de error del componente pero que por alguna razón desea conservar su AVG de esta manera y no desea que se le advierta mediante el icono en la bandeja de sistema.

## 7.5. Estadísticas

La sección ***Estadísticas*** se encuentra en la parte inferior izquierda de la Interfaz del usuario de AVG. Ofrece una lista de información acerca del funcionamiento del programa:

- ***Último análisis***: indica la fecha de realización del último análisis.

- ***Última actualización***: indica la fecha de ejecución de la última actualización.

- ***Base de datos de virus***: informa de la versión de la base de datos de virus instalada en este momento.

- ***Versión AVG***: informa de la versión instalada del programa AVG *(el número tiene el formato 9.0.xx, donde 9.0 es la versión de la línea de producto y xx es el número de compilación).*

- ***Caducidad de la licencia***: indica la fecha de caducidad de la licencia de AVG.

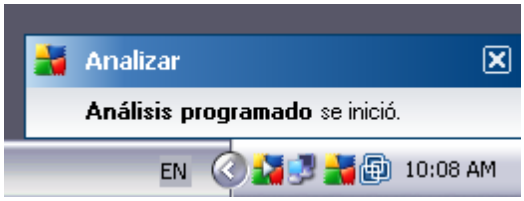
## 7.6. Icono en la bandeja de sistema

***Icono en la bandeja de sistema*** (*en la barra de tareas de Windows*) indica el estado actual de **Anti-Virus AVG 9 más Firewall**. Está visible en todo momento en la bandeja del sistema, tanto si la ventana principal de AVG está abierta como si está cerrada.

Si aparece a todo color , el ***icono de la bandeja del sistema*** indica que todos los componentes de AVG están activos y completamente operativos. También, el icono en la bandeja de sistema AVG se puede mostrar en color completo si AVG está en estado de error pero usted está totalmente conciente de esta situación y ha decidido de manera deliberada ***Ignorar el estado del componente***.

Un icono con un signo de exclamación  indica un problema (*componente inactivo, estado de error, etc.*). Haga doble clic en el ***icono de la bandeja del sistema*** para abrir la ventana principal y editar un componente.

El icono de la bandeja de sistema también informa sobre las actividades actuales de AVG y los cambios posibles de estado en el programa (*por ejemplo, inicio automático de un análisis o de una actualización programados, cambio de perfil del Firewall, cambio de estado de un componente, ocurrencia de estado de error, etc.*) mediante una ventana emergente que se abre desde el icono de la bandeja de sistema AVG:




El ***icono de la bandeja del sistema*** también se puede utilizar como vínculo rápido para obtener acceso a la ventana principal de AVG en cualquier momento haciendo doble clic en el icono. Al hacer clic con el botón secundario en el ***icono de la bandeja de sistema*** se abre un pequeño menú contextual con las opciones siguientes:

- ***Abrir interfaz del usuario de AVG***: haga clic para abrir la Interfaz del usuario de AVG.
- ***Actualizar***: ejecuta una actualización inmediata.

# 8. Componentes de AVG

## 8.1. Antivirus

### 8.1.1. Antivirus Principios de

El motor de análisis del software antivirus analiza todos los archivos y la actividad de archivos (abrir y cerrar archivos, etc.) en busca de virus conocidos. Se bloquearán los virus detectados para que no puedan realizar ninguna acción y después se limpiarán o pondrán en cuarentena. La mayoría del software antivirus también utiliza el análisis heurístico; en este análisis se analizan los archivos para detectar características típicas de los virus, denominadas firmas virales. Esto significa que el analizador de antivirus puede detectar un virus nuevo y desconocido si éste contiene algunas características típicas de los virus ya existentes.

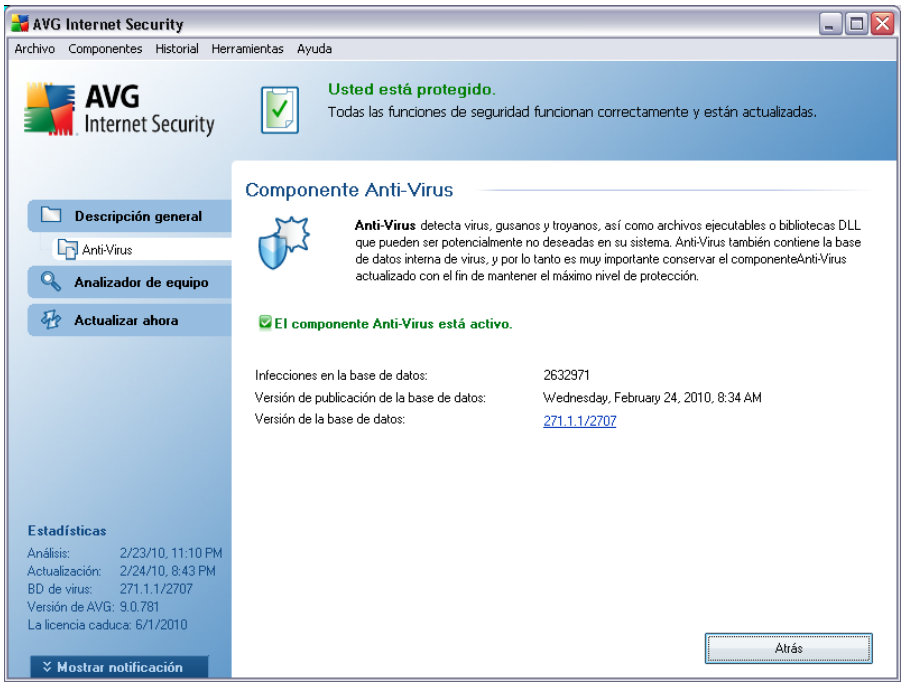
***La función esencial de la protección antivirus es que ningún virus conocido pueda ejecutarse en el equipo.***

Dado que hay casos en que una tecnología por si sola podría no llegar a detectar o identificar un virus, el ***Anti-Virus*** combina varias tecnologías para garantizar que su equipo esté protegido frente a los virus:

- Análisis: búsqueda de cadenas de caracteres que son características de un virus dado.
- Análisis heurístico: emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual.
- Detección genérica: detección de las instrucciones características de un virus o grupo de virus dado.

AVG también puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas dentro del sistema. Llamamos a estas amenazas programas potencialmente no deseados (diversos tipos de spyware, adware etc.). Además, AVG analiza el registro de su sistema para comprobar si posee entradas sospechosas, archivos temporales de Internet y cookies de rastreo, y le permite tratar todos esos elementos potencialmente dañinos de la misma manera que trata cualquier otra infección.

## 8.1.2. Interfaz de Antivirus




La interfaz del componente ***Anti-Virus*** proporciona alguna información básica sobre el funcionamiento del componente, información sobre su estado actual (*el componente Anti-Virus está activo.*), y una breve descripción general de las estadísticas del ***Anti-Virus*** :

- ***Definiciones de virus***: número que proporciona el recuento de los virus definidos en la versión actualizada de la base de datos de virus
- ***Última actualización de la base de datos*** : especifica cuándo y en qué momento se actualizó por última vez la base de datos de virus.
- ***Versión de la base de datos*** : define el número de la última versión de la base de datos de virus; y este número aumenta con cada actualización de la base de datos de virus

Sólo hay un botón de operación dentro de la interfaz de este componente, ***Atrás***: presione el botón para regresar a la interfaz del usuario de AVG predeterminada (descripción general de los componentes).

***Observe que:*** *El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de*

*AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración de AVG, seleccione el elemento del menú del sistema**Herramientas/ Configuración avanzada** y edite la configuración de AVG en el diálogoConfiguración avanzada de AVG abierto recientemente.*

## 8.2. Anti-Spyware

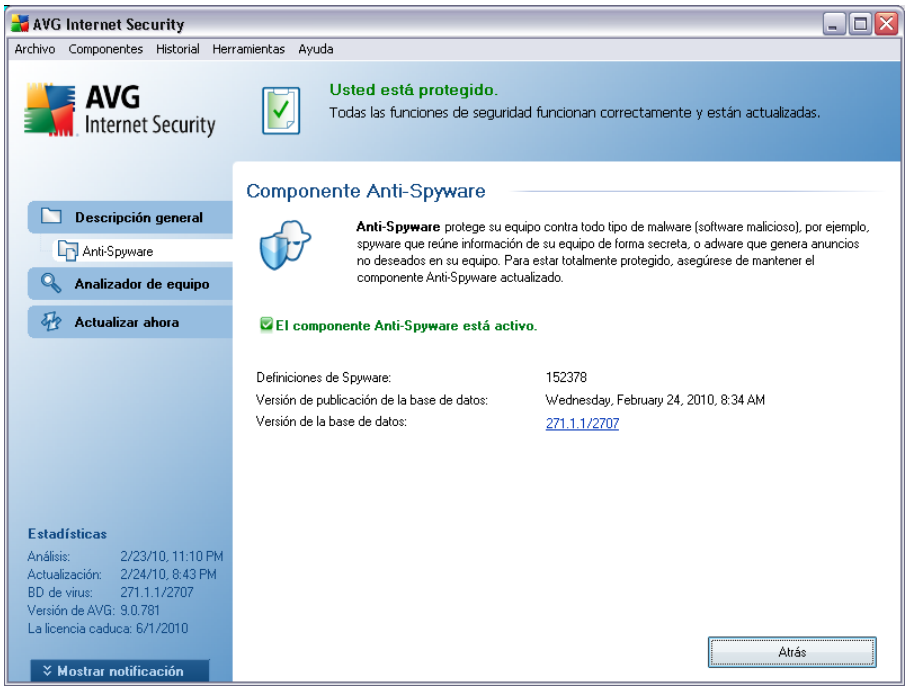
### 8.2.1. Anti-Spyware Principios de

El spyware generalmente se define como un tipo de malware, esto es, un software que recoge información del equipo del usuario sin el conocimiento ni el consentimiento del usuario. Algunas aplicaciones de spyware también pueden instalarse intencionalmente y, con frecuencia, incluyen algunos avisos, ventanas emergentes o diferentes tipos de software desagradable.

Actualmente, el origen más común de la infección suele estar en los sitios web con contenido potencialmente peligroso. Hay otros métodos de transmisión; por ejemplo, a través del correo electrónico infectado con gusanos y virus, lo que también es frecuente. La protección más importante que se debe utilizar es un analizador que se ejecute permanentemente en segundo plano, ***Anti-Spyware***, que actúe como protección residente y analice las aplicaciones en segundo plano mientras el usuario las ejecuta.

También existe el riesgo de que se haya transmitido malware a su equipo antes de que AVG estuviera instalado, o de que usted no haya mantenido su **Anti-Virus AVG 9 más Firewall** actualizado con las últimas actualizaciones de la base de datos y del programa. Por ello, AVG le permite analizar su equipo en busca de malware/spyware por medio de la función de análisis. También detecta malware inactivo y no peligroso, esto es, malware que se ha descargado pero que no se ha activado aún.

## 8.2.2. Interfaz de Anti-Spyware




La interfaz del componente ***Anti-Spyware*** proporciona una breve descripción general sobre el funcionamiento del componente, información sobre su estado actual (*el componente Anti-Spyware está activo.*), y algunos datos estadísticos del ***Anti-Spyware*** :

- ***Definiciones de Spyware***: número que proporciona el recuento de muestras de spyware definido en la última versión de la base de datos de spyware
- ***Última actualización de la base de datos*** : especifica cuándo y en qué momento se actualizó la base de datos de spyware
- ***Versión de la base de datos*** : define el número de la última versión de la base de datos de spyware; y este número aumenta con cada actualización de la base de virus

Sólo hay un botón de operación dentro de la interfaz de este componente, ***Atrás***: presione el botón para regresar a la interfaz del usuario de AVG predeterminada (descripción general de los componentes).

***Observe que:*** El *proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de*

*AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración de AVG, seleccione el elemento del menú del sistema**Herramientas/ Configuración avanzada** y edite la configuración de AVG en el diálogoConfiguración avanzada de AVG abierto recientemente.*

## 8.3. Anti-Rootkit

Un rootkit es un programa diseñado para tomar el control fundamental de un sistema informático, sin la autorización de los propietarios ni de los administradores legítimos del sistema. Raramente se precisa acceso al hardware, ya que un rootkit está pensado para tomar el control del sistema operativo que se ejecuta en el hardware. Normalmente, los rootkits ocultan su presencia en el sistema mediante la subversión o evasión de los mecanismos de seguridad estándar del sistema operativo. A menudo, también son troyanos, con lo que engañan a los usuarios y les hacen creer que son seguros de ejecutar en los sistemas. Las técnicas empleadas para lograrlo pueden consistir en ocultar los procesos en ejecución a los programas de supervisión o esconder archivos o datos del sistema al sistema operativo.

## 8.4. Firewall

Un firewall es un sistema que aplica una política de control de acceso entre dos o más redes bloqueando o permitiendo el tráfico. Cada firewall contiene un conjunto de reglas que protege la red interna de ataques que se originan desde fuera (generalmente desde Internet) y controla toda comunicación en cada puerto de red. La comunicación se evalúa según las reglas definidas y, así, se permite o prohíbe. Si el firewall reconoce cualquier intento de intrusión, "bloquea" el intento y no permite el acceso al equipo.

El Firewall está configurado para permitir o denegar la comunicación interna o externa (bidireccional, de entrada o de salida) mediante puertos definidos y para aplicaciones de software definidas. Por ejemplo, el firewall puede configurarse para permitir que la información Web entrante y saliente fluya únicamente mediante Microsoft Explorer. Cualquier intento de transmitir información Web mediante otro navegador sería bloqueado.

El Firewall protege su información personal para que no se envíe desde su equipo sin su autorización. Controla de qué manera su equipo intercambia datos con otros equipos a través de Internet o una red local. Dentro de una organización, el Firewall también protege al equipo de posibles ataques iniciados por usuarios internos desde otros equipos de la red.

***Recomendación:** normalmente no se recomienda usar más de un firewall en un solo equipo. El equipo no será más seguro si se instalan más firewalls. Es más probable que se produzcan algunos conflictos entre estas dos aplicaciones. Por lo tanto le*

*recomendamos que sólo utilice un firewall en su equipo y desactive los demás; así se elimina el riesgo de posibles conflictos y cualquier problema relacionado con esto.*

### 8.4.1. Principios de Firewall

En AVG, el componente ***Firewall*** verifica todo el tráfico en cada puerto de red de su equipo. El ***Firewall***, de acuerdo con las reglas definidas, evalúa las aplicaciones que están ejecutándose en el equipo (y desean conectarse a Internet o a una red local) o las que abordan su equipo desde el exterior para intentar conectarse a su PC. Para cada una de estas aplicaciones, el ***Firewall*** permite o prohíbe la comunicación en los puertos de red. De forma predeterminada, si la aplicación es desconocida (es decir, no tiene reglas de ***Firewall*** definidas), el ***Firewall*** le preguntará si desea permitir o bloquear el intento de comunicación.

***Nota:*** *el Firewall AVG no está diseñado para plataformas de servidor.*

**El Firewall AVG puede:**

- Permitir o bloquear intentos de comunicación de aplicaciones conocidas de forma automática, o solicitarle una confirmación.
- Utilizar perfiles completos con reglas predefinidas, de acuerdo con sus necesidades
- Cambiar el perfil de forma automática al conectarse a diferentes redes, o utilizar diferentes adaptadores de red

### 8.4.2. Perfiles del Firewall

El Firewall le permite definir reglas de seguridad específicas basándose en si su equipo se ubica en un dominio o es un equipo independiente, o incluso portátil. *** Cada una de estas opciones exige un nivel de protección diferente y los niveles están cubiertos por los perfiles correspondientes. En resumen, un perfil de ***Firewall*** es una configuración específica del componente ***Firewall*** y es posible utilizar varias configuraciones predefinidas.

**Perfiles disponibles**

- ***Permitir todo***: un perfil de sistema de ***Firewall*** que ha preestablecido el fabricante y siempre se encuentra presente. Al activar este perfil, se permite toda la comunicación a través de la red y no se aplican reglas de políticas de seguridad, como si la protección del ***Firewall*** estuviera desactivada *(todas las*

*aplicaciones se permiten, pero los paquetes continúan siendo analizados; para desactivar por completo cualquier filtrado necesita deshabilitar el Firewall)*. El perfil de sistema no puede duplicarse, eliminarse, y su configuración no puede ser cambiada.

- ***Bloquear todo***: un perfil de sistema de ***Firewall*** que ha preestablecido el fabricante y siempre se encuentra presente. Cuando este perfil está activado, se bloquea toda la comunicación de red, y el equipo no estará disponible para las redes externas y tampoco podrá comunicarse con ellas. El perfil de sistema no puede duplicarse, eliminarse, y su configuración no puede ser cambiada.

- ***Perfiles personalizados***:

  - ***Conectado directamente a Internet***: adecuado para equipos domésticos de escritorio comunes conectados directamente a Internet o equipos portátiles que se conectan a Internet fuera de la red segura de la compañía. Seleccione esta opción si se conecta desde casa o se encuentra en la red de una empresa pequeña sin control central. Asimismo, seleccione esta opción si va a viajar y se va a conectar mediante un equipo portátil desde diferentes lugares desconocidos y posiblemente peligrosos (*cafés Internet, habitaciones de hotel, etc.*). Se crearán reglas más restrictivas, ya que se supone que estos equipos no tienen protección adicional y, por lo tanto, necesitan la protección máxima.

  - ***Computadora en un dominio***: adecuada para los equipos dentro de una red local, por ejemplo, corporativa o escolar. Se asume que la red está protegida por algunas medidas adicionales, por lo que el nivel de seguridad puede ser menor que para una computadora independiente.

  - ***Red de casa o pequeña oficina***: adecuada para equipos en redes pequeñas, por ejemplo, en casa o en una oficina pequeña, que funcionan sólo como varios equipos conectados entre sí, sin un administrador central.

## Cambio de perfiles

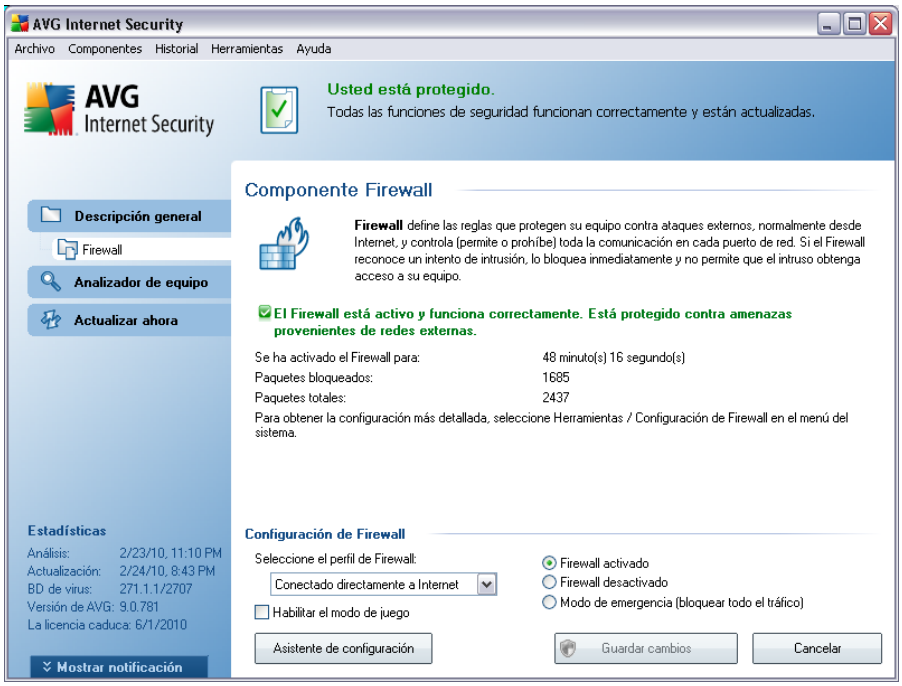
La función de cambio de perfil permite al ***Firewall*** cambiar automáticamente al perfil definido al utilizar un adaptador de red determinado o al conectarse a un cierto tipo de red. Si aún no se ha asignado un perfil al área de red, hasta la siguiente conexión a esa área, el ***Firewall*** mostrará un diálogo que solicitará asignar un perfil.

Puede asignar los perfiles a todas las áreas o interfaces de redes locales y especificar

la configuración más detalladamente en el cuadro de diálogo ***Perfiles de áreas y adaptadores***, donde también puede desactivar la característica si no desea utilizarla ( *posteriormente, para cualquier tipo de conexión, se utilizará el perfil predeterminado*).

Generalmente, los usuarios que tienen un equipo portátil y utilizan varios tipos de conexión encontrarán que esta característica es útil. Si tiene un equipo de escritorio y sólo utiliza un tipo de conexión(*por ejemplo, conexión por cable a Internet*), no necesita preocuparse por el cambio de perfiles, ya que prácticamente no lo utilizará.

## 8.4.3. Interfaz de Firewall




La interfaz del componente ***Firewall*** proporciona información básica acerca de la funcionalidad del componente junto con una breve descripción general de las estadísticas del ***Firewall***:

- ***El Firewall ha estado activado durante***: tiempo transcurrido desde que se inició el Firewall por última vez
- ***Paquetes bloqueados***: número de paquetes bloqueados de la cantidad total de paquetes analizados
- ***Paquetes totales***: número de todos los paquetes analizados durante la ejecución del Firewall

## Configuración básica del componente

- ***Seleccionar el perfil de Firewall***: en el menú desplegable, seleccione uno de los perfiles definidos: existen dos perfiles disponibles en todo momento (los *perfiles predeterminados llamados* ***Permitir todo*** *y* ***Bloquear todo***); otros perfiles se agregaron manualmente mediante la edición de perfiles en el cuadro de diálogo ***Perfiles*** en ***Configuración del Firewall***.

- ***Habilitar el modo de juego***: marque esta opción para asegurarse de que al ejecutar aplicaciones de pantalla completa (juegos, presentaciones de PowerPoint, etc.), el ***Firewall*** no mostrará cuadros de diálogo de confirmación para permitir o bloquear la comunicación para las aplicaciones desconocidas. Si en ese momento una aplicación desconocida intenta comunicarse mediante la red, el ***Firewall*** permitirá o bloqueará automáticamente el intento de acuerdo a la configuración que existe en el perfil actual.

- ***Estado del Firewall***:

  - ***Firewall activado***: seleccione esta opción para permitir la comunicación con aquellas aplicaciones que tienen la asignación de 'permitido' en el conjunto de reglas definido dentro del perfil de ***Firewall*** seleccionado

  - ***Firewall desactivado***: esta opción desactiva el ***Firewall*** por completo, se permite todo el tráfico pero no se analiza

  - ***Modo de emergencia (bloquear todo el tráfico de Internet)***: seleccione esta opción para bloquear todo el tráfico en todos los puertos de red; el ***Firewall*** está aún en ejecución pero se detiene todo el tráfico de red

***Observe que:*** *El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración del Firewall, seleccione el elemento del menú del sistema* ***Herramientas/Configuración del Firewall*** *y edite la configuración del Firewall en el cuadro de diálogo que se acaba de abrir****Configuración del Firewall****.*

## Botones de control

- ***Asistente de configuración***: presione este botón para cambiar al cuadro de diálogo correspondiente (*utilizado dentro del proceso de instalación*)

denominado ***Selección de uso de equipo***, donde puede especificar la configuración del componente ***Firewall***

- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este diálogo.

- ***Cancelar***: presione este botón para volver a la interfaz del usuario de AVG predeterminada (*vista general de componentes*)

## 8.5. Analizador de correos electrónicos

Una de las fuentes más comunes de virus y troyanos es a través de correo electrónico. El phishing (suplantación de identidad) y el spam hacen del correo electrónico una fuente aún mayor de riesgos. Las cuentas de correo electrónico gratuitas aumentan la probabilidad de recibir esos correos maliciosos (*ya que es muy raro que empleen tecnología anti-spam*), y los usuarios domésticos confían demasiado en tales correos. Asimismo, al navegar por sitios desconocidos y rellenar formularios en línea con datos personales (*como la dirección de correo electrónico*), los usuarios domésticos están más expuestos a ataques a través del correo electrónico. Las compañías normalmente utilizan cuentas de correo electrónico corporativas y emplean filtros anti-spam, etc, para reducir el riesgo.

### 8.5.1. Principios del analizador de correos electrónicos

El componente ***Analizador de correos electrónicos*** analiza automáticamente los correos electrónicos entrantes/salientes. Puede utilizarlo con los clientes de correo electrónico que no cuentan con su propio complemento en AVG (*por ejemplo, Outlook Express, Mozilla, Incredimail, etc.*).

Durante la instalación de AVG hay dos servidores automáticos de AVG creados para controlar el correo electrónico: uno para comprobar los correos electrónicos entrantes y el otro para comprobar los correos electrónicos salientes. Utilizando estos dos servidores, los correos electrónicos se analizan automáticamente en los puertos 110 y 25 (*puertos estándar para enviar o recibir correo electrónico*).

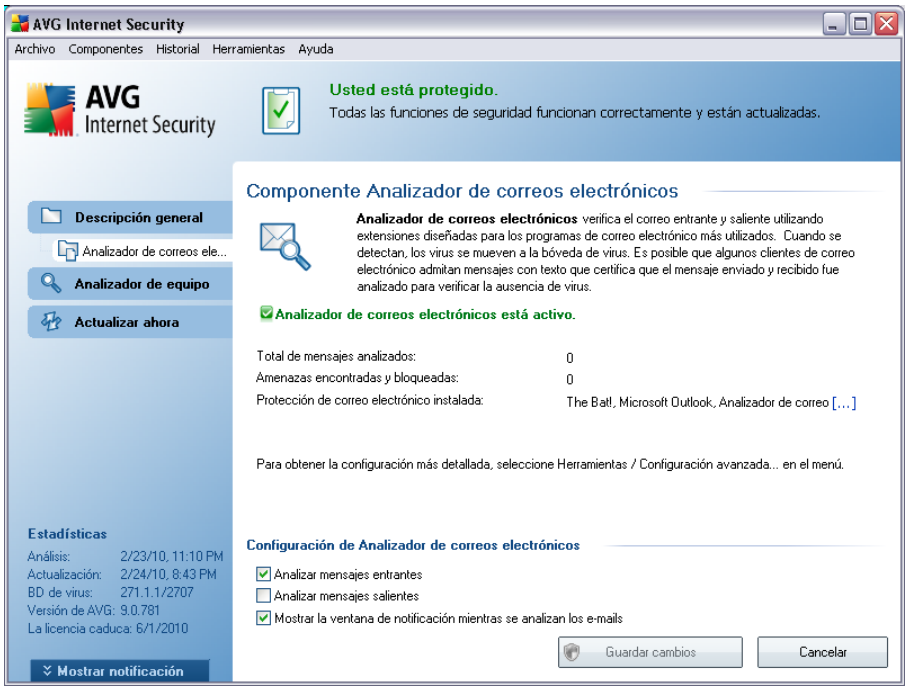
***El Analizador de correos electrónicos*** funciona como una interfaz entre el cliente de correo electrónico y los servidores de correo electrónico en Internet.

- ***Correo entrante:*** al recibir un mensaje del servidor, el componente ***Analizador de correos electrónicos*** lo analiza en busca de virus, elimina los archivos adjuntos infectados y agrega una certificación. Si se detectan virus, éstos se pondrán en cuarentena en la ***Bóveda de virus*** de forma inmediata. Después pasa el mensaje al cliente de correo.

- ***Correo saliente:*** el mensaje se envía desde el cliente de correo electrónico al Analizador de correos electrónicos, el cual analiza el mensaje y los archivos adjuntos en busca de virus y después envía el mensaje al servidor SMTP (*el análisis de los correos electrónicos salientes está desactivado de forma predeterminada y se puede configurar manualmente*).

***Nota:*** *el analizador de correos electrónicos AVG no está diseñado para plataformas de servidor.*

## 8.5.2. Interfaz del analizador de correos electrónicos




En el diálogo del componente ***Analizador de correos electrónicos*** puede encontrar un breve texto con una descripción de las funciones del componente, información sobre su estado actual (El *Analizador de correos electrónicos está activo.*) y las estadísticas siguientes:

- ***Número total de mensajes de correo electrónico analizados***: indica cuántos mensajes de correo electrónico se han analizado desde la última ejecución del ***Analizador de correos electrónicos*** (*si es necesario, este valor puede ser restablecido, por ejemplo, por cuestiones estadísticas: Restablecer valor*)

- ***Amenazas encontradas y bloqueadas***: indica el número de infecciones

detectadas en mensajes de correo electrónico desde la última ejecución del ***Analizador de correos electrónicos***.

- ***Protección de correos electrónicos instalada***: información acerca de algún complemento para protección del correo electrónico instalado, específico para su cliente de correo instalado.

## Configuración básica del componente

En la parte inferior del diálogo puede encontrar la sección denominada ***Configuración del Analizador de correos electrónicos*** donde puede editar algunas funciones básicas del componente:

- ***Analizar mensajes entrantes***: seleccione este elemento para especificar que todos los correos electrónicos entregados en la cuenta deben analizarse en busca de virus. De manera predeterminada, este elemento está activado, y se recomienda no cambiar esta configuración.

- ***Analizar mensajes salientes***: seleccione este elemento para confirmar que se deben analizar en busca de virus todos los correos enviados desde la cuenta. De forma predeterminada, este elemento se encuentra desactivado.

- ***Mostrar icono de notificación cuando se estén analizando correos electrónicos***: marque este elemento para confirmar que desea utilizar el cuadro de diálogo de notificación que aparece sobre el icono de AVG en la bandeja del sistema durante el análisis del correo con el componente ***Analizador de correos electrónicos***. De manera predeterminada, este elemento está activado, y se recomienda no cambiar esta configuración.

Se puede obtener acceso a la configuración avanzada del componente ***Analizador de correos electrónicos*** mediante el elemento ***Herramientas/Configuración avanzada*** del menú del sistema; no obstante, la configuración avanzada sólo está recomendada para los usuarios con experiencia.

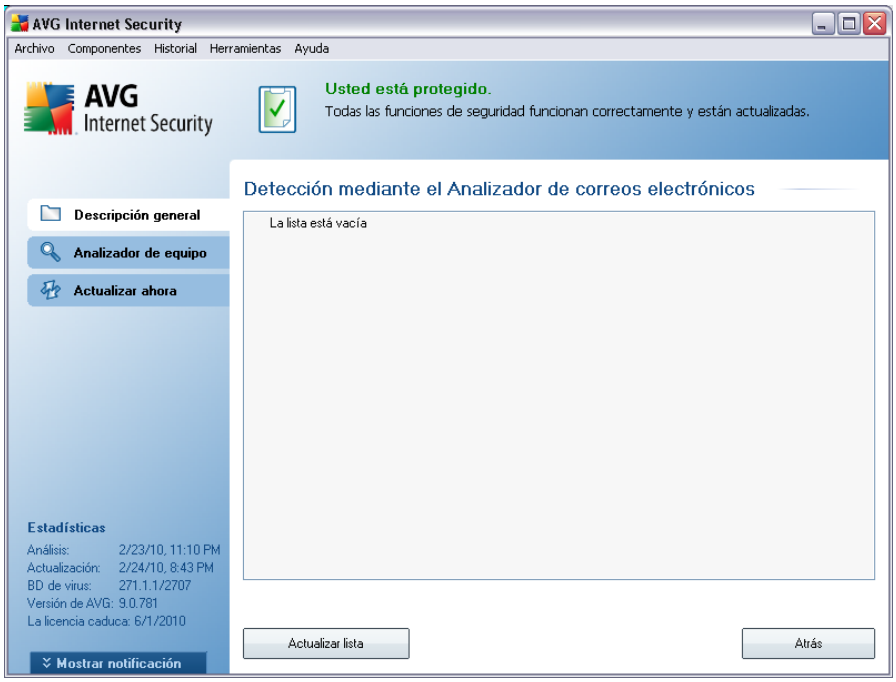
***Observe que:*** *El proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración de AVG, seleccione el elemento del menú del sistema****Herramientas/ Configuración avanzada*** *y edite la configuración de AVG en el diálogo*Configuración avanzada de AVG *abierto recientemente.*

## Botones de control

Los botones de control disponibles en la interfaz del ***Analizador de correos electrónicos*** son:

- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este diálogo.
- ***Cancelar***: presione este botón para volver a la interfaz del usuario de AVG predeterminada (vista general de componentes).

## 8.5.3. Detección del analizador de correos electrónicos




En el cuadro de diálogo ***Detección mediante el Analizador de correos electrónicos*** (*accesible mediante la opción de menú del sistema Historial/Detección mediante el Analizador de correos electrónicos*) podrá ver una lista de todos los hallazgos detectados por el componente ***Analizador de correos electrónicos***. Para cada objeto detectado se proporciona la siguiente información:

- ***Infección***: descripción (y posiblemente el nombre) del objeto detectado

- ***Objeto***: ubicación del objeto
- ***Resultado***: acción realizada con el objeto detectado
- ***Tiempo de detección***: fecha y hora en que se detectó el objeto sospechoso
- ***Tipo de objeto***: tipo del objeto detectado

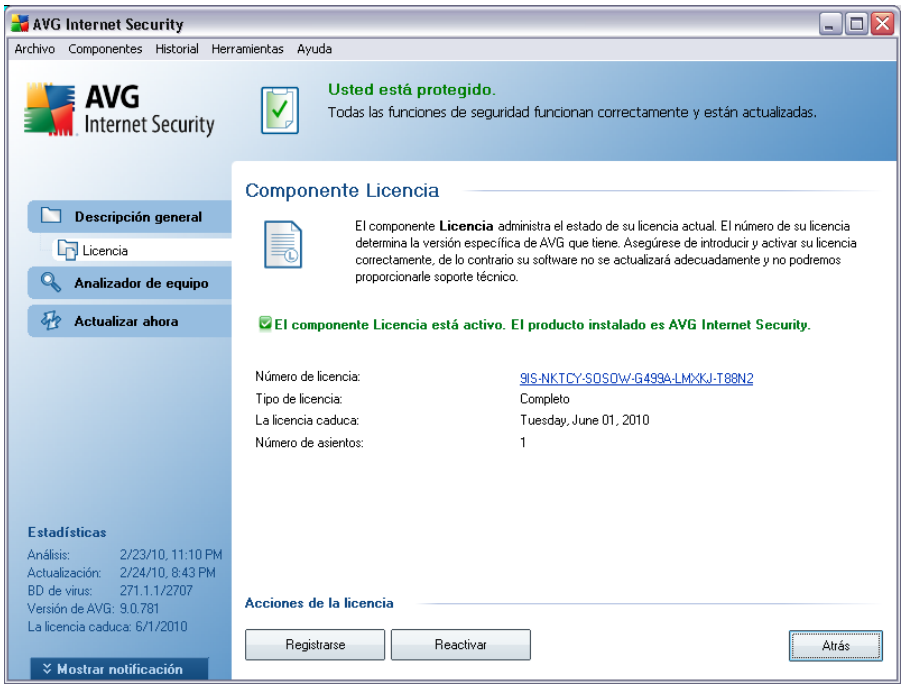
En la parte inferior del diálogo, debajo de la lista, encontrará información sobre el número total de los objetos detectados listados anteriormente. Adicionalmente puede exportar toda la lista de objetos detectados en un archivo (***Exportar lista a archivo***) y eliminar todas las entradas en los objetos detectados (***Vaciar lista***).

## Botones de control

Los botones de control disponibles en la interfaz de ***Detección del Analizador de correos electrónicos*** son:

- ***Actualizar lista***: actualiza la lista de amenazas detectadas
- ***Atrás***: lo regresará a la ***Interfaz del usuario de AVG*** predeterminada (descripción general de los componentes)

## 8.6. Licencia




En la interfaz del componente ***Licencia*** encontrará una breve descripción de las funciones del componente, información sobre su estado actual (*El componente Licencia está activo.*) y la información siguiente:

- ***Número de licencia***: indica el formato exacto del número de licencia. Al especificar el número de licencia, debe ser totalmente preciso y escribirlo exactamente como aparece. Por lo tanto, recomendamos utilizar siempre el método "copiar y pegar" para cualquier manipulación con el número de licencia.

- ***Tipo de licencia***: especifica el tipo de producto instalado.

- ***Caducidad de la licencia***: esta fecha determina el período de validez de la licencia. Si desea seguir utilizando **Anti-Virus AVG 9 más Firewall**después de esta fecha, tendrá que renovar la licencia. La renovación de la licencia se puede efectuar en línea en el sitio Web de AVG (http://www.avg.com/).

- ***Número de puestos***: indica en cuántas estaciones de trabajo puede instalar el programa **Anti-Virus AVG 9 más Firewall**.

**Botones de control**

- ***Registrarse***: permite conectarse a la página de registro del sitio Web de AVG (http://www.avg.com/). Introduzca su información de registro; sólo los clientes con productos AVG registrados pueden recibir soporte técnico gratuito.

- ***Reactivar***: abre el cuadro de diálogo ***Activar AVG*** con la información introducida en el cuadro de diálogo ***Personalizar AVG*** del proceso de instalación. Dentro de este cuadro de diálogo puede introducir el número de licencia para reemplazar el número de venta (*el número con el que instaló AVG*) o el número de licencia antiguo (*como al actualizar a un nuevo producto AVG*).

***Nota***: *si utiliza la versión de prueba de* **Anti-Virus AVG 9 más Firewall***, los botones aparecen como* ***Compre ahora*** *y* ***Activar****, que le permiten comprar la versión completa del programa inmediatamente. Para* **Anti-Virus AVG 9 más Firewall** *instalado con un número de venta, los botones aparecen como* ***Registrar*** *y* ***Activar****.*

- ***Atrás***: presione este botón para volver a la interfaz del usuario de AVG predeterminada (vista general de componentes).

## 8.7. Link Scanner

### 8.7.1. Principios de Link Scanner

El componente ***LinkScanner*** proporciona protección frente a sitios Web que se han creado con el objetivo de instalar malware en el equipo a través del navegador Web o sus complementos. La tecnología de ***LinkScanner*** consta de dos funciones, ***Protección de búsqueda AVG*** y ***Protección de navegación activa AVG***:

- ***Protección de búsqueda AVG*** contiene una lista de sitios Web (*direcciones URL*) que se sabe que son peligrosos. Al realizar una búsqueda en Google, Yahoo!, Bing, Baidu, Altavista o Yandex, todos los resultados de la búsqueda se verifican en función de esta lista y se muestra un icono de veredicto (*para Yahoo! sólo se muestran iconos de veredicto del tipo "sitio Web vulnerable"*). Además, si escribe una dirección directamente en el navegador o hace clic en un vínculo de un sitio Web o de su correo electrónico, éste se comprueba automáticamente y se bloquea si es necesario.

- ***La Protección de navegación activa AVG*** analiza el contenido de los sitios

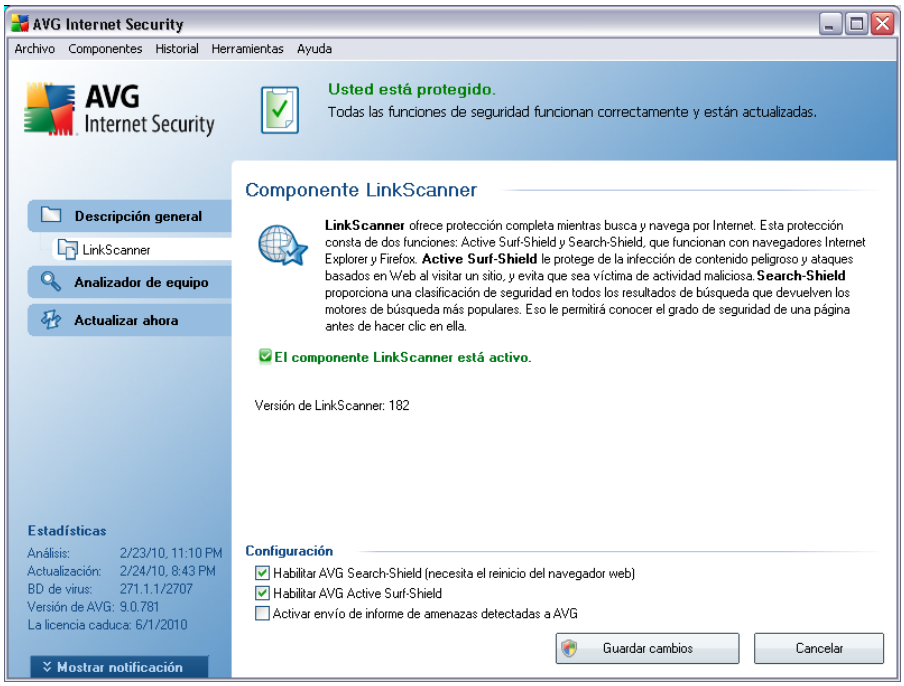
Web que visita, independientemente de la dirección del sitio Web. Aunque la ***Protección de búsqueda AVG*** no detecte alguno de estos sitios Web (*por ejemplo, un sitio Web malicioso que se haya creado recientemente o un sitio Web que antes estaba limpio y ahora contiene malware*), la ***Protección de navegación activa AVG*** lo detectará y lo bloqueará cuando intente visitarlo.

***Nota:*** *AVG Link Scanner no está diseñado para plataformas de servidor.*

## 8.7.2. Interfaz de Link Scanner

El componente ***LinkScanner*** consta de dos partes que se pueden activar o desactivar en la interfaz del ***componente LinkScanner***:

La interfaz del componente ***LinkScanner***proporciona una breve descripción del funcionamiento del componente e información sobre su estado actual (*el componente LinkScanner está activo.*). Además, puede encontrar la información acerca del número de versión de la base de datos más reciente de ***LinkScanner*** (|*Versión de LinkScanner* ).




En la parte inferior del cuadro de diálogo, puede editar varias opciones:

- ***Activar la Protección de búsqueda AVG*** (*seleccionada de modo predeterminado*): iconos asesores de notificación en las búsquedas efectuadas

en Google, Yahoo!, Bing, Baidu, Yandex o Altavista que verifican por adelantado el contenido de los sitios devuelto por el motor de búsqueda.

- ***Activar la Protección de navegación activa AVG*** *(activada de manera predeterminada)*: protección (*en tiempo real*) activa contra sitios de explotación cuando se tiene acceso a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario accede a ellos a través de un navegador Web (*o cualquier otra aplicación que utilice HTTP*).

- ***Activar envío de informe de amenazas detectadas a AVG***: seleccione este elemento para permitir que el usuario informe acerca de los sitios peligrosos y de vulnerabilidades encontrados mediante ***Navegación segura*** o ***Búsqueda segura*** y ampliar así la información de la base de datos acerca de actividad maliciosa en la Web.

### 8.7.3. AVG Search-Shield

Al realizar búsquedas en Internet con ***AVG Search-Shield*** activado, todos los resultados de búsqueda que devuelven los motores de búsqueda más populares como Yahoo!, Google, Bing, Altavista, Yandex, etc. se evalúan para buscar vínculos peligrosos o sospechosos. Al comprobar estos vínculos y marcar los vínculos malos, ***AVG LinkScanner*** muestra una advertencia antes de hacer clic en los vínculos peligrosos o sospechosos, así puede estar seguro de que sólo visitará sitios Web seguros.

Mientras se evalúa un vínculo en la página de resultados de búsqueda, verá un símbolo situado junto a él para informarle de que la verificación del vínculo está en curso. Al finalizar la evaluación se mostrará el icono informativo respectivo:

La página vinculada es segura (*con el motor de búsqueda de Yahoo! en la barra de herramientas AVG Security (este icono no se mostrará).*).

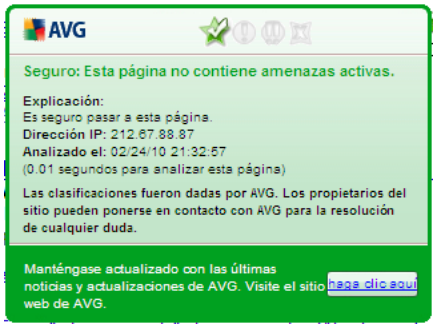
La página vinculada no contiene amenazas pero es algo sospechosa (*origen o motivos cuestionables, por lo tanto no recomendable para realizar compras por Internet, etc.*).

La página vinculada puede ser segura por sí misma pero contiene vínculos a páginas definitivamente peligrosas, o contener un código sospechoso, aunque no emplee ninguna amenaza directa en ese momento.

La página vinculada contiene amenazas activas! Por su seguridad, no se le permitirá visitar esta página.

La página vinculada no es accesible, y por ello no puede analizarse.

Al desplazarse sobre un icono de calificación se mostrarán detalles acerca del vínculo en cuestión. La información incluye detalles adicionales acerca de la amenaza (si hubiere), la dirección IP del vínculo y la fecha en que la página fue analizada con AVG:




## 8.7.4. Protección de navegación activa AVG

Esta poderosa protección bloqueará el contenido malicioso de cualquier página que intente abrir, y evitará que se descargue en su equipo. Con esta característica activada, al hacer clic en un vínculo o escribir la URL de un sitio peligroso se evitará que se abra la página Web, y le protegerá por lo tanto de infecciones inadvertidas. Es importante recordar que las páginas Web con vulnerabilidades pueden infectar su equipo por el mero hecho de visitar el sitio afectado; por esta razón, cuando solicita una página peligrosa que contiene vulnerabilidades u otras amenazas serias, ***AVG Link Scanner*** no permitirá que su navegador la muestre.

Si encuentra un sitio web malicioso, ***AVG Link Scanner*** del navegador web le advertirá con un mensaje similar al siguiente:

***¡Entrar en este sitio web es muy arriesgado y no es recomendable!***

## 8.8. Online Shield

### 8.8.1. Principios de Online Shield

***Online Shield*** es un tipo de protección residente en tiempo real; analiza el contenido de las páginas Web visitadas (y los archivos que puedan contener) incluso antes de que se visualicen en el navegador Web o de que se descarguen en el equipo.

***Online Shield*** detecta si la página que se va a visitar contiene algún javascript peligroso e impide que se visualice la página. Asimismo, reconoce el malware que contiene una página y detiene su descarga de inmediato para que nunca entre en el equipo.

***Nota:*** *AVG Online Shield no está diseñado para plataformas de servidor.*

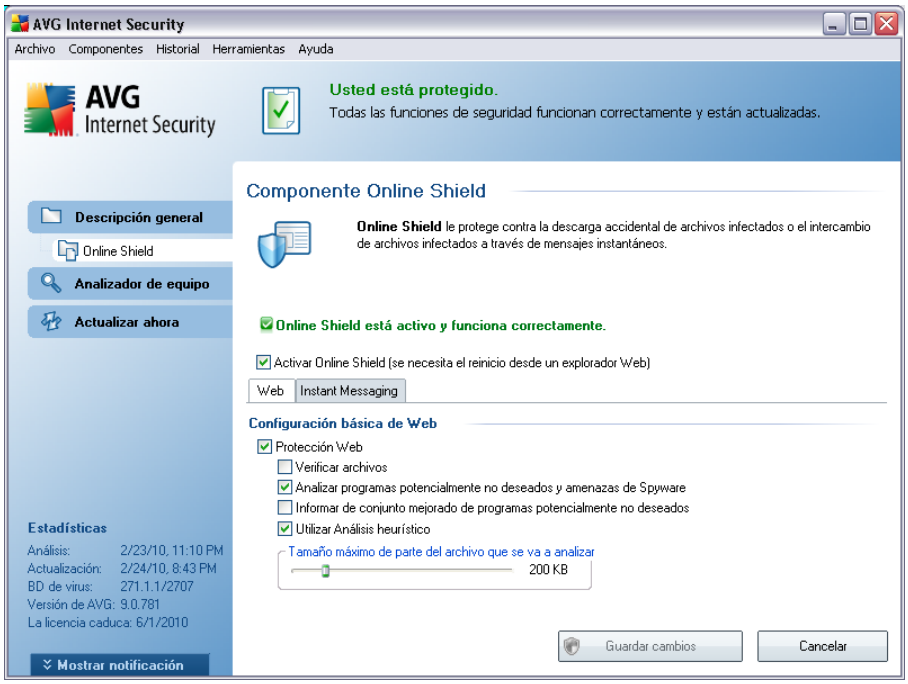
### 8.8.2. Interfaz de Online Shield

La interfaz del componente ***Online Shield*** describe el comportamiento de este tipo de protección. Adicionalmente puede encontrar información acerca del estado actual del componente (*Online Shield está activo y completamente funcional.*). En parte inferior del diálogo encontrará a continuación las opciones de edición básicas de funcionamiento de este componente.

#### Configuración básica del componente

Antes que nada, tiene la opción de activar/desactivar inmediatamente ***Online Shield*** haciendo clic en el elemento ***Activar Online Shield***. Esta opción está habilitada de manera predeterminada y el componente ***Online Shield*** está activo. Sin embargo, si no tiene una buena razón para cambiar esta configuración, le recomendamos mantener el componente activo. Si el elemento está seleccionado y ***Online Shield*** se está ejecutando, hay más opciones de configuración disponibles y editables en dos pestañas:

- ***Web*** : puede editar la configuración del componente en relación con el análisis del contenido de sitios web. La interfaz de edición permite configurar las opciones básicas siguientes:




- ***Protección Web***: esta opción confirma que ***Online Shield*** debe analizar el contenido de las páginas Web. Mientras esta opción esté seleccionada (*valor predeterminado*), podrá activar o desactivar estos elementos:

  - ***Examinar archivos***: analiza el contenido de los archivos que probablemente contenga la página web que se visualizará.

  - ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione esta opción para activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo

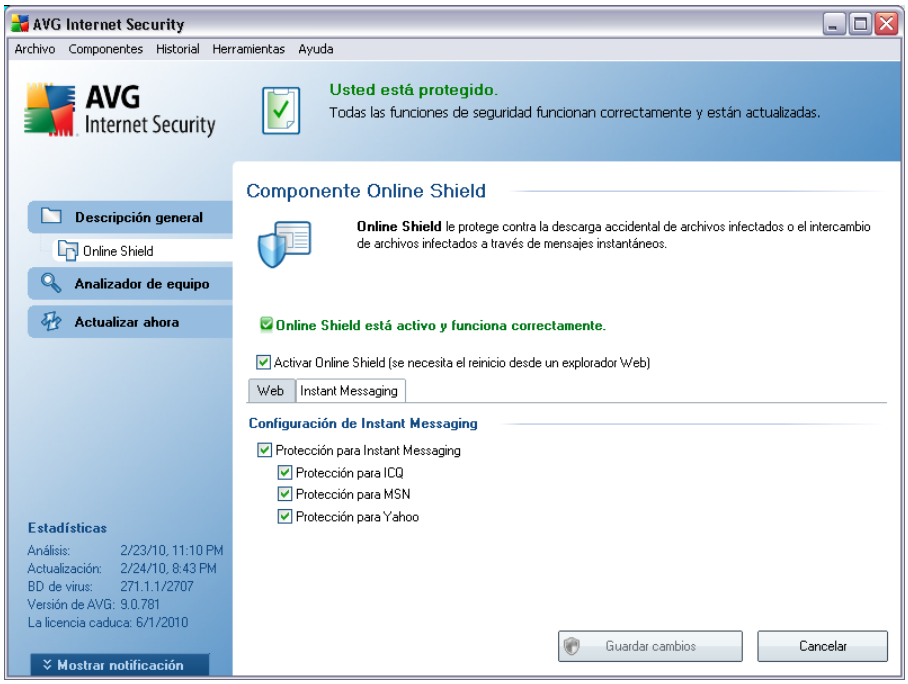
  - ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su

equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

- ***Utilizar método heurístico***: analiza el contenido de la página que se visualizará utilizando el método de análisis heurístico (simulación y evaluación de las instrucciones del objeto analizado en un entorno informático virtual. Por lo tanto, es capaz de detectar un código malicioso aún no descrito en la base de datos de virus *(consulte Principios del Anti-Virus*).

- ***Tamaño de archivo máximo de análisis***: si la página visualizada incluye archivos, también puede analizar su contenido incluso antes de que se descarguen en el equipo. Sin embargo, el análisis de archivos grandes toma bastante tiempo y es posible que la descarga de la página web se ralentice de modo notable. Puede emplear la barra deslizante para especificar el tamaño máximo de archivo que se analizará con ***Online Shield***. Aunque el tamaño del archivo descargado sea superior al valor especificado, y por consiguiente no se analice con ***Online Shield***, seguirá estando protegido: si el archivo está infectado, la ***Protección residente*** lo detectará de inmediato.

- ***Mensajería instantánea***: le permite editar la configuración de los componentes que se refieren al análisis de la mensajería instantánea (*por ejemplo ICQ, MSN Messenger, Yahoo ...*).




- Protección para mensajería instantánea: seleccione este elemento si desea que Online Shield compruebe que la comunicación en línea no contenga virus. Mientras esta opción esté activada, puede adicionalmente especificar cuál aplicación de la mensajería instantánea desea controlar; actualmente **Anti-Virus AVG 9 más Firewall** es compatible con las aplicaciones ICQ, MSN y Yahoo.

***Observe que:*** El *proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración de AVG, seleccione el elemento del menú del sistema**Herramientas/ Configuración avanzada** y edite la configuración de AVG en el diálogoConfiguración avanzada de AVG abierto recientemente.*

## Botones de control

Los botones de control disponibles dentro de la interfaz de ***Online Shield*** son:

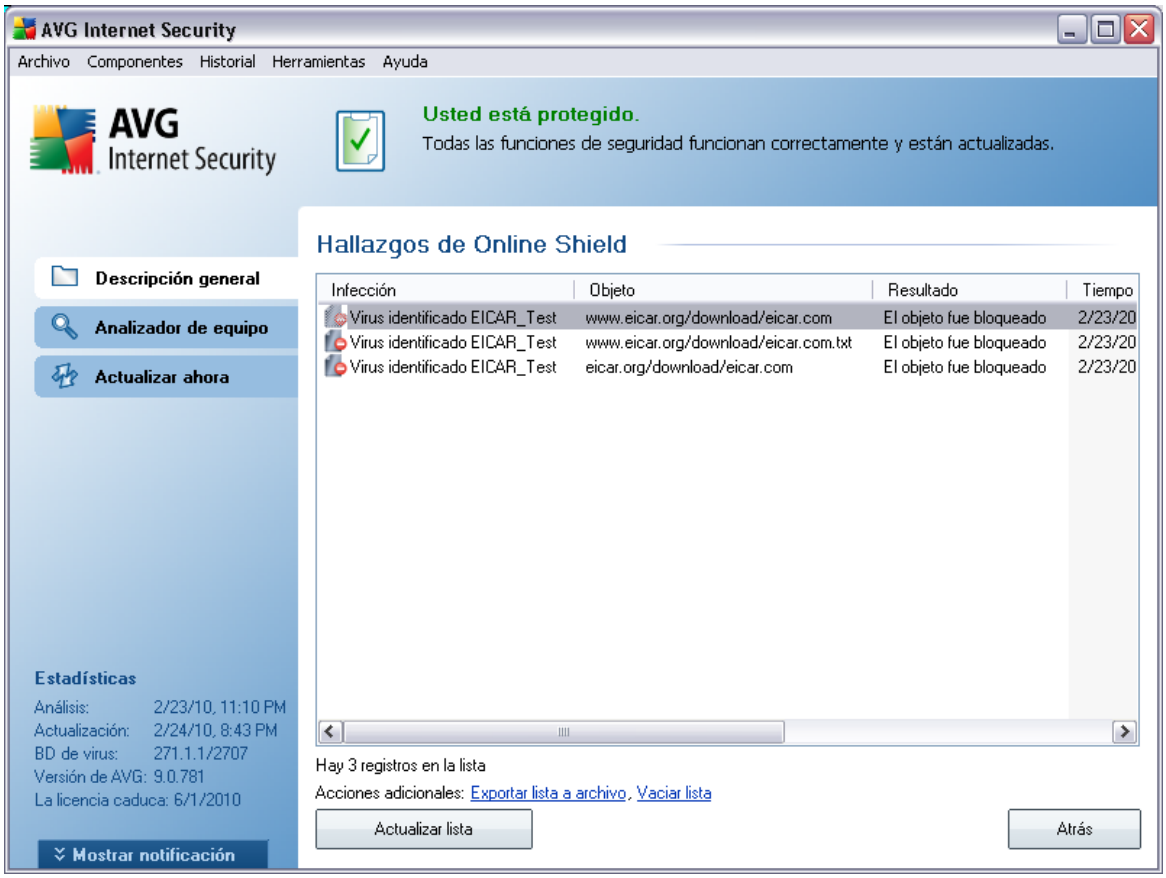
- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este diálogo.

- ***Cancelar***: presione este botón para volver a la Interfaz de usuario de AVG predeterminada (*descripción general de los componentes*).

### 8.8.3. Detección de Online Shield

***Online Shield*** analiza el contenido de las páginas Web visitadas y los archivos que puedan contener incluso antes de que se visualicen en el navegador Web o de que se descarguen en el equipo. Si se detecta una amenaza, se le avisará de forma inmediata mediante el siguiente diálogo:

La página Web sospechosa no se abrirá y se registrará la detección de amenaza en la lista de ***hallazgos de Online Shield***; esta descripción general de las amenazas detectadas es accesible mediante el menú de sistema ***Historial / Hallazgos de Online Shield***.




Para cada objeto detectado se proporciona la siguiente información:

- ***Infección***: descripción (*y posiblemente el nombre*) del objeto detectado
- ***Objeto***: fuente de donde proviene el objeto (*página Web*)
- ***Resultado***: acción realizada con el objeto detectado
- ***Tiempo de detección***: fecha y hora en que se detectó y bloqueó la amenaza
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: qué acción se llevó a cabo para señalar al objeto potencialmente peligroso de manera que se haya podido detectar

En la parte inferior del diálogo, debajo de la lista, encontrará información sobre el número total de los objetos detectados listados anteriormente. Adicionalmente puede

exportar toda la lista de objetos detectados en un archivo (***Exportar lista a archivo***) y eliminar todas las entradas en los objetos detectados (***Vaciar lista***). El botón ***Actualizar lista*** actualizará la lista de hallazgos detectados por ***Online Shield***. El botón ***Atrás*** lo regresará a la ***Interfaz del usuario de AVG*** predeterminada (descripción general de los componentes).

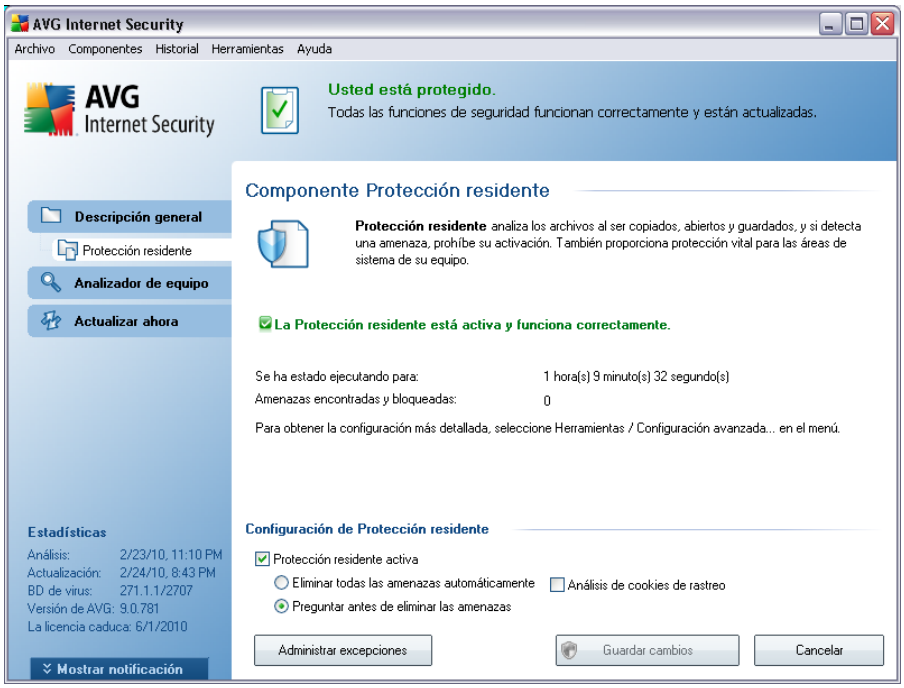
## 8.9. Protección residente

### 8.9.1. Protección residente Principios de

El componente ***Protección residente*** brinda protección continua a su equipo. Analiza cada archivo abierto, guardado o copiado, y protege las áreas de sistema del equipo. Cuando la ***Protección residente*** descubre un virus en un archivo al que se está teniendo acceso, detiene la operación que se está realizando y no permite que el virus se active. Normalmente no se advierte su presencia, ya que se ejecuta "en segundo plano", y usted sólo recibe notificaciones cuando se encuentran amenazas; al mismo tiempo, la ***Protección residente*** bloquea la activación de la amenaza y la elimina. La ***Protección residente*** se carga en la memoria del equipo durante el inicio del sistema.

***Advertencia: la Protección residente se carga en la memoria del equipo durante el inicio del sistema, y es vital que la mantenga activada todo el tiempo.***

## 8.9.2. Interfaz de protección residente




Además de una descripción general de los datos estadísticos más importantes y la información sobre el estado actual del componente (*la Protección residente está activa y completamente funcional*), la interfaz de la ***Protección residente*** ofrece algunas opciones de configuración básica del componente. La estadística es la siguiente:

- ***La Protección resident ha estado activa durante*** : proporciona el tiempo desde la última ejecución del componente
- ***Amenazas detectadas y bloqueadas***: número de infecciones detectadas cuya ejecución/apertura se evitó (*si es necesario, este valor puede ser restablecido, por ejemplo, por cuestiones estadísticas: Restablecer valor*)

### Configuración básica del componente

En la parte inferior de la ventana de diálogo encontrará la sección ***Configuración de la protección residente*** , donde puede editar algunas configuraciones básicas de funcionamiento del componente (*la configuración detallada, como con todos los demás componentes, está disponible a través de Herramientas/Configuración*

*avanzada del menú del sistema*).

La opción ***La Protección residente está activa*** le permite activar/desactivar fácilmente la protección residente. De manera predeterminada, la función está activada. Con la protección residente activada puede decidir de manera adicional como se deben tratar (eliminar) las infecciones que sea posible detectar.

- automáticamente (***Eliminar todas las amenazas automáticamente***)
- o sólo después de la aprobación del usuario (***Preguntarme antes de eliminar las amenazas***)

Esta opción no tiene impacto sobre el nivel de seguridad, y sólo refleja sus preferencias.

En ambos casos, puede seleccionar si desea ***Analizar cookies de rastreo***. En los casos específicos puede activar esta opción para alcanzar los máximos niveles de seguridad, sin embargo esta opción está desactivada de manera predeterminada. ( *cookies = paquetes de texto enviados por un servidor a un explorador Web y después enviado de regreso sin cambios por el explorador cada vez que tiene acceso a ese servidor. Las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico*).

***Observe que:*** El *proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración de AVG, seleccione el elemento del menú del sistema**Herramientas/ Configuración avanzada** y edite la configuración de AVG en el diálogoConfiguración avanzada de AVG abierto recientemente.*

## Botones de control

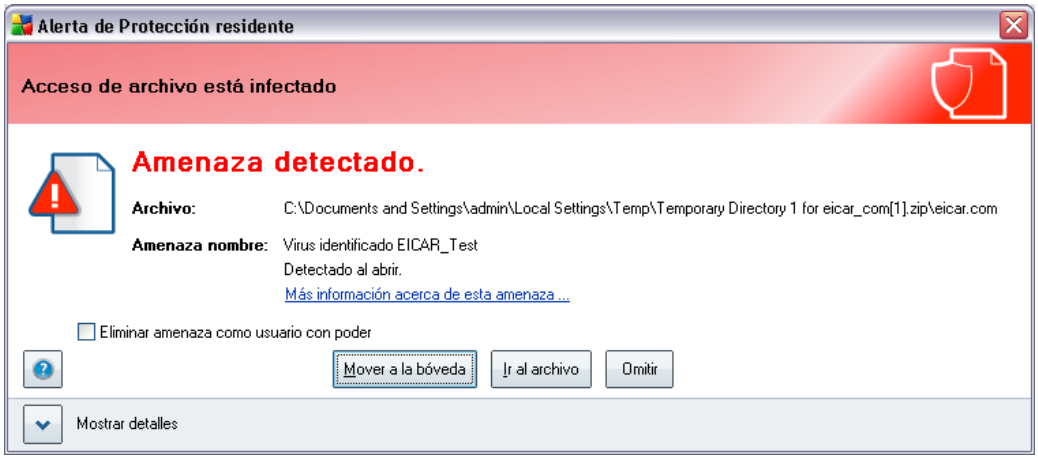
Los botones de control disponibles dentro de la interfaz de la ***Protección residente*** son:

- ***Administrar excepciones***: abre el cuadro de diálogo ***Protección residente: Exclusiones del directorio***, donde puede definir las carpetas que deben excluirse del análisis de la ***Protección residente***
- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este diálogo.

- ***Cancelar***: presione este botón para volver a la ***interfaz del usuario de AVG*** predeterminada (vista general de componentes).

### 8.9.3. Detección de protección residente

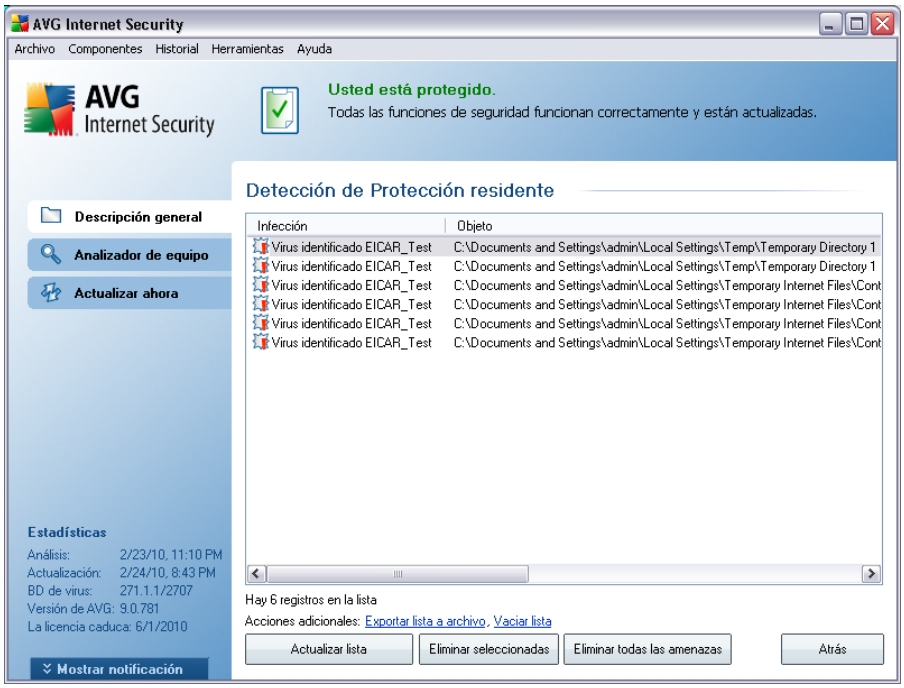
***La Protección residente*** analiza los archivos mientras éstos se copian, se abren o se guardan. Cuando se detecta una amenaza de virus o de cualquier tipo, se le advertirá inmediatamente mediante este diálogo:




El diálogo proporciona información acerca de la amenaza detectada y le invita a decidir qué acción se debe realizar:

- ***Reparar***: si existe una cura disponible, AVG reparará el archivo infectado de forma automática; esta opción es la recomendada.
- ***Mover a la Bóveda***: el virus será movido a la Bóveda de virus ***AVG.***
- ***Ir al archivo***: esta opción lo redirige a la ubicación del objeto sospechoso (*abre una ventana nueva del Explorador de Windows*)
- ***Ignorar***: recomendamos encarecidamente NO utilizar esta opción, a menos que tenga una muy buena razón para hacerlo.

La descripción general de todas las amenazas detectadas por la ***Protección residente*** puede encontrarse en el cuadro de diálogo de detección de la ***Protección residente***, accesible desde la opción de menú del sistema ***Historial / Hallazgos de la Protección residente***:




La ***Detección de protección residente*** ofrece una descripción general de los objetos que detectó la ***Protección residente***, evaluados como peligrosos y reparados o movidos a la ***Bóveda de virus***. Para cada objeto detectado se proporciona la siguiente información:

- ***Infección***: descripción (y posiblemente el nombre) del objeto detectado
- ***Objeto***: ubicación del objeto
- ***Resultado***: acción realizada con el objeto detectado
- ***Tiempo de detección***: fecha y hora en que el objeto fue detectado
- ***Tipo de objeto***: tipo del objeto detectado
- ***Proceso***: qué acción se llevó a cabo para señalar al objeto potencialmente peligroso de manera que se haya podido detectar

En la parte inferior del diálogo, debajo de la lista, encontrará información sobre el número total de los objetos detectados listados anteriormente. Adicionalmente puede exportar toda la lista de objetos detectados en un archivo (***Exportar lista a archivo***) y eliminar todas las entradas en los objetos detectados (***Vaciar lista***). El botón ***Actualizar lista*** actualizará la lista de hallazgos detectados por la ***Protección***

***residente***. El botón ***Atrás*** lo regresará a la ***Interfaz del usuario de AVG*** predeterminada (descripción general de los componentes).

## 8.10. Administrador de actualización

### 8.10.1. Principios de administrador de actualización

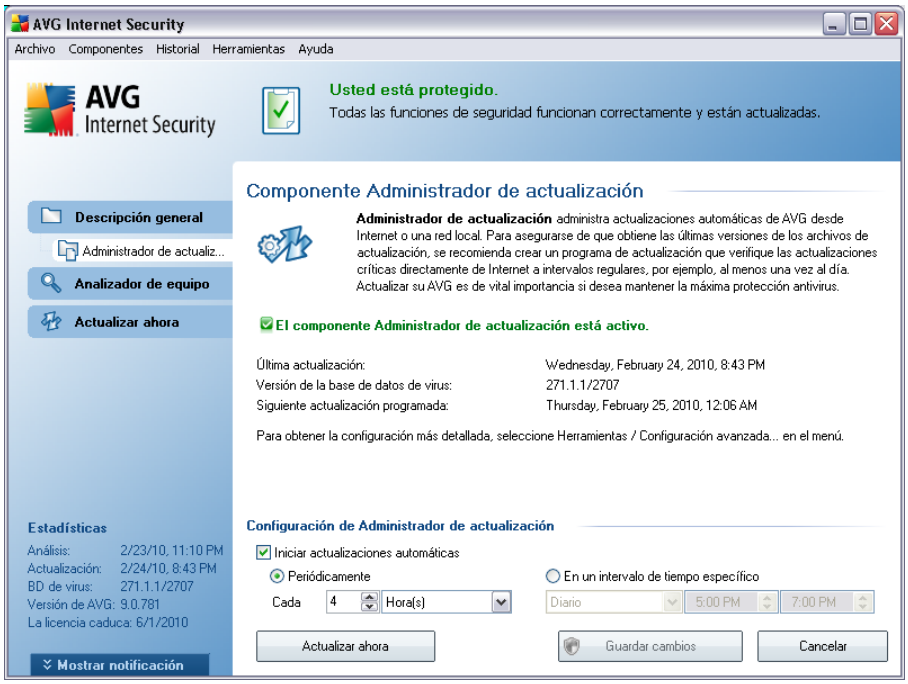
Ningún software de seguridad puede garantizar una verdadera protección ante los diversos tipos de amenazas si no se actualiza periódicamente. Los desarrolladores de virus siempre buscan nuevas fallas que explotar en el software y el sistema operativo. Diariamente aparecen nuevos virus, nuevo malware y nuevos ataques de hackers. Por ello, los proveedores de software generan constantes actualizaciones y parches de seguridad, con objeto de corregir las deficiencias de seguridad descubiertas.

***Es fundamental actualizar el programa AVG periódicamente.***

El ***Administrador de actualizaciones*** ayuda a controlar las actualizaciones periódicas. En este componente, puede programar las descargas automáticas de archivos de actualización desde Internet o la red local. Las actualizaciones de definiciones de virus esenciales deben ser diarias si es posible. Las actualizaciones del programa menos urgentes pueden efectuarse semanalmente.

***Nota:*** *preste atención al capítulo Actualizaciones de AVG para obtener más información sobre los tipos y niveles de actualización.*

## 8.10.2. Interfaz de administrador de actualización




La interfaz del ***Administrador de actualizaciones*** muestra información sobre las funciones del componente y su estado actual (*El Administrador de actualizaciones está activo.*), además de proporcionar los datos estadísticos relevantes:

- ***Actualización más reciente***: especifica la fecha y la hora en que se ha actualizado la base de datos.
- ***Versión de la base de datos de virus***: define el número de la última versión de la base de datos de virus, cuyo valor aumenta con cada actualización de dicha base de datos.
- ***Siguiente actualización programada***: especifica cuándo y a qué hora está programada la siguiente actualización de la base de datos

### Configuración básica del componente

En la parte inferior del diálogo puede encontrar la sección ***Configuración del Administrador de actualizaciones*** donde puede efectuar algunos cambios en las reglas de ejecución del proceso de actualización. Puede definir si desea descargar los archivos de actualización automáticamente (***Iniciar actualizaciones automáticas***) o

solo a pedido. De modo predeterminado, la opción ***Iniciar actualizaciones automáticas*** está seleccionada, y recomendamos dejarla así. La descarga periódica de los archivos de actualización más recientes es fundamental para el correcto funcionamiento de cualquier software de seguridad.

De modo adicional, puede definir cuándo debe ejecutarse la actualización:

- ***Periódicamente***: defina el intervalo de tiempo.
- ***En un momento concreto***: defina la fecha y la hora exactas.

De modo predeterminado, el valor de actualización configurado es cada 4 horas. Se recomienda encarecidamente que no modifique esta configuración salvo que tenga un motivo real para hacerlo.

***Observe que:*** El *proveedor del software ha configurado todos los componentes de AVG para que proporcionen un rendimiento óptimo. No modifique la configuración de AVG salvo que tenga un motivo real para hacerlo. Sólo un usuario experimentado puede llevar a cabo cualquier cambio en la configuración. Si necesita cambiar la configuración de AVG, seleccione el elemento del menú del sistema****Herramientas/ Configuración avanzada*** *y edite la configuración de AVG en el diálogoConfiguración avanzada de AVG abierto recientemente.*

## Botones de control

Los botones de control disponibles en la interfaz del ***Administrador de actualizaciones*** son:

- ***Actualizar ahora***: ejecuta una actualización inmediata a pedido.
- ***Guardar cambios***: presione este botón para guardar y aplicar los cambios efectuados en este diálogo.
- ***Cancelar***: presione este botón para volver a la ***interfaz del usuario de AVG*** predeterminada (vista general de componentes).

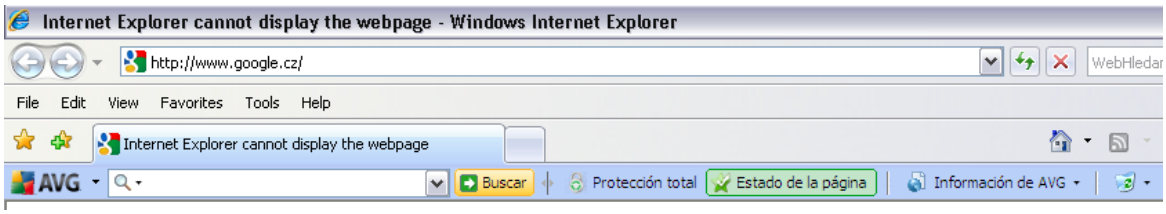
# 9. Barra de herramientas AVG Security

***La barra de herramientas AVG Security*** es una nueva herramienta que funciona con el componente ***AVG LinkScanner*** y que comprueba los resultados de búsqueda de los motores de búsqueda de Internet compatibles (*Yahoo!, Google, Bing, Altavista, Baidu*). ***La barra de herramientas AVG Security*** se puede utilizar para controlar las funciones de ***AVG LinkScanner*** y para ajustar su comportamiento.

Si elige instalar la barra de herramientas durante la instalación de **Anti-Virus AVG 9 más Firewall**, se agregará automáticamente en el navegador Web. Si está utilizando algún otro navegador de Internet (*por ejemplo, Avant Browser*), puede producirse un comportamiento inesperado.

## 9.1. Barra de herramientas AVG Security Interfaz

La ***barra de herramientas AVG Security*** está diseñada para funcionar con ***MS Internet Explorer*** (*versión 6.0 o posterior*) y ***Mozilla Firefox*** (*versión 2.0 o posterior*). Una vez que haya decido instalar la ***barra de herramientas AVG Security*** (*durante el proceso de instalación de AVG se le solicita si desea instalar este componente*), el componente se ubicará en el navegador Web, justo debajo de la barra de direcciones:




***Nota:*** *La barra de herramientas AVG Security no está diseñada para plataformas de servidor.*

La ***barra de herramientas AVG Security*** consta de los siguientes elementos:

- ***Logotipo de AVG***: proporciona acceso a los elementos generales de la barra de herramientas. Haga clic en el botón del logotipo para ir al sitio Web de AVG (http://www.avg.com/). Al hacer clic con el puntero al lado del icono AVG se abrirán las siguientes opciones:
  - ***Información de la barra de herramientas***: vínculo a la página de inicio de la ***barra de herramientas AVG Security***, que contiene información detallada acerca de la protección que le ofrece la barra de herramientas.
  - ***Iniciar Anti-Virus AVG 9 más Firewall***: abre la interfaz del usuario

- ***Opciones***: abre un cuadro de diálogo de configuración donde puede ajustar la configuración de la ***barra de herramientas AVG Security*** para adaptarla a sus necesidades. Consulte el siguiente capítulo: ***Opciones de la barra de herramientas AVG Security***

- ***Eliminar historial***: le permite *eliminar el historial completo* de la barra de herramientas AVG Security o *eliminar el historial de búsqueda, eliminar el historial del navegador, eliminar el historial de descargas* y *eliminar las cookies*.

- ***Actualizar***: comprueba si existen nuevas actualizaciones para su ***barra de herramientas AVG Security***

- ***Ayuda***: proporciona opciones para abrir el archivo de ayuda, enviar comentarios acerca del producto o ver los detalles de la versión actual de la barra de herramientas

- ***Cuadro de búsqueda***: introduzca una palabra o una frase en el cuadro de búsqueda. Presione ***Buscar*** para iniciar la búsqueda mediante el motor de búsqueda especificado (*puede especificarlo en Barra de herramientas AVG Security > Opciones avanzadas y elegir Yahoo!, Wikipedia, Baidu, WebHledani o Yandex*), independientemente de la página que se muestre en estos momentos. El cuadro de búsqueda también muestra el historial de búsqueda. Las búsquedas hechas mediante el cuadro de búsqueda se analizan utilizando la ***Protección de búsqueda AVG***.

- ***Protección total***: este botón puede aparecer como ***Protección total*** / ***Protección limitada*** / ***Sin protección*** en función de la **Anti-Virus AVG 9 más Firewall**configuración

- ***Estado de la página***: ubicado directamente en la barra de herramientas, este botón muestra la evaluación de la página Web cargada actualmente en función de los criterios del componente ***Protección de búsqueda AVG*** (*la página es segura, sospechosa, definitivamente peligrosa, contiene amenazas, o no pudo analizarse*). Haga clic en este botón para abrir un panel con información detallada sobre la página Web específica.

- ***Información de AVG***: proporciona vínculos a información de seguridad importante ubicada en el sitio Web de AVG (http://www.avg.com/).

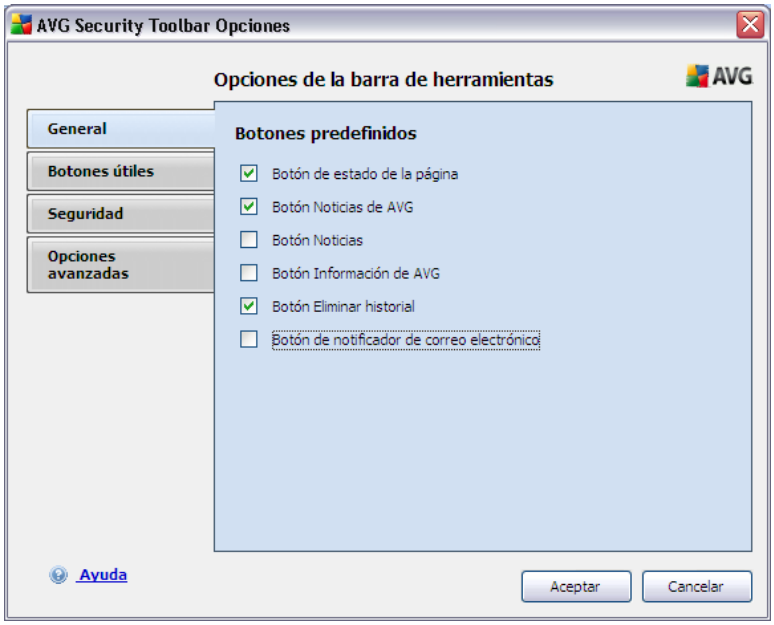
    - ***Información de la barra de herramientas***: vínculo a la página de inicio de la ***barra de herramientas AVG Security***, que contiene información detallada acerca de la protección que le ofrece la barra de herramientas.

- ***Acerca de las amenazas***: abre la página Web de AVG, que contiene información sobre los virus y amenazas actuales en Internet
- ***Noticias de AVG***: abre la página Web que proporciona los comunicados de prensa relacionados con AVG más recientes
- ***Nivel de amenaza actual***: abre la página Web del laboratorio de virus con una visualización gráfica del nivel de amenaza actual en Internet
- ***Enciclopedia de virus***: abre la página Enciclopedia de virus, en la cual puede encontrar los virus específicos por nombre junto con información detallada de cada uno de ellos

## 9.2. Opciones de la Barra de herramientas AVG Security

Toda la configuración de los parámetros de la ***barra de herramientas AVG Security*** puede modificarse directamente en el panel de la ***barra de herramientas AVG Security***. La interfaz de edición se abre mediante el elemento de menú de la barra de herramientas *AVG / Opciones* en un nuevo cuadro de diálogo denominado ***Opciones de la barra de herramientas***, el cual se divide en cuatro secciones:

### 9.2.1. Pestaña General

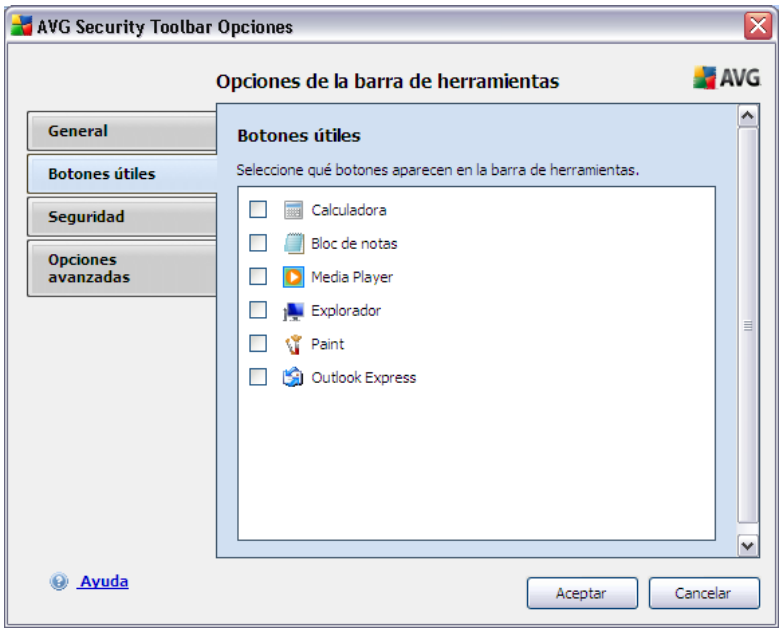



En esta pestaña puede especificar los botones de control de la barra de herramientas

que deben mostrarse u ocultarse en el panel ***Barra de herramientas AVG Security***. Marque las opciones para las cuales desea que se muestre el botón respectivo. A continuación encontrará una descripción de la función de los botones de la barra de herramientas:

- ***Botón Noticias de AVG***: abre una página Web que proporciona los comunicados de prensa relacionados con AVG más recientes
- ***Botón Noticias***: proporciona una descripción general estructurada de las noticias actuales de la prensa diaria
- ***Botón Información de AVG***: ofrece información sobre la barra de herramientas AVG, las amenazas actuales y el nivel de amenaza en Internet, abre la enciclopedia de virus y proporciona más noticias relacionadas con los productos AVG
- ***Botón Eliminar historial***: este botón permite eliminar el historial completo o eliminar el historial de búsqueda, eliminar el historial del navegador, eliminar el historial de descargas o eliminar las cookiesdirectamente desde el panel de la barra de herramientas de AVG Security.

### 9.2.2. Pestaña Botones útiles




La pestaña ***Botones útiles*** permite seleccionar aplicaciones de una lista y visualizar su

icono en la interfaz de la barra de herramientas. De esta manera, el icono sirve de vínculo rápido que permite iniciar inmediatamente la aplicación correspondiente.

### 9.2.3. Pestaña Seguridad

La pestaña ***Seguridad*** se divide en dos secciones, ***Seguridad del navegador de AVG*** y ***Clasificaciones***, en donde puede seleccionar casillas de verificación específicas para asignar la funcionalidad de la ***barra de herramientas AVG Security*** que desee utilizar:

- ***Seguridad del navegador de AVG***: seleccione este elemento para activar o desactivar el servicio ***Protección de búsqueda AVG*** o ***Protección de navegación activa AVG***

- ***Clasificaciones***: seleccione los símbolos gráficos utilizados para las clasificaciones de los resultados de búsqueda por el componente ***Protección de búsqueda AVG*** que desee utilizar:

  - la página es segura

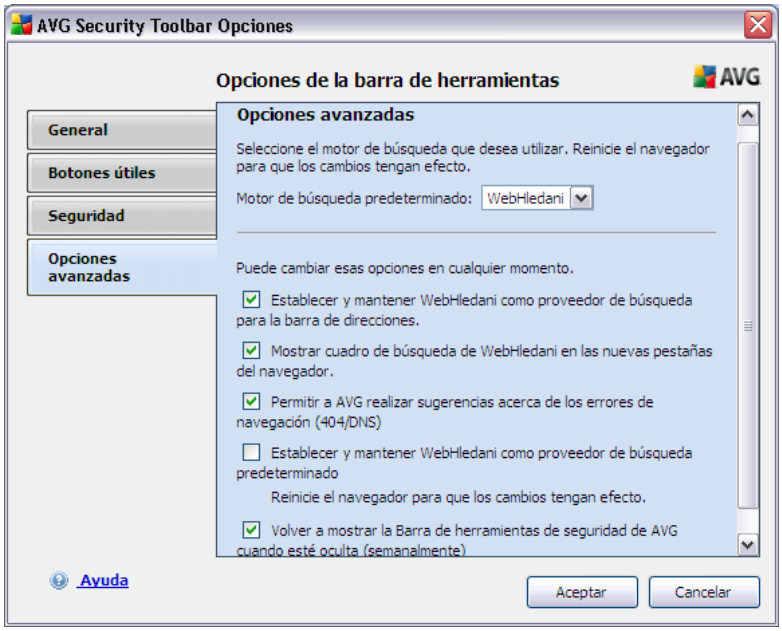
  - la página es algo sospechosa

  - la página contiene vínculos a páginas definitivamente peligrosas

- o la página contiene amenazas activas
- o la página no es accesible, por lo tanto, no puede analizarse

Seleccione la opción correspondiente para confirmar que desea recibir información acerca de este nivel de amenaza específico. Sin embargo, la marca roja asignada a las páginas que contienen amenazas activas y peligrosas no se puede desactivar. ***Nuevamente, se recomienda conservar la configuración predeterminada que estableció el proveedor del programa a menos que cuente con una razón real para cambiarla.***

## 9.2.4. Pestaña Opciones avanzadas




En la pestaña ***Opciones avanzadas*** seleccione primero qué motor de búsqueda desea utilizar de forma predeterminada. Puede elegir entre *Yahoo!, Baidu, WebHledani* y *Yandex*. Si ha cambiado el motor de búsqueda predeterminado, reinicie su navegador de Internet para que el cambio surta efecto.

Además, puede activar o desactivar valores específicos de la ***Barra de herramientas AVG Security***:

- ***Establecer y mantener Yahoo! como el proveedor de búsqueda de la barra de direcciones*** (*activada de forma predeterminada*): si esta opción

está seleccionada, puede escribir un término de búsqueda directamente en la barra de direcciones del navegador de Internet, y el servicio de Yahoo! se utilizará automáticamente para buscar los sitios Web de interés.

- ***Permitir a AVG realizar sugerencias acerca de los errores de navegación del navegador (404/DNS)*** (*activada de forma predeterminada*): si durante la búsqueda en Internet se encuentra con una página que no existe o que no se puede visualizar (error 404), se le mostrará automáticamente una página Web que permite seleccionar entre algunas páginas alternativas relacionadas con el tema.

- ***Establecer y mantener Yahoo! como proveedor de búsqueda para el navegador***: (*desactivada de forma predeterminada*): Yahoo! es el motor de búsqueda predeterminado para la búsqueda en Internet en la barra de herramientas AVG Security, y al activar esta opción se puede convertir también en el motor de búsqueda predeterminado del navegador Web.

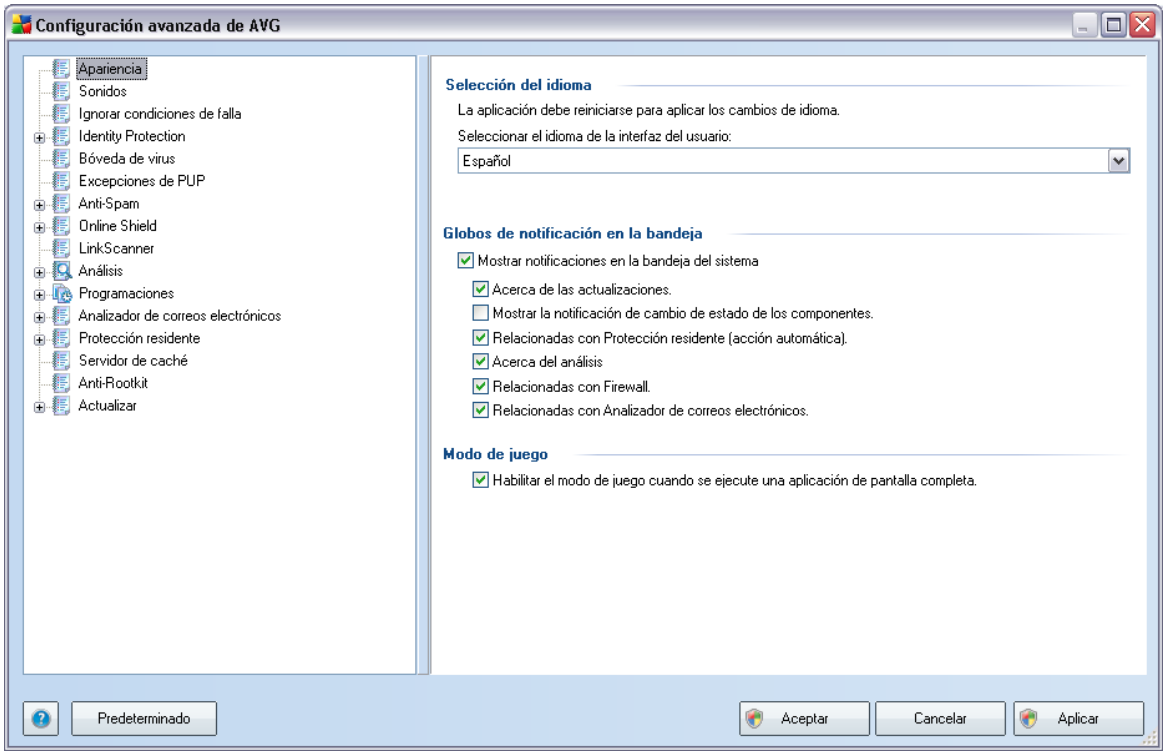
- ***Volver a mostrar la barra de herramientas AVG Security cuando esté oculta (semanalmente)*** (*activada de forma predeterminada*): esta opción está seleccionada de manera predeterminada, así que cuando la ***barra de herramientas AVG Security*** se oculte accidentalmente, se volverá a mostrar nuevamente en el término de una semana.

# 10. Configuración avanzada de AVG

El cuadro de diálogo de configuración avanzada de **Anti-Virus AVG 9 más Firewall** se abre en una ventana nueva denominada ***Configuración avanzada de AVG***. La ventana está dividida en dos secciones: la parte izquierda ofrece una navegación organizada en forma de árbol hacia las opciones de configuración del programa. Seleccione el componente del que desea cambiar la configuración (*o su parte específica*) para abrir el diálogo de edición en la sección del lado derecho de la ventana.

## 10.1. Apariencia

El primer elemento del árbol de navegación, ***Apariencia***, hace referencia a la configuración general de la Interfaz del usuario de AVG y a unas cuantas opciones básicas del comportamiento de la aplicación:

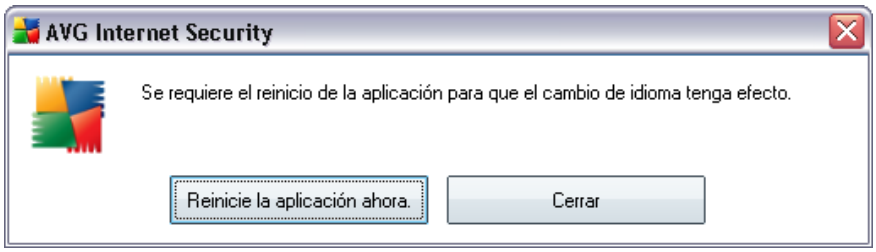



### Selección de idioma

En la sección ***Selección de idioma***, puede elegir el idioma deseado en el menú

desplegable; este idioma será el que se utilice en toda la Interfaz del usuario de AVG. El menú desplegable sólo ofrece aquellos idiomas que se seleccionaron previamente para que se instalaran durante el proceso de instalación (consulte el capítulo Instalación personalizada - Selección de componentes). Sin embargo, para finalizar el cambio de la aplicación a otro idioma se tiene que reiniciar la interfaz de usuario; siga estos pasos:

- Seleccione el idioma deseado de la aplicación y confirme su selección presionando el botón ***Aplicar*** (esquina inferior derecha)
- Presione el botón ***Aceptar*** para confirmar
- El nuevo cuadro de diálogo emergente que le informa del cambio de idioma de la interfaz del usuario de AVG requiere reiniciar la aplicación:




## Notificaciones de globo en la bandeja

Dentro de esta sección se puede suprimir la visualización de las notificaciones de globo sobre el estado de la aplicación en la bandeja del sistema. De manera predeterminada, se permite la visualización de las notificaciones de globo, y se recomienda mantener esta configuración. Las notificaciones de globo normalmente informan acerca del cambio de estado de algún componente AVG, y se les debe prestar atención.

Sin embargo, si por alguna razón decide que no se visualicen estas notificaciones, o desea que sólo se muestren ciertas notificaciones (relacionadas con un componente AVG específico), se pueden definir y especificar las preferencias seleccionando/ quitando la marca de selección de las siguientes opciones:

- ***Mostrar las notificaciones en la bandeja de sistema:*** de manera predeterminada, este elemento está seleccionado (*activado*) y las notificaciones se visualizan. Quite la marca de selección de este elemento para desactivar la visualización de todas las notificaciones de globo. Cuando se encuentra activado, puede también seleccionar qué notificaciones en concreto deben visualizarse:

- ***Mostrar las notificaciones de la bandeja acerca de las actualizaciones***: decida si debe visualizarse información sobre la ejecución, el progreso y la finalización del proceso de actualización de AVG;

- ***Mostrar las notificaciones de cambio de estado de los componentes*** : decida si debe visualizarse información relativa a la actividad o inactividad de los componentes o los posibles problemas. A la hora de notificar un estado de error de un componente, esta opción equivale a la función informativa del icono de la bandeja del sistema (que cambia de color) que notifica un problema en cualquier componente AVG;

- ***Mostrar las notificaciones de la bandeja relacionadas con la Protección residente***: decida si debe visualizarse o suprimirse la información relativa a los procesos de guardado, copia y apertura de los archivos (*esta configuración sólo muestra si la opción Autoreparar de Protección residente está activa*);

- ***Mostrar las notificaciones de la bandeja acerca del análisis***: decida si debe visualizarse información sobre la ejecución automática del análisis programado, su progreso y resultados;

- ***Mostrar las notificaciones de la bandeja relacionadas con el Firewall*** : decida si debe visualizarse la información relativa al estado y los procesos relacionados con el Firewall, por ejemplo, las advertencias de activación/desactivación del componente, el posible bloqueo de tráfico, etc.

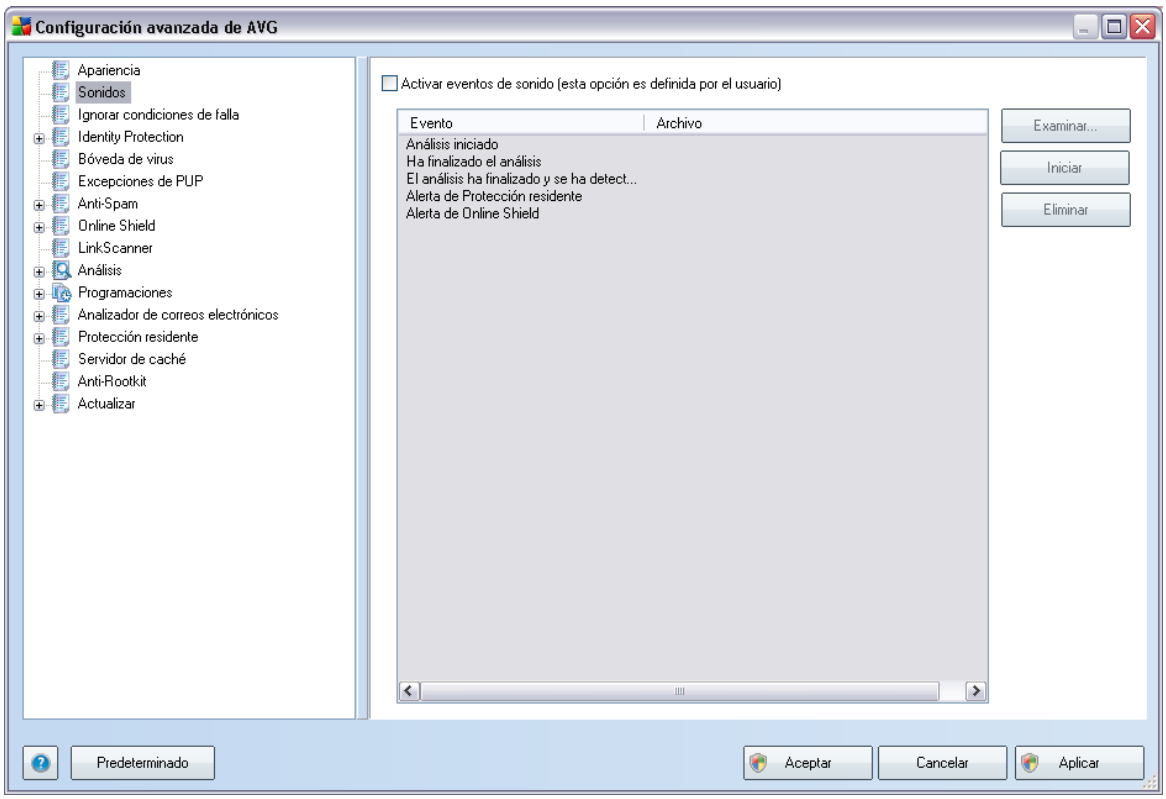
- ***Mostrar las notificaciones de la bandeja relacionadas con el Analizador de correos electrónicos***: decida si debe visualizarse información sobre análisis de todos los mensajes de correo electrónico entrantes y salientes.

## Modo de juego

Esta función de AVG está diseñada para aplicaciones de pantalla completa donde los globos de información de AVG (*que se abren al iniciar un análisis programado, por ejemplo*) pueden resultar molestos (*pueden minimizar la aplicación o dañar los gráficos* ). Para evitar esta situación, mantenga seleccionada la casilla de verificación ***Habilitar el modo de juego cuando se ejecute una aplicación de pantalla completa***( *configuración predeterminada*).

## 10.2. Sonidos

En el cuadro de diálogo ***Sonidos***, puede especificar si desea que se le informe acerca de acciones específicas de AVG mediante una notificación sonora. Si es así, seleccione la opción ***Activar eventos de sonido*** (*desactivada de forma predeterminada*) para activar la lista de acciones de AVG:

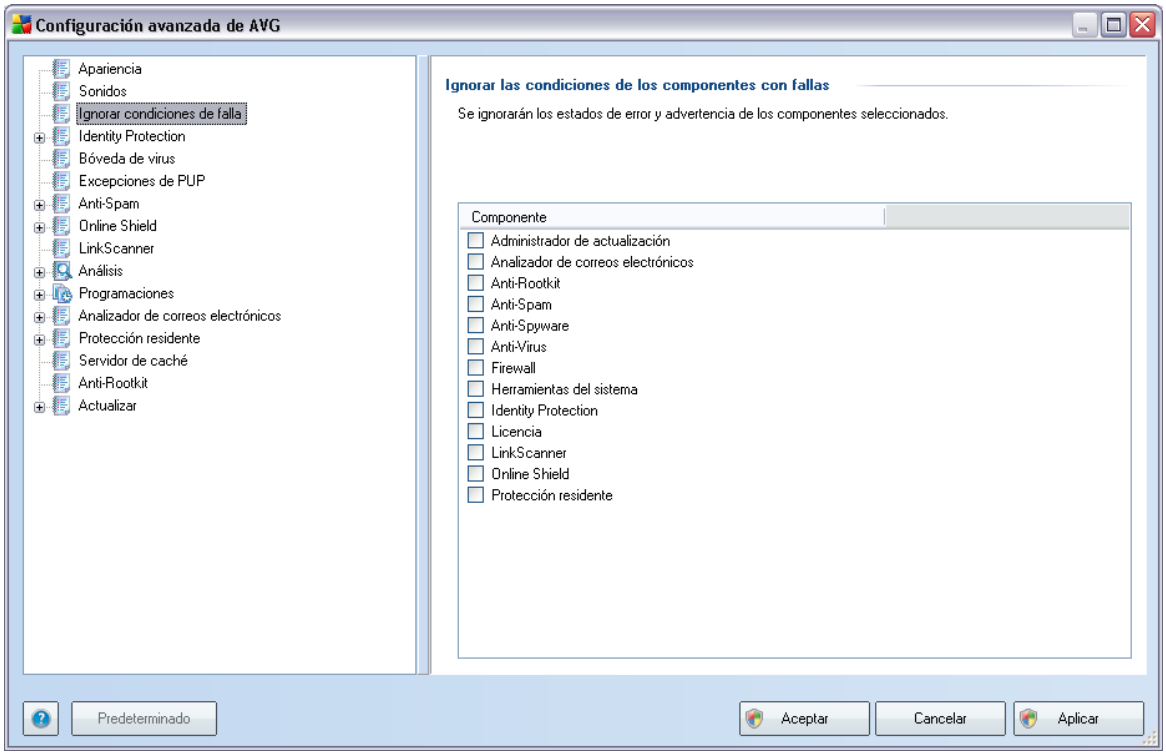



A continuación, seleccione el evento correspondiente de la lista y busque (***Examinar***) en el disco el sonido adecuado que desea asignar a este evento. Para escuchar el sonido seleccionado, resalte el evento en la lista y presione el botón ***Reproducir***. Utilice el botón ***Eliminar*** para eliminar el sonido asignado a un evento específico.

***Nota:*** *solamente los sonidos *.wav son compatibles.*

## 10.3. Ignorar condiciones de falla

En el diálogo ***Ignorar las condiciones de los componentes con fallas***puede marcar aquellos componentes de los que no desea estar informado:




De manera predeterminada, ningún componente está seleccionado en esta lista. Lo cual significa que si algún componente se coloca en un estado de error, se le informará de inmediato mediante:

- ***el icono en la bandeja de sistema***: mientras todas las partes de AVG funcionen correctamente, el icono se muestra en cuatro colores; sin embargo, si ocurre un error,  el icono aparece con un signo de admiración amarillo

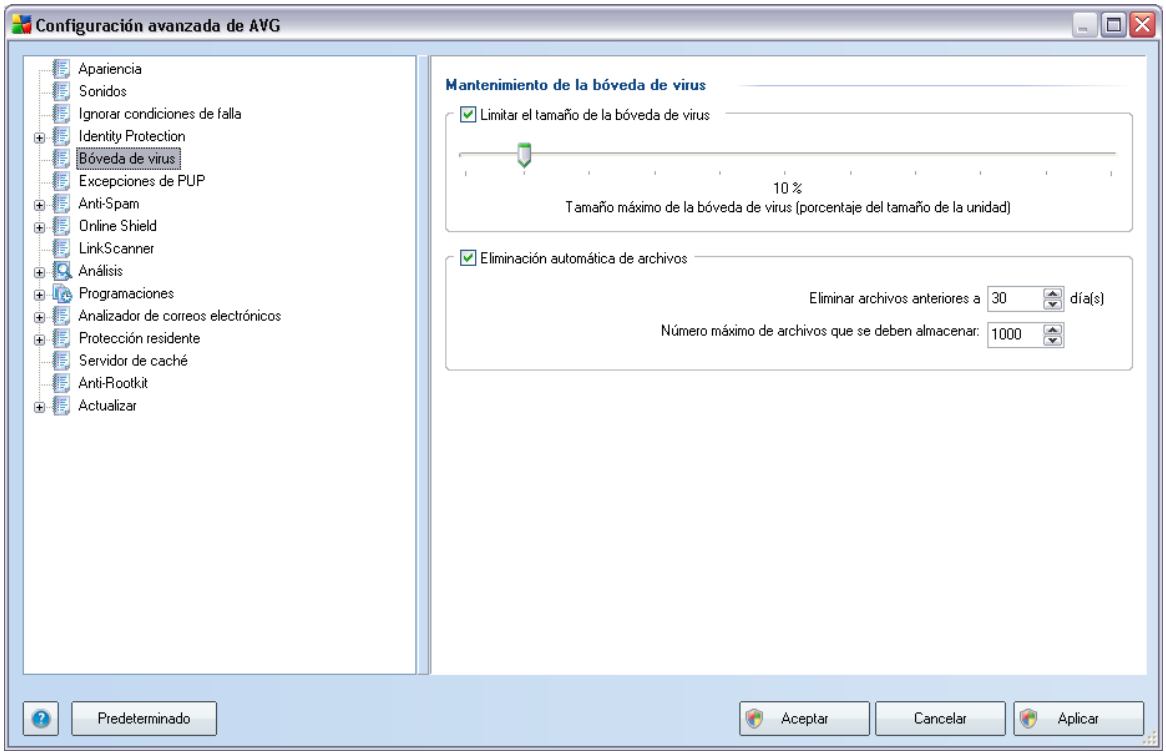
- la descripción de texto del problema existente en la sección ***Información del estado de seguridad*** de la ventana principal de AVG

Puede haber una situación en la cual por alguna razón es necesario desactivar un componente temporalmente (*no es recomendable, se debe intentar conservar todos los componentes activados permanentemente y con la configuración predeterminada, pero esto puede suceder*). En ese caso el icono en la bandeja de sistema informa

automáticamente del estado de error del componente. Sin embargo, en este caso específico no podemos hablar de un error real debido a que usted mismo lo introdujo deliberadamente, y está consciente del riesgo potencial. A su vez, una vez que el icono se muestra en color gris, no puede informar realmente de ningún error adicional posible que pueda aparecer.

Para esta situación, dentro del diálogo anterior puede seleccionar los componentes que pueden estar en un estado de error (*o desactivados*) y de los cuales no desea estar informado. La misma opción de ***Ignorar el estado del componente*** también está disponible para componentes específicos directamente desde la descripción general de los componentes en la ventana principal de AVG.

## 10.4. Bóveda de Virus




El cuadro de diálogo ***Mantenimiento de la Bóveda de virus*** permite definir varios parámetros relacionados con la administración de objetos almacenados en la ***Bóveda de virus***:

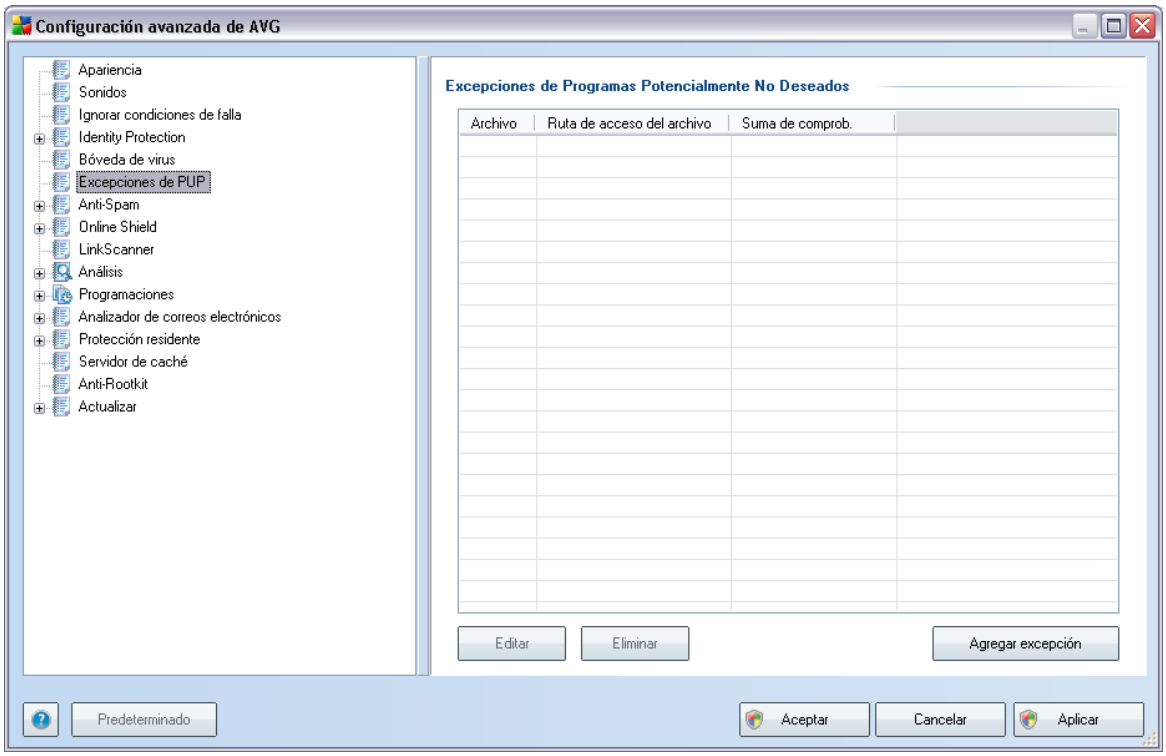
- ***Limitar el tamaño de la Bóveda de virus***: utilice el control deslizante para configurar el tamaño máximo de la ***Bóveda de virus***. El tamaño se especifica

proporcionalmente en comparación con el tamaño del disco local.

- ***Eliminación automática de archivos***: en esta sección, defina la longitud máxima de tiempo que se almacenarán los objetos en la ***Bóveda de Virus*** ( ***Eliminar archivos anteriores a... días***) y el número máximo de archivos que se almacenarán en la ***Bóveda de Virus*** (***Número máximo de archivos que se deben almacenar***).

## 10.5. Excepciones de PUP

**Anti-Virus AVG 9 más Firewall** puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas en el sistema. En algunos casos, el usuario puede querer mantener ciertos programas no deseados en el equipo ( *programas que fueron instalados intencionalmente*). Algunos programas, en especial los gratuitos, incluyen adware. Dicho adware puede ser detectado y presentado por AVG como ***un Programa potencialmente no deseado*** . Si desea mantener este programa en su equipo, lo puede definir como una excepción de programas potencialmente no deseados:



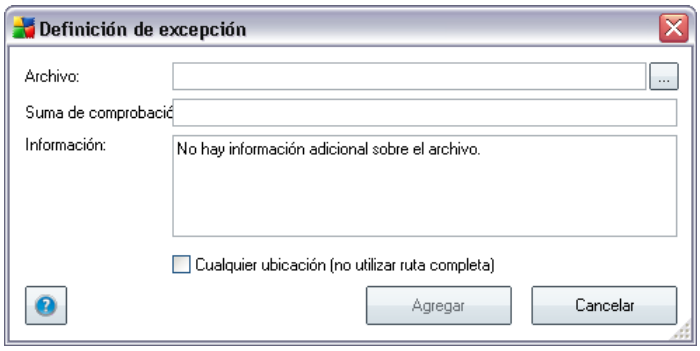

El diálogo ***Excepciones de Programas potencialmente no deseados*** muestra una

lista de excepciones definidas y válidas de programas potencialmente no deseados. Puede editar la lista, eliminar elementos existentes o agregar nuevas excepciones. En la lista, puede encontrar la siguiente información sobre cada excepción:

- ***Archivo***: proporciona el nombre de la aplicación en cuestión
- ***Ruta de acceso del archivo***: muestra el camino a la ubicación de la aplicación
- ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de verificación es una cadena de caracteres generados automáticamente que permite a AVG distinguir de manera inequívoca los archivos elegidos de otros archivos. La suma de verificación se genera y se muestra después de haber agregado el archivo correctamente.

## Botones de control

- ***Editar***: abre un cuadro de diálogo de edición (*idéntico al cuadro de diálogo para la definición de una nueva excepción, consulte a continuación*) para una excepción definida, donde puede cambiar los parámetros de la excepción
- ***Eliminar***: elimina el elemento seleccionado de la lista de excepciones
- ***Agregar excepción***: abre un cuadro de diálogo de edición en el cual es posible definir parámetros para una excepción que se creará:



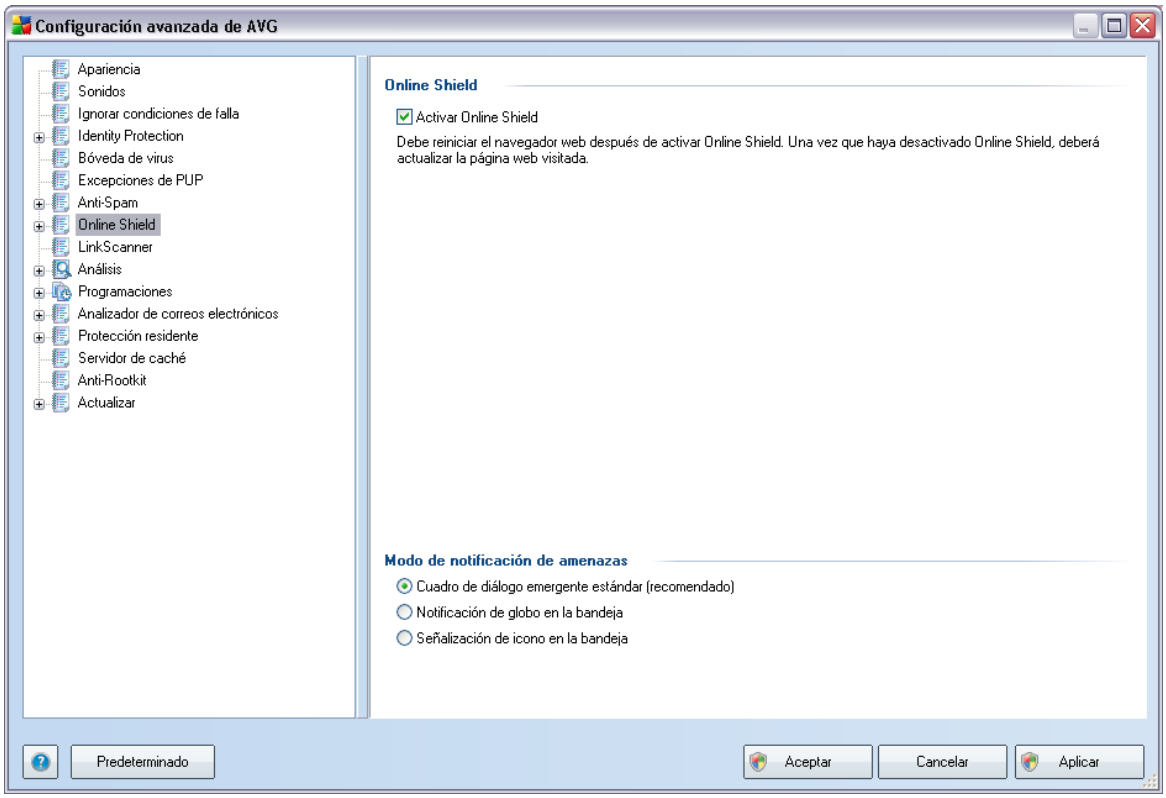

  - ***Archivo***: introduzca la ruta completa del archivo que desea marcar como una excepción
  - ***Suma de comprobación***: muestra la "firma" única del archivo elegido. Esta suma de verificación es una cadena de caracteres generados automáticamente que permite a AVG distinguir de manera inequívoca los archivos elegidos de otros archivos. La suma de verificación se genera y

se muestra después de haber agregado el archivo correctamente.

- ***Información del archivo***: muestra cualquier información disponible acerca del archivo (*información de licencia, versión, etc.*)

- ***Cualquier ubicación (no utilizar ruta completa)*** si desea definir este archivo como una excepción sólo para la ubicación específica, deje esta casilla sin marcar

## 10.6. Online Shield




El cuadro de diálogo ***Protección Web*** le permite activar o desactivar el componente ***Online Shield*** mediante la opción ***Activar Online Shield*** (*activada de forma predeterminada*). Para ver más opciones de configuración avanzada de este componente, continúe con los cuadros de diálogo posteriores que se muestran en la navegación de árbol:

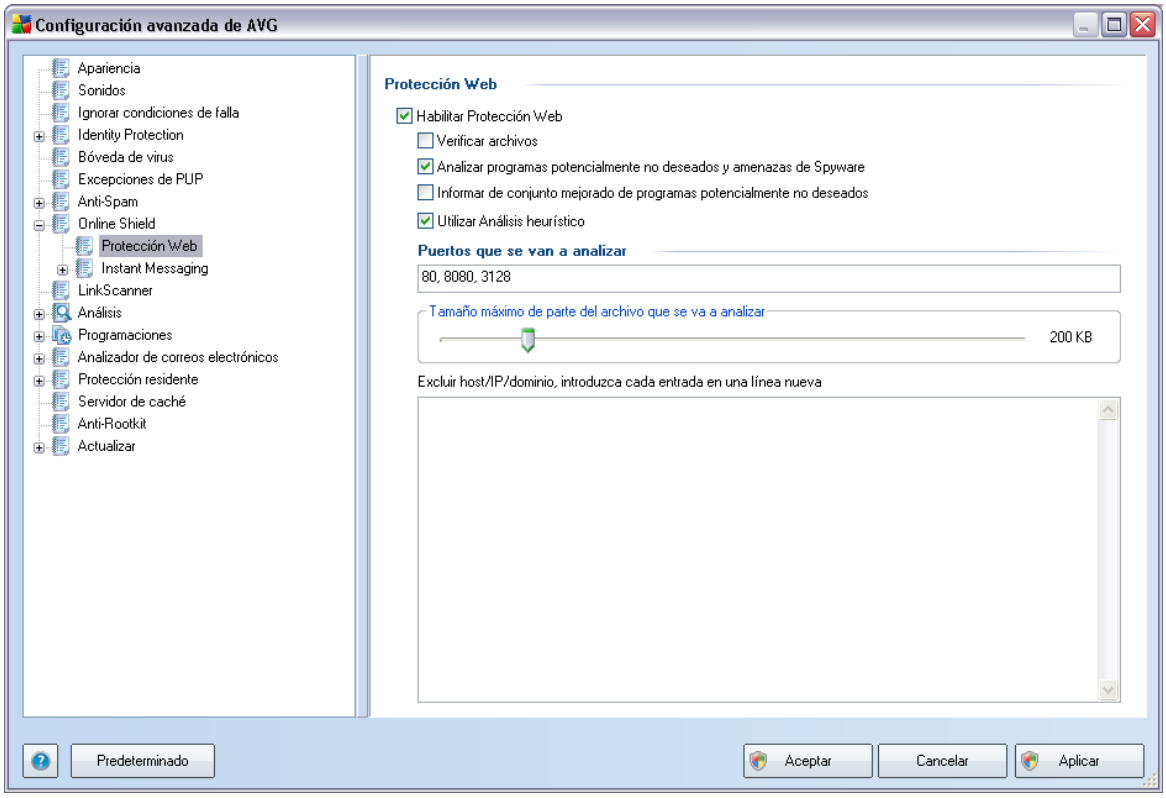
- ***Protección Web***

- ***Mensajería instantánea***

### Modo de notificación de amenazas

En la sección inferior del cuadro de diálogo, seleccione de qué forma desea estar informado acerca de posibles amenazas detectadas: mediante un cuadro de diálogo emergente estándar, mediante notificación de globo en la bandeja de sistema o mediante información en el icono de la bandeja de sistema.

## 10.6.1. Protección Web




En el cuadro de diálogo ***Protección Web*** puede editar la configuración del componente en relación con el análisis del contenido de sitios web. La interfaz de edición permite configurar las opciones básicas siguientes:

- ***Habilitar Protección Web***: esta opción confirma que ***Online Shield*** debe analizar el contenido de las páginas Web. Mientras esta opción esté seleccionada (*valor predeterminado*), podrá activar o desactivar estos

elementos:

- ***Examinar archivos***: analiza el contenido de los archivos que pudieran existir en la página Web que se visualizará.

- ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione esta opción para activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

- ***Utilizar método heurístico***: analiza el contenido de la página que se visualizará utilizando el método de análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).

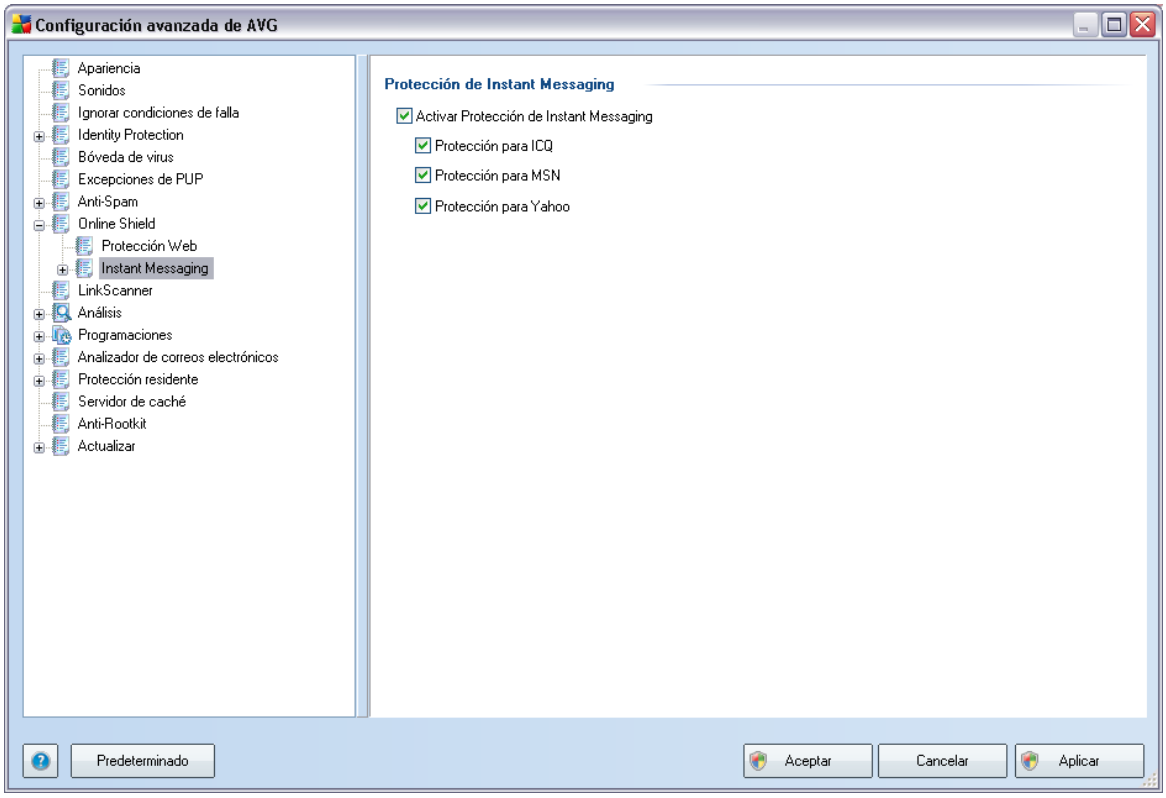
- ***Puertos que se van a analizar***: este campo indica los números de puerto de comunicación http estándar. Si la configuración de su equipo es diferente, puede modificar los números de puertos según sea necesario.

- ***Tamaño máximo de parte del archivo que se va a analizar***: si los archivos incluidos están presentes en la página visualizada, también puede analizar su contenido incluso antes de que se descarguen en el equipo. Sin embargo, el análisis de archivos grandes toma bastante tiempo y es posible que la descarga de la página web se ralentice de modo notable. Puede emplear la barra deslizante para especificar el tamaño máximo de archivo que se analizará con ***Online Shield***. Aunque el tamaño del archivo descargado sea superior al valor especificado, y por consiguiente no se analice con Online Shield, seguirá estando protegido: si el archivo está infectado, la ***Protección residente*** lo detectará de

inmediato.

- ***Excluir host/IP/dominio***: en el campo de texto puede escribir el nombre exacto de un servidor (*host, dirección IP, dirección IP con máscara o URL*) o un dominio que ***Online Shield*** *no debe analizar.* Por lo tanto excluya sólo el host del que esté absolutamente seguro de que nunca le proveerá de contenido de sitio Web peligroso.

## 10.6.2. Mensajería instantánea



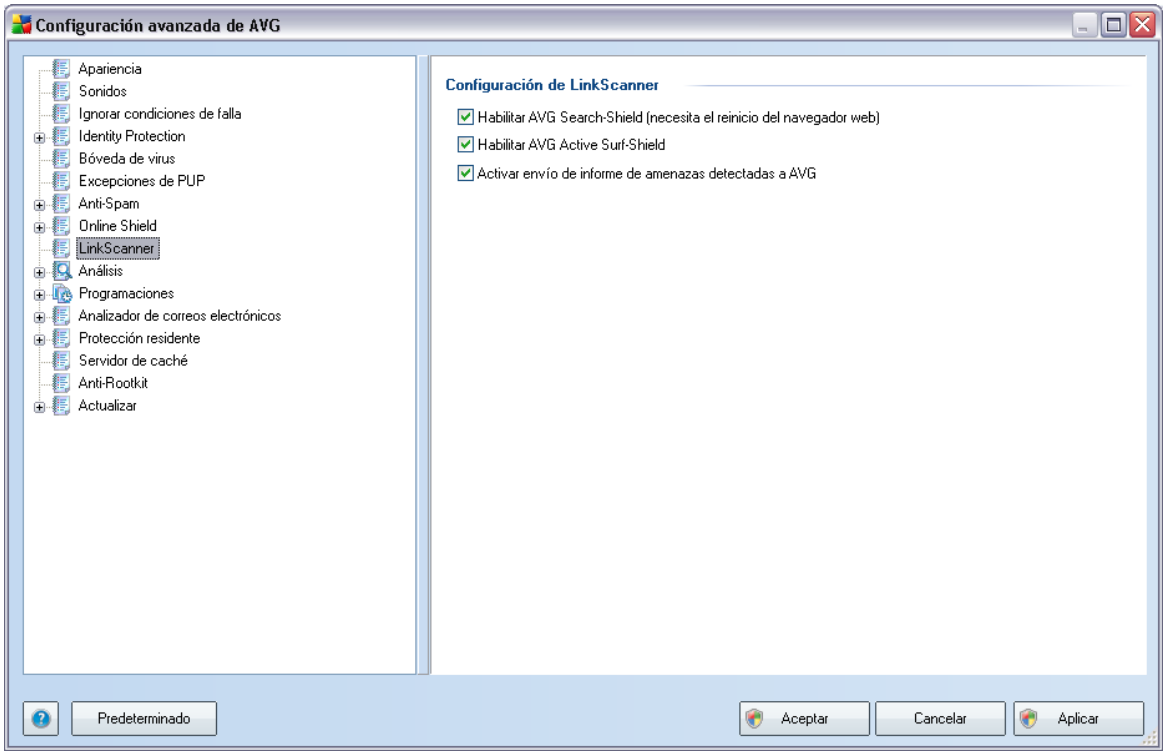

En el cuadro de diálogo ***Protección de mensajería instantánea*** puede editar la configuración del componente ***Online Shield*** relativa al análisis de la mensajería instantánea. Actualmente sólo se admiten tres programas de mensajería instantánea: ***ICQ***, ***MSN*** y ***Yahoo***: marque el elemento correspondiente a cada uno de ellos si desea que ***Online Shield*** compruebe que la comunicación en línea no contiene virus.

Para obtener una especificación más detallada de los usuarios permitidos y bloqueados, puede ver y editar el cuadro de diálogo correspondiente (***ICQ avanzado***, ***MSN avanzado o Yahoo avanzado***) y especificar la ***Lista de remitentes autorizados*** (

*lista de usuarios a los que se permitirá la comunicación con su equipo*) y la ***Lista de remitentes no autorizados***(*usuarios que se bloquearán*).

## 10.7. Link Scanner

El cuadro de diálogo ***Configuración de LinkScanner*** le permite activar o desactivar las funciones básicas de ***LinkScanner***:




- ***Activar la Protección de búsqueda AVG*** (*seleccionada de modo predeterminado*): iconos asesores de notificación en las búsquedas efectuadas en Google, Yahoo, Bing, Yandex, Altavista o Baidu que verifican por adelantado el contenido de los sitios devuelto por el motor de búsqueda.

- ***Activar la Protección de navegación activa AVG*** (*activada de manera predeterminada*): protección (*en tiempo real*) activa contra sitios de explotación cuando se tiene acceso a ellos. Las conexiones a los sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario accede a ellos a través de un navegador Web (*o cualquier otra aplicación que utilice HTTP*).

- ***Activar envío de informe de amenazas detectadas a AVG*** (*activado de forma predeterminada*): seleccione este elemento para permitir que el usuario informe acerca de los sitios peligrosos y de vulnerabilidades encontrados mediante ***Protección de navegación activa AVG*** o ***Protección de búsqueda AVG*** y ampliar así la información de la base de datos acerca de la actividad maliciosa en la Web.

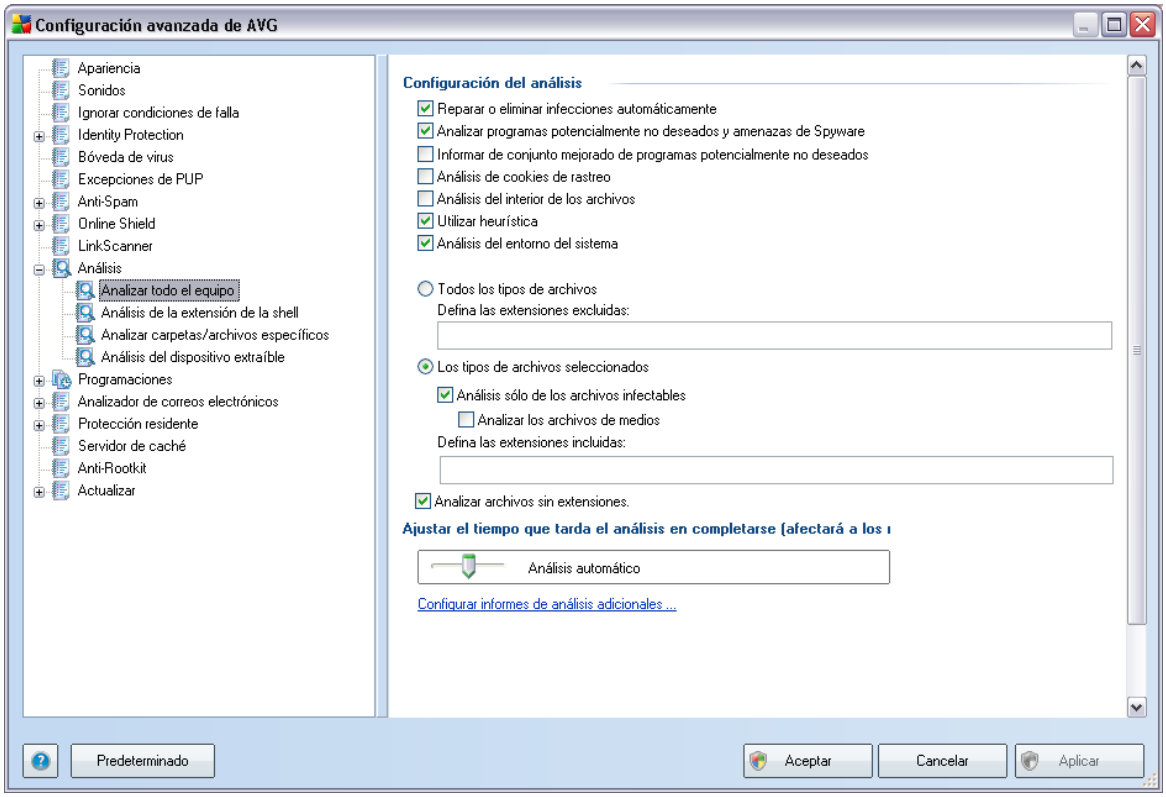
## 10.8. Análisis

La configuración avanzada del análisis se divide en tres categorías con referencia a los tipos específicos de análisis definidos por el proveedor del software:

- ***Analizar todo el equipo*** : análisis estándar predefinido de todo el equipo
- ***Análisis de extensión de la Shell*** : análisis específico de un objeto seleccionado directamente del entorno del Explorador de Windows
- ***Analizar archivos o carpetas específicos***: análisis estándar predefinido de áreas seleccionadas del equipo
- ***Análisis de dispositivos extraíbles***: análisis específico de dispositivos extraíbles conectados a su equipo

## 10.8.1. Analizar todo el equipo

La opción ***Analizar todo el equipo*** permite editar los parámetros de uno de los análisis predefinidos por el proveedor de software, ***Análisis de todo el equipo***:




### Configuración del análisis

La sección ***Configuración del análisis*** ofrece una lista de parámetros de análisis que se pueden activar y desactivar:

- ***Reparar o eliminar infecciones automáticamente***: si se identifica un virus durante el análisis, se puede reparar automáticamente si existe una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la ***Bóveda de virus***.

- ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione esta opción para activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de

virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

- ***Analizar cookies de rastreo***: este parámetro del componente Anti-Spyware define que las cookies deben detectarse; (*las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de sitios o el contenido de su carrito de compras electrónico*).

- ***Análisis del interior de los archivos***: este parámetro define que el análisis debe examinar todos los archivos, incluso los archivos internos almacenados (por ejemplo, ZIP, RAR...).

- ***Utilizar método heurístico***: el análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*) será uno de los métodos empleados para la detección de virus durante el análisis.

- ***Analizar el entorno del sistema***: el análisis también examinará las áreas del sistema de su equipo.

Después sería conveniente decidir si desea analizar

- ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas (*una vez guardado, la coma pasa a ser punto y coma*);

- ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia ( *archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede

especificar las extensiones de los archivos que siempre deben analizarse.

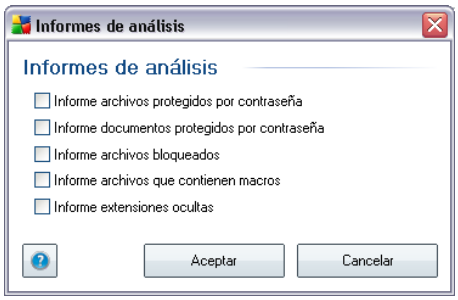
- En forma opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

### Prioridad del proceso de análisis

Dentro de la sección ***Prioridad del proceso de análisis*** se puede especificar de manera adicional la velocidad de análisis deseada dependiendo del empleo de recursos del sistema. De manera predeterminada, el valor de esta opción está establecido en el nivel medio de empleo automático de recursos. Si desea que el análisis se realice a más velocidad, tardará menos tiempo pero el uso de recursos del sistema aumentará de modo notable durante el análisis, y el resto de actividades del PC se ralentizará ( *esta opción se puede emplear cuando el equipo está encendido pero no hay nadie trabajando en él*). Por otra parte, puede reducir el uso de recursos del sistema prolongando la duración del análisis.

### Configurar informes de análisis adicionales ...

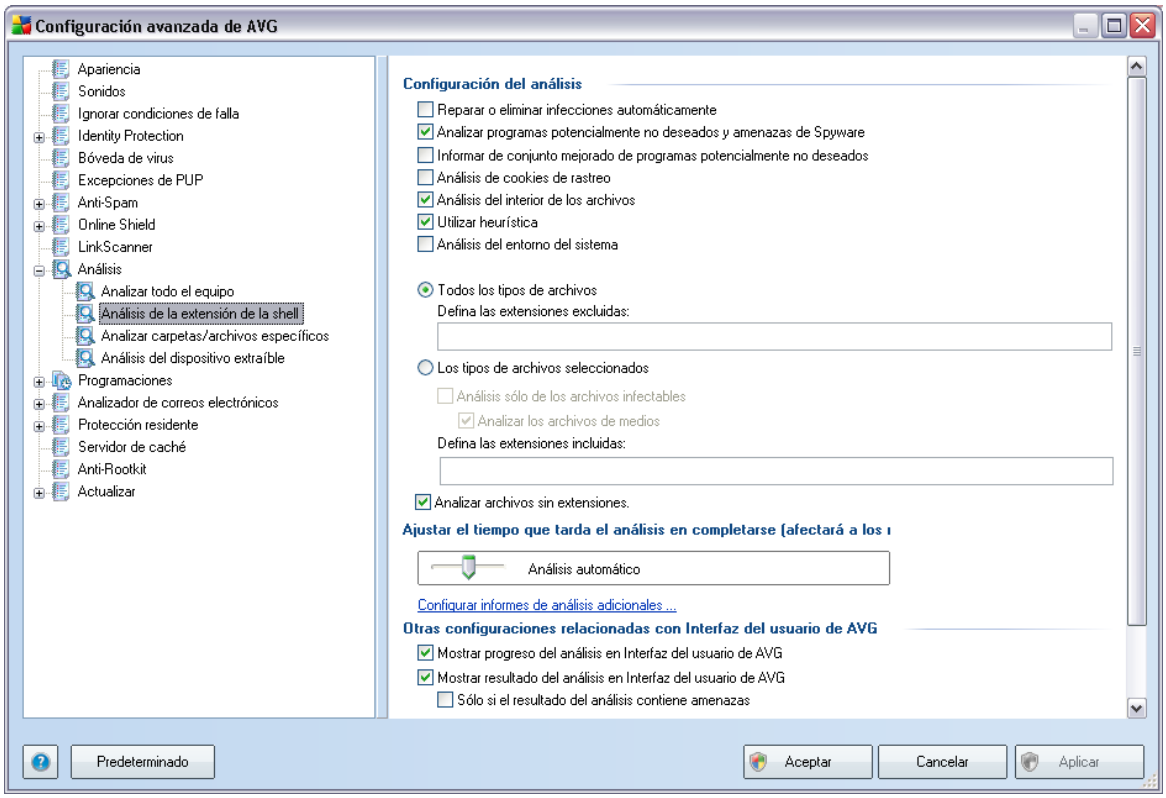
Haga clic en el vínculo ***Configurar informes de análisis adicionales...*** para abrir una ventana de diálogo denominada ***Informes de análisis*** donde puede marcar varios elementos para definir de qué hallazgos se debería informar:




## 10.8.2. Análisis de extensión de la shell

De modo parecido al anterior elemento ***Analizar todo el equipo***, este elemento denominado ***Análisis de extensión de la shell*** también ofrece varias opciones para editar el análisis predefinido por el proveedor de software. En esta ocasión, la configuración está relacionada con el análisis de objetos específicos ejecutados

directamente desde el entorno del Explorador de Windows (*extensión de la shell*); consulte el capítulo ***Análisis en el Explorador de Windows***:

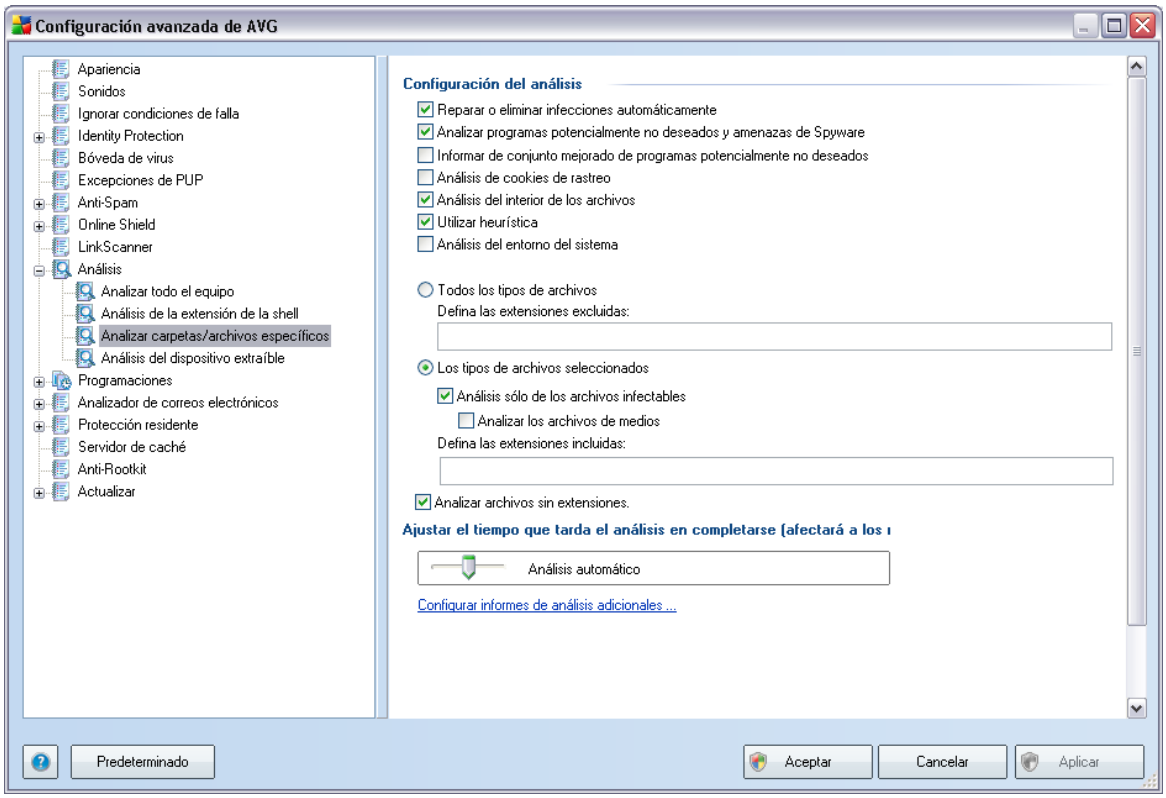



La lista de parámetros muestra parámetros idénticos a los que están disponibles en ***Análisis de todo el equipo***. Sin embargo, la configuración predeterminada varía: con ***Análisis de todo el equipo*** la mayoría de los parámetros están seleccionados, mientras que con ***Análisis de extensión de la shell*** (***Análisis en el Explorador de Windows***) sólo están seleccionados los parámetros relevantes.

***Nota:****Para obtener una descripción de los parámetros específicos, consulte el capítulo* ***Configuración avanzada de AVG/Análisis/Análisis de todo el equipo****.*

## 10.8.3. Analizar carpetas o archivos específicos

La interfaz de edición para***analizar carpetas o archivos específicos*** es idéntica al diálogo de edición para ***analizar todo el equipo*** Todas las opciones de configuración son iguales; sin embargo, la configuración predeterminada es más estricta para el ***análisis de todo el equipo***:

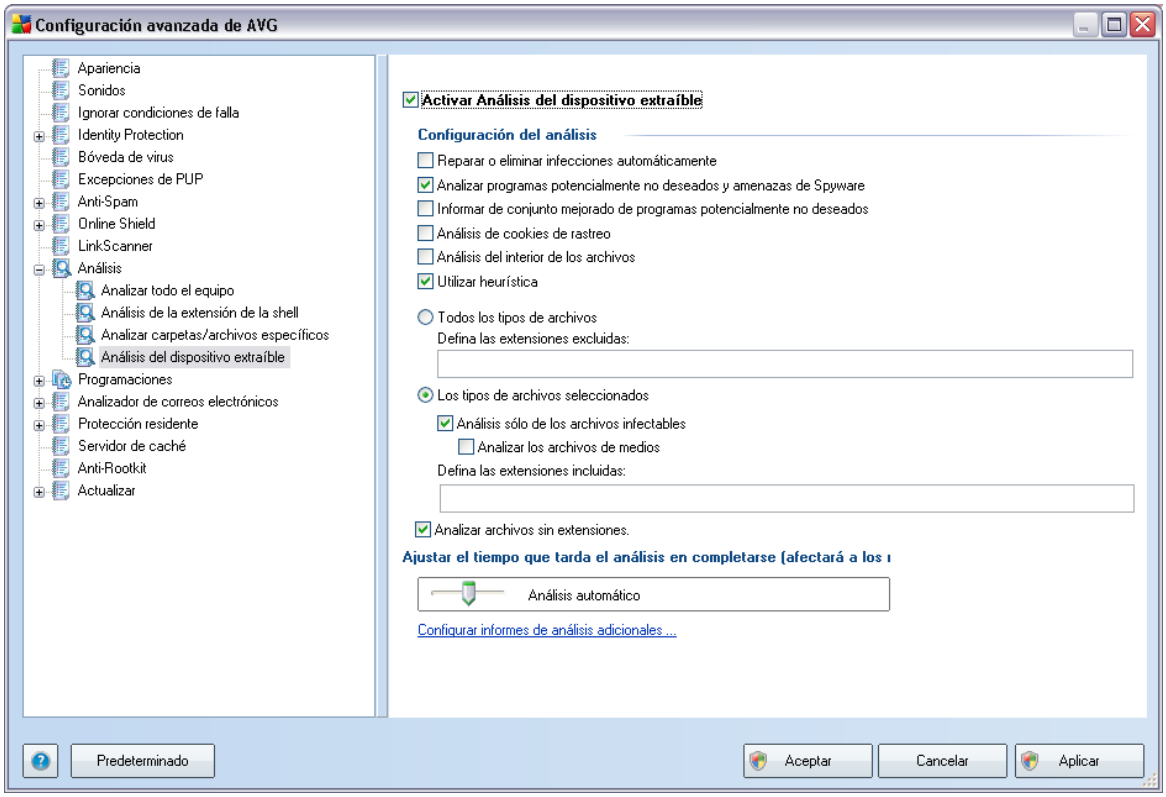



Todos los parámetros definidos en este cuadro de diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con ***Análisis de archivos o carpetas específicos***.

***Nota:****Para obtener una descripción de los parámetros específicos, consulte el capítulo* ***Configuración avanzada de AVG/Análisis/Análisis de todo el equipo****.*

## 10.8.4. Análisis de dispositivos extraíbles

La interfaz de edición para ***Análisis del dispositivo extraíble*** también es muy parecida al diálogo de edición ***Analizar todo el equipo***.




El ***Análisis del dispositivo extraíble*** se inicia automáticamente cada vez que conecta algún dispositivo extraíble a su equipo. De forma predeterminada, este análisis está desactivado. Sin embargo, es crucial analizar los dispositivos extraíbles en busca de amenazas potenciales, ya que éstos son una fuente importante de infección. Para tener este análisis listo y activarlo de forma automática cuando sea necesario, marque la opción ***Activar análisis de dispositivos extraíbles***.

***Nota:****Para obtener una descripción de los parámetros específicos, consulte el capítulo* ***Configuración avanzada de AVG/Análisis/Análisis de todo el equipo****.*

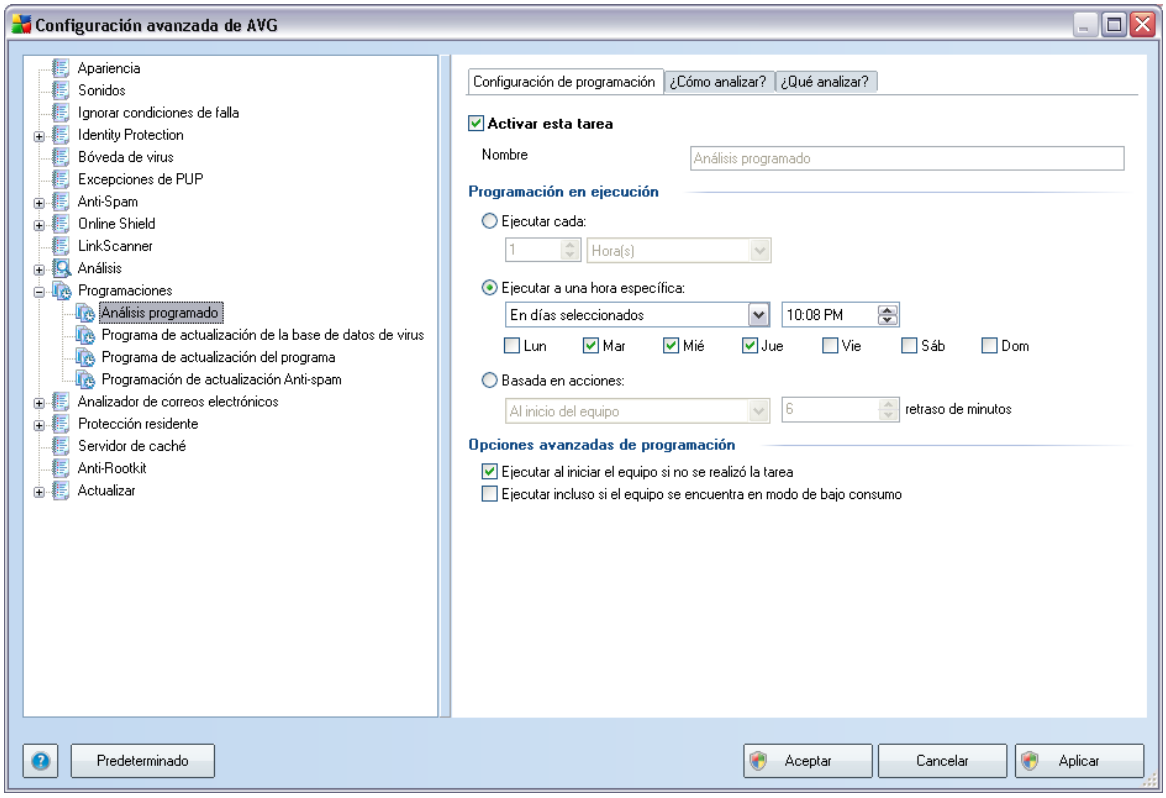
## 10.9. Programaciones

En la sección ***Programas*** puede editar la configuración predeterminada de:

- Programación de análisis de todo el equipo
- Programación de actualización de la base de datos de virus
- Programación de actualización del programa

### 10.9.1. Análisis programado

Los parámetros del análisis programado se pueden editar (*o se puede configurar una nueva programación*) en tres pestañas:




En la pestaña ***Configuración de programación*** puede seleccionar o cancelar la selección del elemento ***Activar esta tarea*** para desactivar el análisis programado de

forma temporal, y volverlo a activar cuando sea necesario.

A continuación, en el campo de texto denominado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*), se encuentra el nombre asignado a esta misma programación por el proveedor del programa. Para programaciones agregadas recientemente (*puede agregar una nueva programación haciendo clic con el botón secundario del mouse en el elemento* ***Análisis programado*** *en el árbol de navegación izquierdo*), puede especificar su propio nombre, y en ese caso el campo de texto se abrirá para que lo edite. Intente utilizar nombres cortos, descriptivos y adecuados para los análisis a fin de distinguirlos después fácilmente.

***Ejemplo:****no es adecuado llamar al análisis por el nombre "Nuevo análisis" o "Mi análisis" ya que estos nombres no hacen referencia a lo que el análisis realmente verifica. En cambio, un ejemplo de un buen nombre descriptivo sería "Análisis de áreas del sistema", etc. Además, no es necesario especificar en el nombre del análisis si es el análisis de todo el sistema o solo de archivos o carpetas seleccionados; sus propios análisis siempre serán una versión específica del análisis de archivos o carpetas seleccionados.*

En este diálogo puede definir con más detalle los siguientes parámetros del análisis:

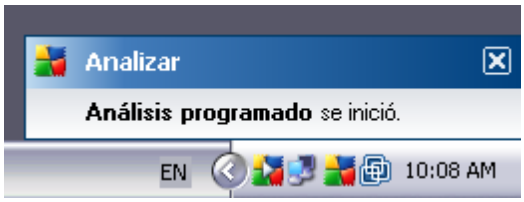
## Programación en ejecución

Aquí, puede especificar los intervalos de tiempo para la ejecución del análisis programado recientemente. El tiempo se puede definir con la ejecución repetida del análisis tras un periodo de tiempo determinado (***Ejecutar cada...***), estableciendo una fecha y una hora exactas (***Ejecutar a un intervalo específico de tiempo...***) o estableciendo un evento al que debe estar asociada la ejecución del análisis (***Acción basada en el inicio del equipo***).

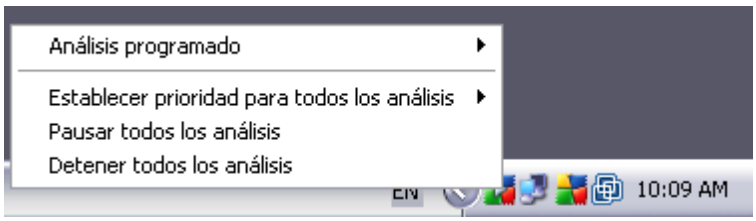
## Opciones avanzadas de programación

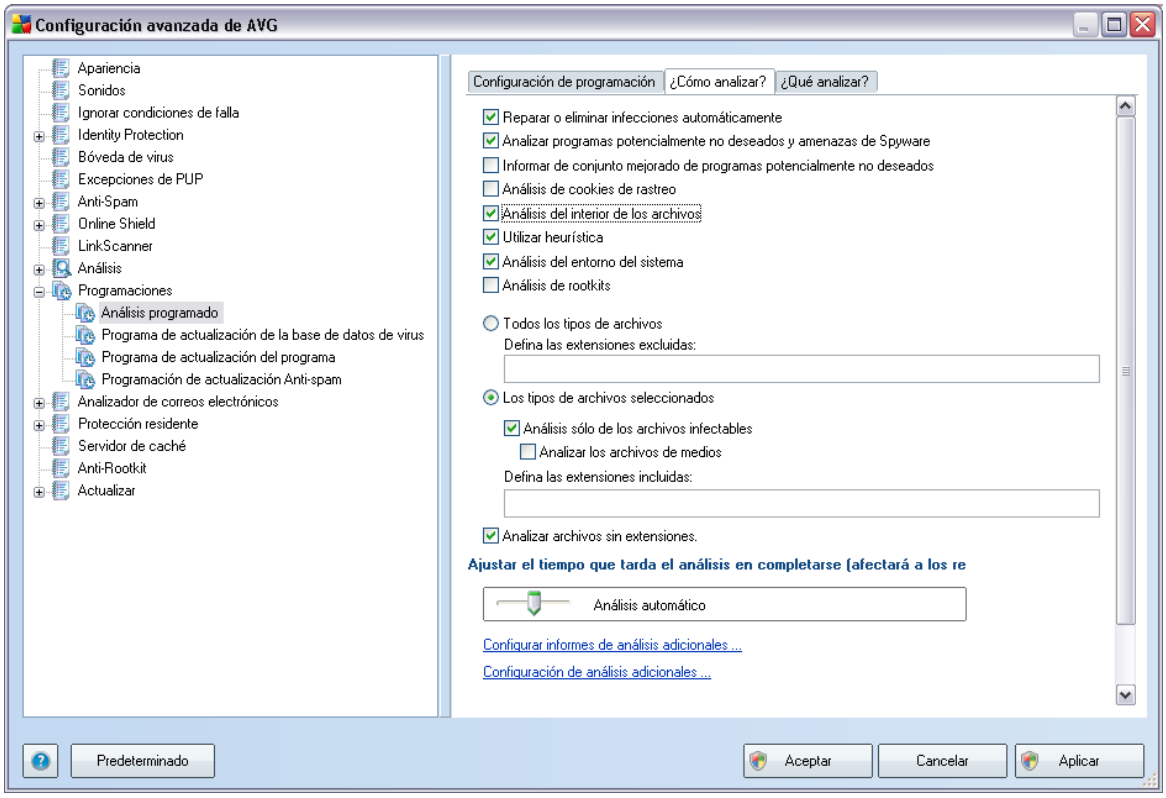
Esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

Una vez que se inicia el análisis programado en la hora que se especificó, se le informará de este hecho mediante una ventana emergente que se abre sobre el Icono en la bandeja de sistema AVG:




A continuación aparece un nuevo Icono en la bandeja de sistema AVG (*a todo color con una flecha blanca; vea la figura anterior*) informando que se está ejecutando un análisis programado. Haga clic con el botón secundario en el icono de ejecución del análisis AVG para abrir un menú de contexto donde puede decidir pausar o detener la ejecución del análisis:






En la pestaña ***Cómo analizar*** se encontrará una lista de parámetros de análisis que de manera opcional se pueden activar/desactivar. De manera predeterminada, la mayoría de los parámetros están activados y su funcionamiento se aplicará durante el análisis. A menos que se cuente con una razón válida para cambiar esta configuración recomendamos mantenerla:

- ***Reparar o eliminar infecciones automáticamente***: si se identifica un virus durante el análisis, se puede reparar automáticamente si existe una cura disponible. Si no se puede reparar automáticamente el archivo infectado, el objeto infectado se trasladará a la ***Bóveda de Virus***.

- ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*seleccionada de modo predeterminado*): seleccione la opción para activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

- ***Analizar cookies de rastreo*** (*activado de manera predeterminada*): este parámetro del componente ***Anti-Spyware*** define que deben detectarse cookies durante el análisis (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica acerca de los usuarios, como los sitios que prefieren o los contenidos de sus carritos de compra electrónicos*)

- ***Análisis del interior de los archivos*** : (*activado, de manera predeterminada* ): este parámetro define que el análisis debe comprobar todos los archivos, aún aquellos que se encuentran comprimidos dentro de algún tipo de archivo, por ejemplo ZIP, RAR, ...

- ***Utilizar método heurístico*** (*activado, de manera predeterminada*): la emulación dinámica del análisis heurístico (*de las instrucciones del objeto analizadoen el entorno virtual del equipo*) será uno de los métodos empleados para la detección de virus durante el análisis;

- ***Analizar el entorno del sistema*** : (*activado, de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo;

- ***Analizar en busca de rootkits***: marque este elemento si desea incluir la detección de rootkits en el análisis de todo el equipo. La detección de rootkits también está disponible de forma independiente en el componente ***Anti-Rootkit;***

Después sería conveniente decidir si desea analizar

- ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas (*una vez guardado, la coma pasa a ser punto y coma*);

- ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia ( *archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más*

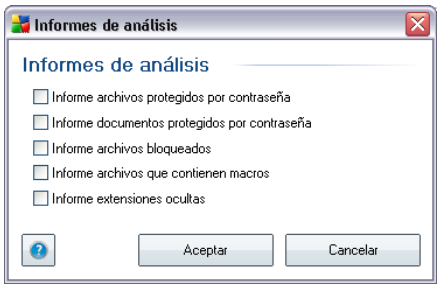
*el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

- En forma opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

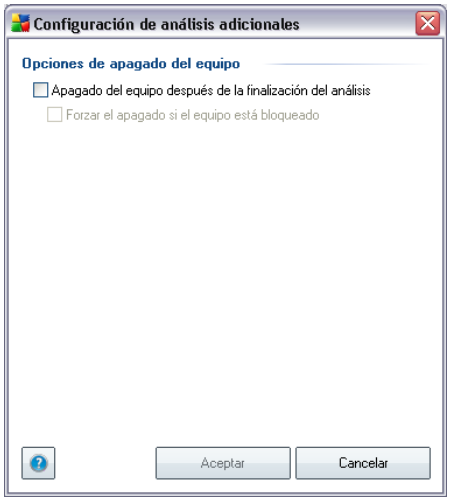
## Prioridad del proceso de análisis

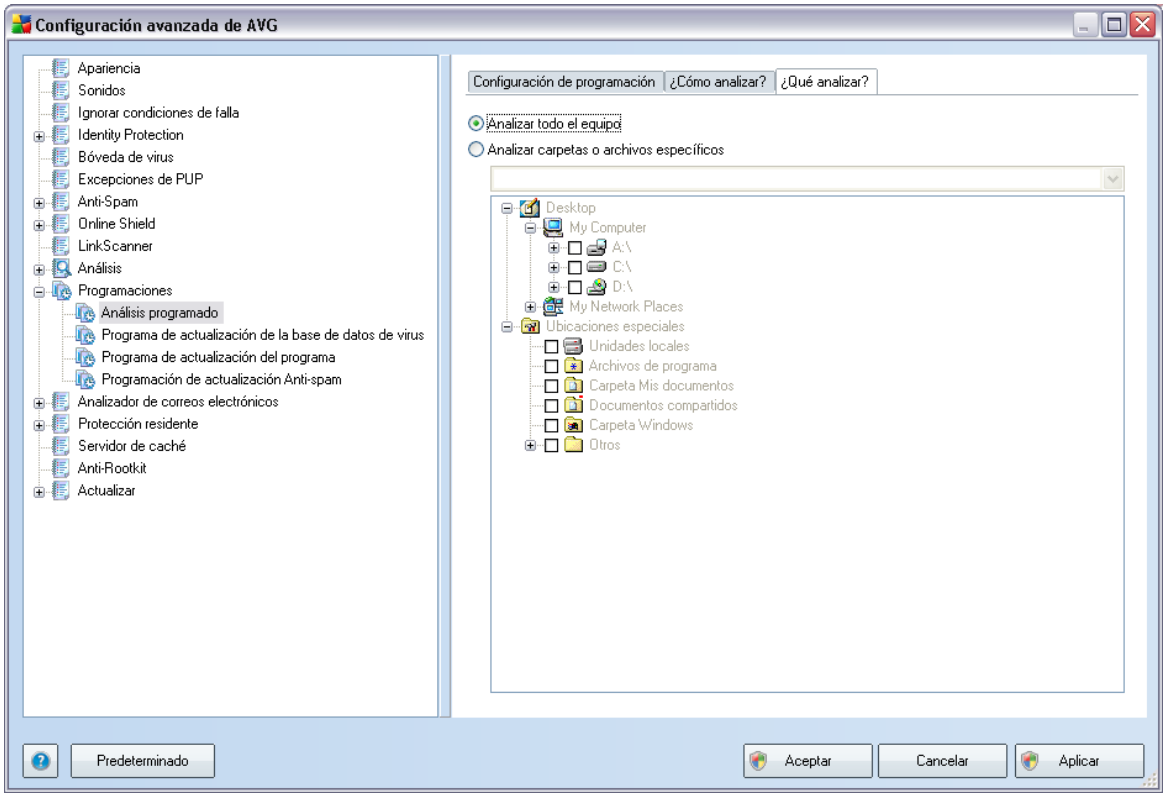
Dentro de la sección ***Prioridad del proceso de análisis*** se puede especificar de manera adicional la velocidad de análisis deseada dependiendo del empleo de recursos del sistema. De manera predeterminada, esta opción está establecida en el nivel medio de empleo automático de recursos. Si desea que el análisis se realice a más velocidad, tardará menos tiempo pero el uso de recursos del sistema aumentará de modo notable durante el análisis, y el resto de actividades del equipo se ralentizará (*esta opción se puede emplear cuando el equipo está encendido pero no hay nadie trabajando en él*). Por otro lado, puede reducir el uso de recursos del sistema prolongando la duración del análisis.

Haga clic en el vínculo ***Configurar informes de análisis adicionales...*** para abrir una ventana de diálogo denominada ***Informes de análisis*** donde puede marcar varios elementos para definir de qué hallazgos se debería informar:




Haga clic en ***Configuración de análisis adicional***para abrir un nuevo diálogo de ***Opciones de apagado del equipo***, donde puede decidir si el equipo se debería apagar automáticamente en cuanto haya finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

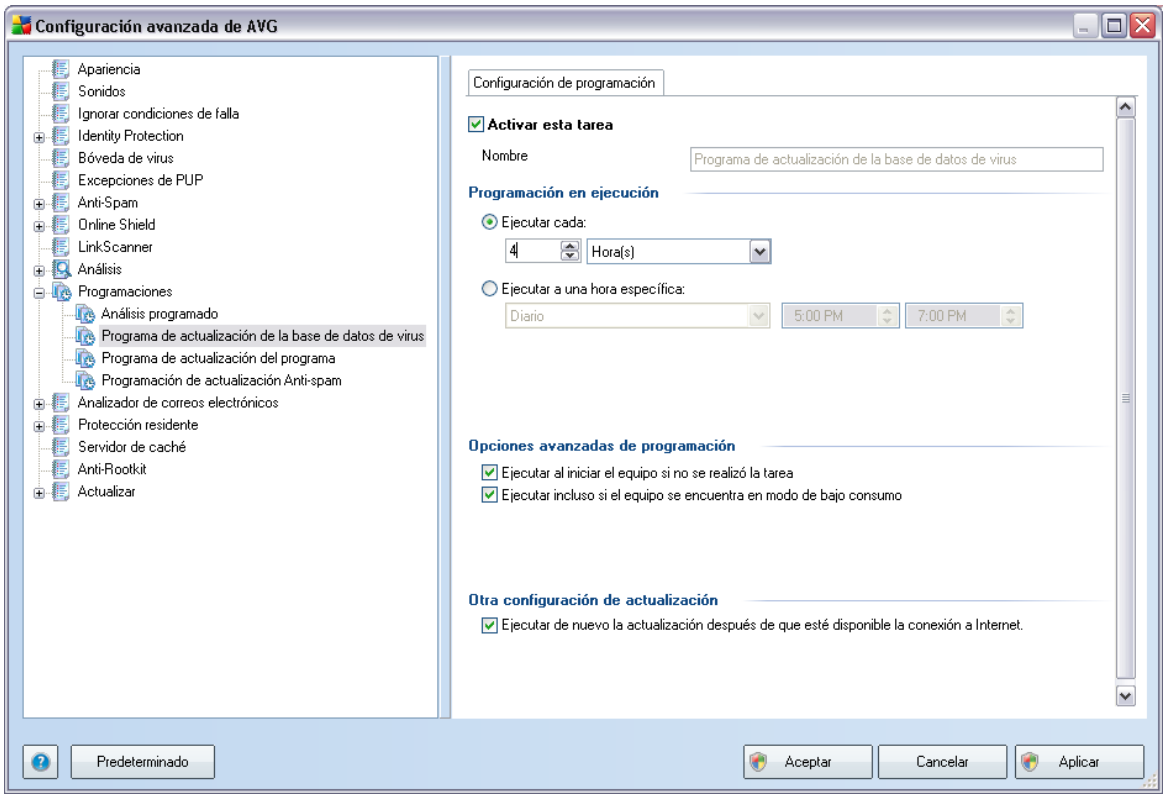



En la pestaña ***Qué analizar***puede definir si desea programar el análisis de todo el

equipo o el análisis de archivos o carpetas específicos. Si selecciona analizar archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activará la estructura de árbol visualizada y podrá especificar las carpetas que se analizarán.

## 10.9.2. Programación de actualización de la base de datos de virus




En la pestaña ***Configuración de programación*** puede seleccionar o cancelar la selección del elemento ***Activar esta tarea*** para desactivar la actualización de la base de datos de virus programada de forma temporal, y volverla a activar cuando sea necesario. La programación de actualización básica de la base de datos de virus se trata en el componente***Administrador de actualizaciones***. En este diálogo puede configurar algunos parámetros detallados de la programación de actualización de la base de datos de virus. En el campo de texto denominado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

### Programación en ejecución

En esta sección, especifique los intervalos de tiempo para la ejecución de la actualización de la base de datos de virus programada recientemente. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto periodo de tiempo (***Ejecutar cada...***) o definiendo una fecha y hora exactas ( ***Ejecutar a un intervalo específico de tiempo...***).

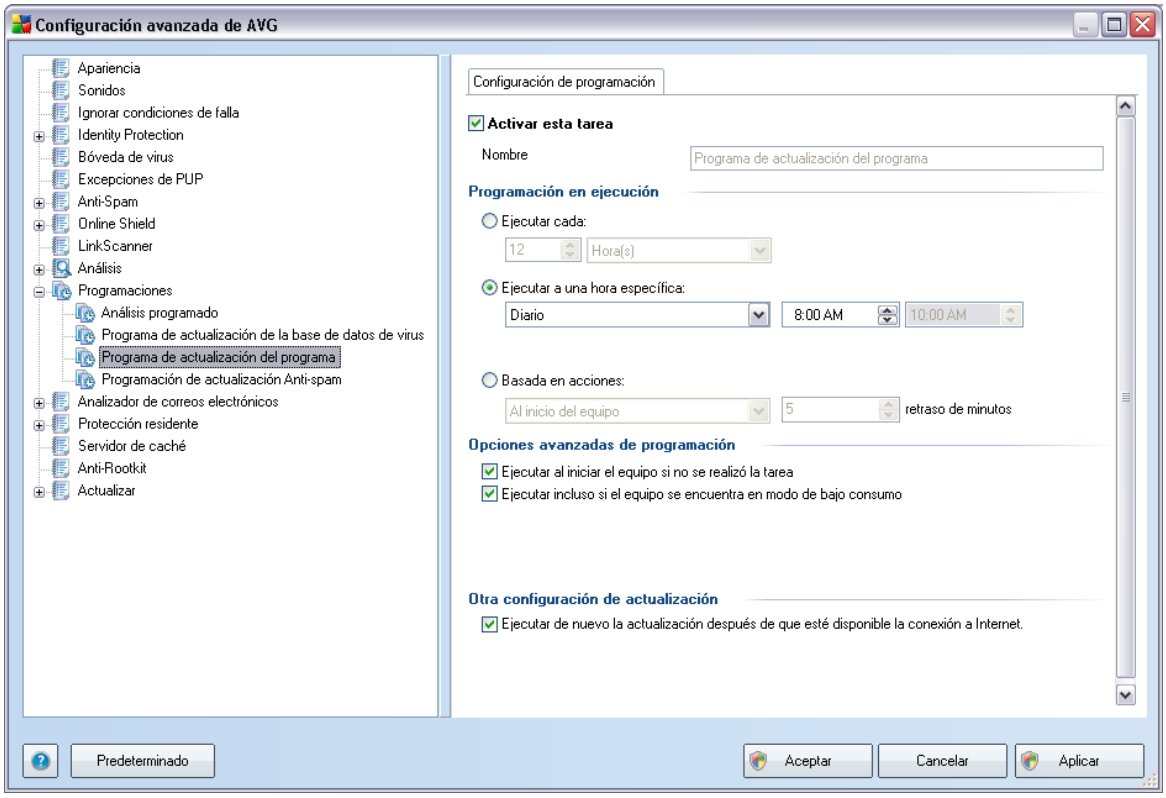
## Opciones avanzadas de programación

Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización de la base de datos de virus si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

## Otra configuración de actualización

Finalmente, seleccione la opción ***Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet*** para asegurarse de que, en caso de que se interrumpa la conexión a Internet y se detenga el proceso de actualización, éste se vuelva a iniciar tan pronto se restablezca.

Una vez que se ejecuta la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el icono de la bandeja del sistema AVG (*siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo* ***Configuración avanzada/Apariencia****)*.




En la pestaña ***Configuración de programación*** puede seleccionar o cancelar la selección del elemento ***Activar esta tarea*** para desactivar la actualización programada de forma temporal, y volverla a activar cuando sea necesario. En el campo de texto denominado ***Nombre*** (*desactivado para todas las programaciones predeterminadas*) existe un nombre asignado a esta programación por el proveedor del programa.

## Programación en ejecución

Aquí, especifique los intervalos de tiempo para la ejecución de la actualización del programa recién programada. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto periodo de tiempo (***Ejecutar cada ...***), definiendo una fecha y hora exactas (***Ejecutar a una hora específica ...***) o posiblemente definiendo un evento con el que se debe asociar la ejecución de la actualización ( ***Acción basada en el inicio del equipo***).

## Opciones avanzadas de programación

Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización del programa si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

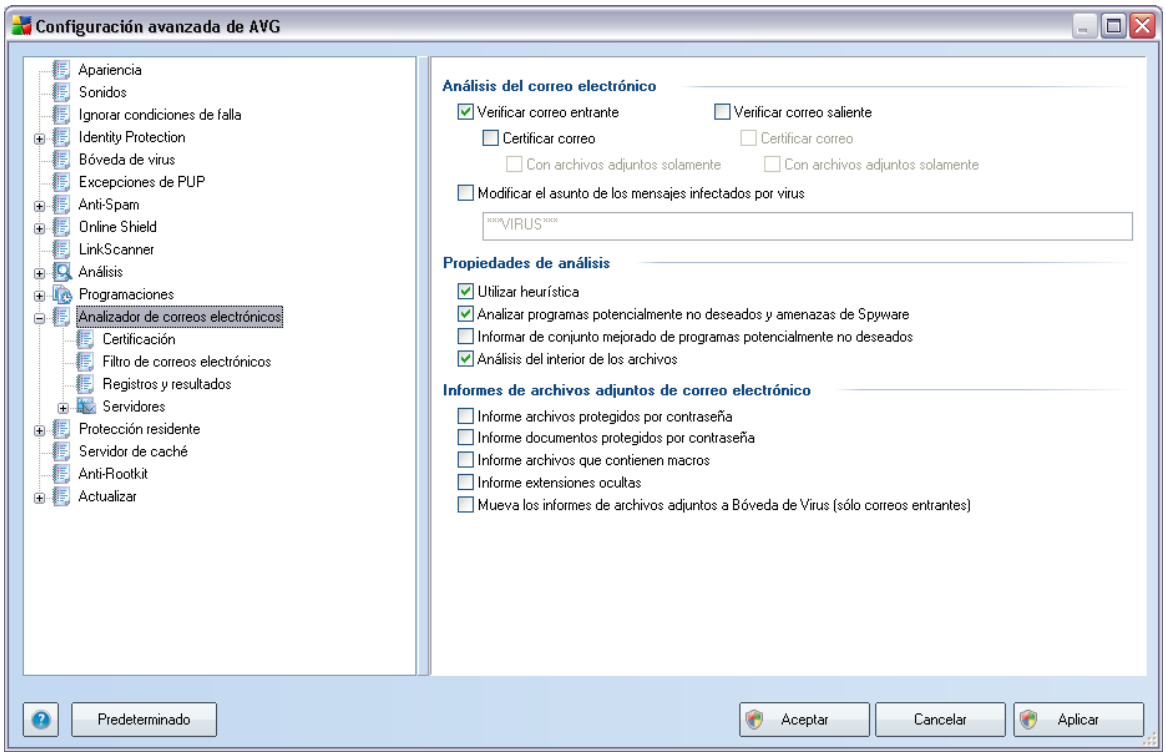
## Otra configuración de actualización

Seleccione la opción ***Ejecutar de nuevo la actualización tan pronto como esté disponible la conexión a Internet*** para asegurarse de que en caso de interrupción del proceso de actualización debido a una falla en la conexión a Internet, el proceso se reinicie inmediatamente después de recuperarla.

Una vez que se ejecuta la actualización programada en la hora que ha especificado, se le informará de este hecho mediante una ventana emergente en el icono de la bandeja del sistema AVG (*siempre y cuando haya conservado la configuración predeterminada del cuadro de diálogo* ***Configuración avanzada/Apariencia****)*.

***Nota:*** *si coinciden una actualización programada y un análisis programado al mismo tiempo, el proceso de actualización tendrá más prioridad, y por consiguiente se interrumpirá el proceso de análisis.*

## 10.10. Analizador de correos electrónicos




El diálogo ***Analizador de correos electrónicos*** se divide en tres secciones:

- ***Análisis del correo electrónico***: en esta sección puede establecer la siguiente configuración básica para los mensajes entrantes y/o salientes:
  - Si los mensajes de correo electrónico deben analizarse en busca de virus.
  - Si el texto de certificación debe agregarse al final de cada mensaje para afirmar que no contiene virus. El texto puede ajustarse en el cuadro de diálogo Certificación.
  - Si el texto de certificación sólo debe agregarse a mensajes con archivos adjuntos.

Para ***Modificar el asunto de mensajes infectados con virus***, marque la casilla y escriba el valor deseado en el campo de texto. Entonces se agregará al campo de asunto de cada mensaje de correo electrónico infectado con el fin de facilitar

la identificación y el filtrado. El valor predeterminado es ***VIRUS***, y recomendamos conservarlo.

- ***Propiedades de análisis***: en esta sección puede especificar cómo deben analizarse los mensajes.
    - ***Utilizar método heurístico***: seleccione esta opción para utilizar el método de detección heurístico al analizar los mensajes de correo electrónico. Cuando esta opción está activada, se pueden filtrar los archivos adjuntos de correo electrónico no sólo por extensión sino que también se considerará el contenido real del archivo adjunto. El filtro se puede establecer en el diálogo Filtro de correos electrónicos.
    - ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione la opción para activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.
    - ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.
    - ***Analizar el interior de los archivos***: seleccione para analizar el contenido de los archivos adjuntos a los mensajes de correo electrónico.
- ***Informes de archivos adjuntos de correo electrónico***: en esta sección se pueden establecer reportes adicionales acerca de archivos potencialmente peligrosos o sospechosos. Tenga en cuenta que no se mostrará cuadro de diálogo de advertencia, sólo se agregará un texto de certificación al final del mensaje de correo electrónico, y todos esos reportes se listarán en el cuadro de diálogo Detección mediante el Analizador de correos electrónicos:
    - ***Informar de los archivos protegidos por contraseña***: los archivos comprimidos (ZIP, RAR, etc.) protegidos por contraseña no se pueden analizar en busca de virus; seleccione la casilla para informar de ellos como potencialmente peligrosos.

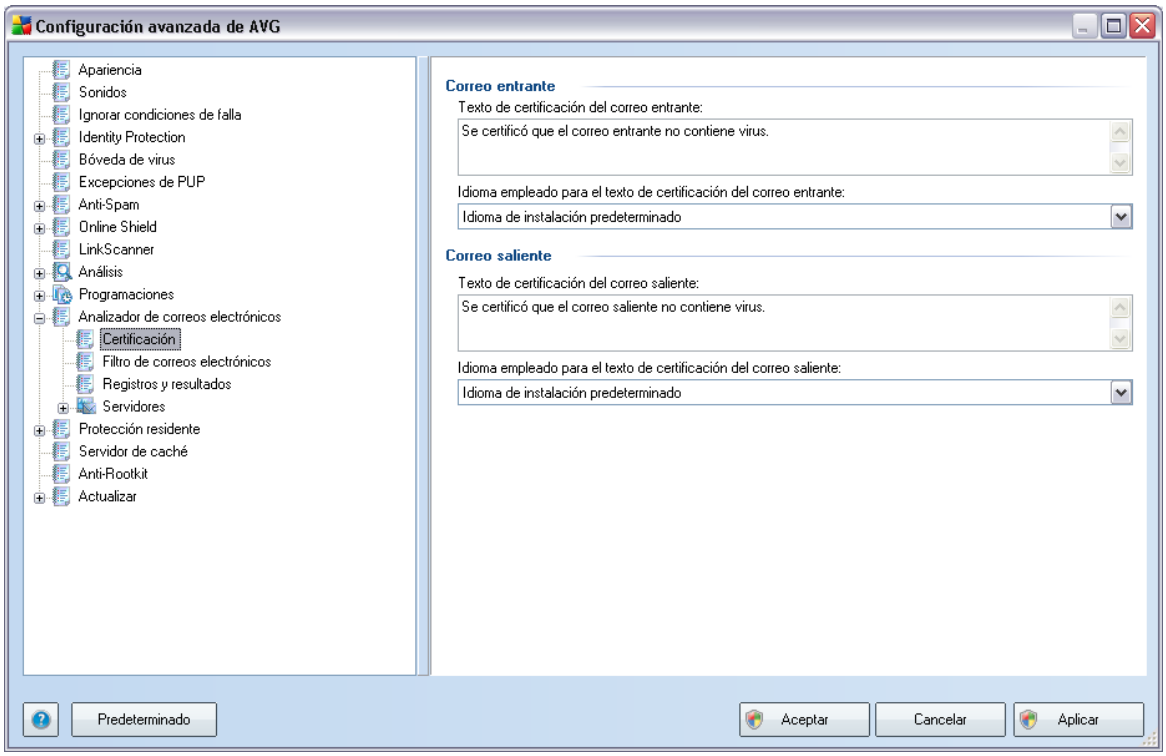
- ***Informar acerca de los documentos protegidos por contraseña***: no es posible analizar los documentos protegidos por contraseña en busca de virus; seleccione la casilla para informar de ellos como potencialmente peligrosos.

- ***Informar acerca de los archivos que contienen macros***: una macro es una secuencia predefinida de pasos encaminados a hacer que ciertas tareas sean más fáciles para el usuario (las macros de MS Word son ampliamente conocidas). Como tal, una macro puede contener instrucciones potencialmente peligrosas, y podría ser útil seleccionar la casilla para asegurar que los archivos con macros se reporten como sospechosos.

- ***Informar acerca de las extensiones ocultas***: la extensión oculta puede hacer, por ejemplo, que un archivo ejecutable sospechoso "algo.txt.exe" parezca como un archivo de texto simple inofensivo "algo.txt"; seleccione la casilla para informar de estos archivos como potencialmente peligrosos.

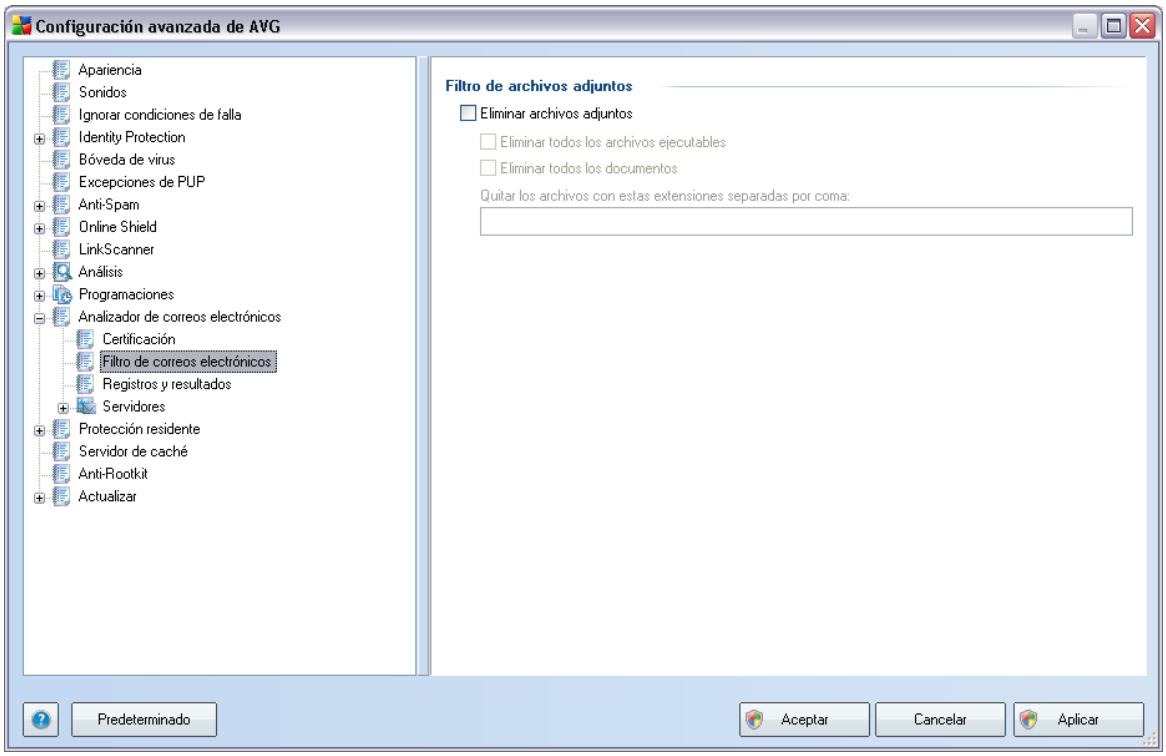
- ***Mover los archivos adjuntos reportados a la Bóveda de virus***: especifique si desea que se le notifique mediante correo electrónico acerca de los archivos protegidos con contraseña, los documentos protegidos por contraseña, los archivos que contienen macros y los archivos con extensión oculta detectados como un dato adjunto del mensaje del correo electrónico analizado. Si durante el análisis se identifica un mensaje en estas condiciones, defina si el objeto infeccioso detectado se debe mover a la ***Bóveda de virus***.

## 10.10.1. Certificación




En el diálogo ***Certificación*** puede especificar exactamente qué texto debe contener la nota de certificación y en qué idioma debe aparecer. Este valor debe especificarse por separado para ***Correo entrante*** y ***Correo saliente***.

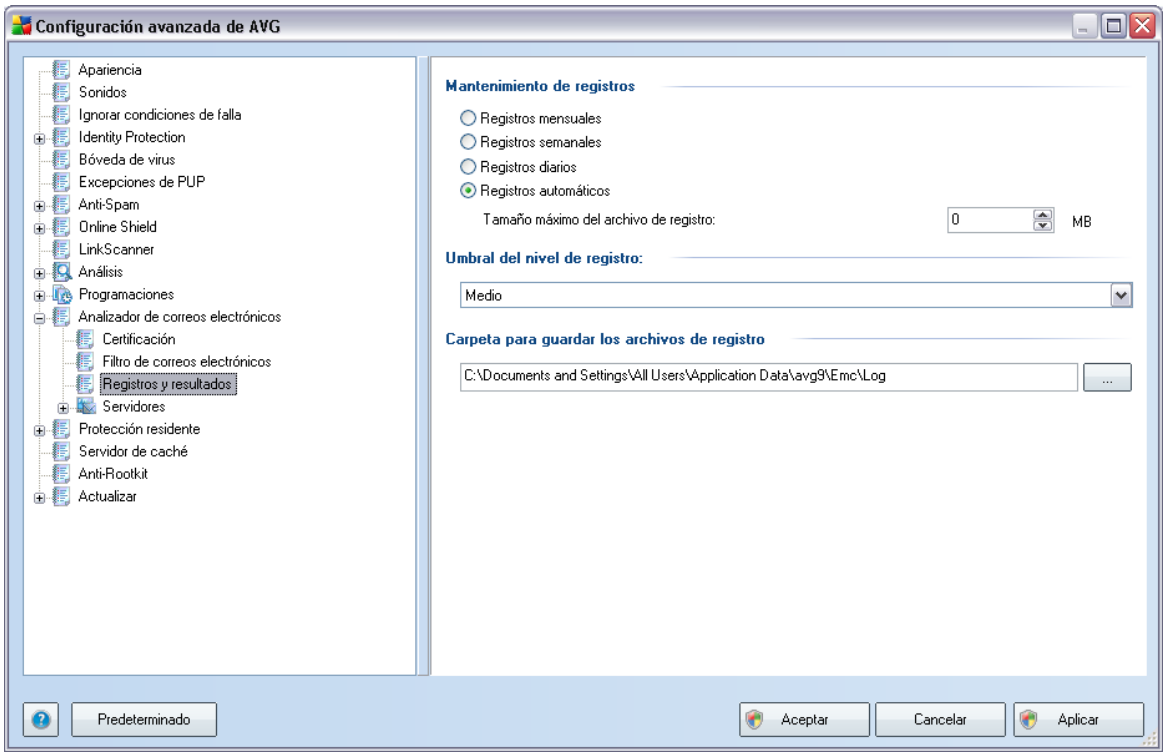
## 10.10.2. Filtro de correos electrónicos




El diálogo ***Filtro de archivos adjuntos***le permite establecer los parámetros para el análisis de los archivos adjuntos de los mensajes de correo electrónico. De manera predeterminada, la opción ***Quitar archivos adjuntos*** está desactivada. Si decide activarla, todos los archivos adjuntos de los mensajes de correo electrónico detectados como infectados o potencialmente peligrosos se eliminarán automáticamente. Si desea definir los tipos específicos de archivos adjuntos que se deben eliminar, seleccione la opción respectiva:

- ***Quitar todos los archivos ejecutables***: se eliminarán todos los archivos *.exe
- ***Quitar todos los documentos***: se eliminarán todos los archivos *.doc, *.docx, *.xls y *.xlsx
- ***Eliminar los archivos con las siguientes extensiones separadas por coma*** : se eliminarán todos los archivos con las extensiones definidas

## 10.10.3. Registros y resultados




El diálogo abierto mediante el elemento de navegación ***Registros y resultados*** permite especificar los parámetros para el mantenimiento de los resultados del análisis de los correos electrónicos. El diálogo se divide en varias secciones:

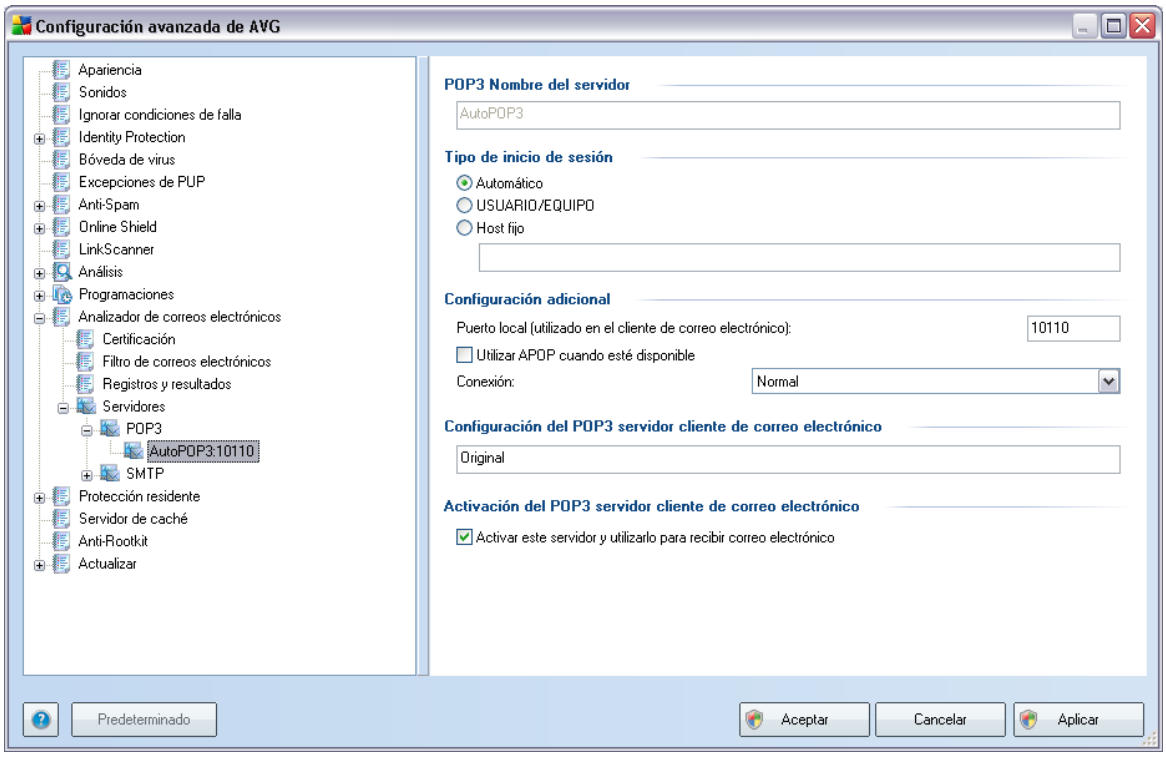
- ***Mantenimiento de registros***: define si desea registrar la información de análisis de los correos electrónicos diaria, semanal, mensualmente, ... ; y también especifica el tamaño máximo del archivo de registro *en MB*

- ***Umbral de nivel de registro***: el nivel medio se configura de manera predeterminada; se puede seleccionar un nivel más bajo (*registrando la información de conexión elemental*) o el nivel más alto (*registrando todo el tráfico*)

- ***Carpeta utilizada para almacenar los archivos de registro***: define dónde se deben ubicar los archivos de registro

## 10.10.4. Servidores

En la sección ***Servidores*** puede editar los parámetros de los servidores del componente ***Analizador de correos electrónicos***, o establecer algún servidor nuevo utilizando el botón ***Agregar nuevo servidor***.




En este diálogo (abierto a través de***Servidores /POP3***) puede configurar un nuevo servidor del***Analizador de correos electrónicos*** utilizando el protocolo POP3 para el correo electrónico entrante:

- ***Nombre del servidor POP3***: escriba el nombre del servidor o conserve el nombre predeterminado AutoPOP3
- ***Tipo de inicio de sesión***: define el método para determinar el servidor de correo empleado para el correo entrante:
  - ***Automático***: el inicio de sesión se realizará de manera automática, de acuerdo con la configuración del cliente de correo electrónico.

- ***USUARIO/EQUIPO***: el método más simple y más frecuente para determinar el servidor de correo de destino es el método proxy. Para utilizar este método, especifique el nombre o la dirección (o también el puerto) como parte del nombre de usuario de inicio de sesión para el servidor de correo dado, separándolos con el carácter /. Por ejemplo, para la cuenta user1 en el servidor pop.acme.com y el puerto 8200, usted utilizaría user1/pop.acme.com:8200 para el nombre de inicio de sesión.

- ***Host fijo*** : en este caso, el programa siempre utilizará el servidor especificado aquí. Especifique la dirección o el nombre de su servidor de correo. El nombre de inicio de sesión permanece invariable. Como nombre, puede utilizar un nombre de dominio (por ejemplo, pop.acme.com) así como también una dirección IP (por ejemplo, 123.45.67.89). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (por ejemplo, pop.acme.com:8200). El puerto estándar para comunicaciones POP3 es 110.

- ***Configuración adicional***: especifica los parámetros con más detalle:

  - ***Puerto local***: especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Luego debe especificar en su aplicación de correo este puerto como el puerto para comunicaciones POP3.

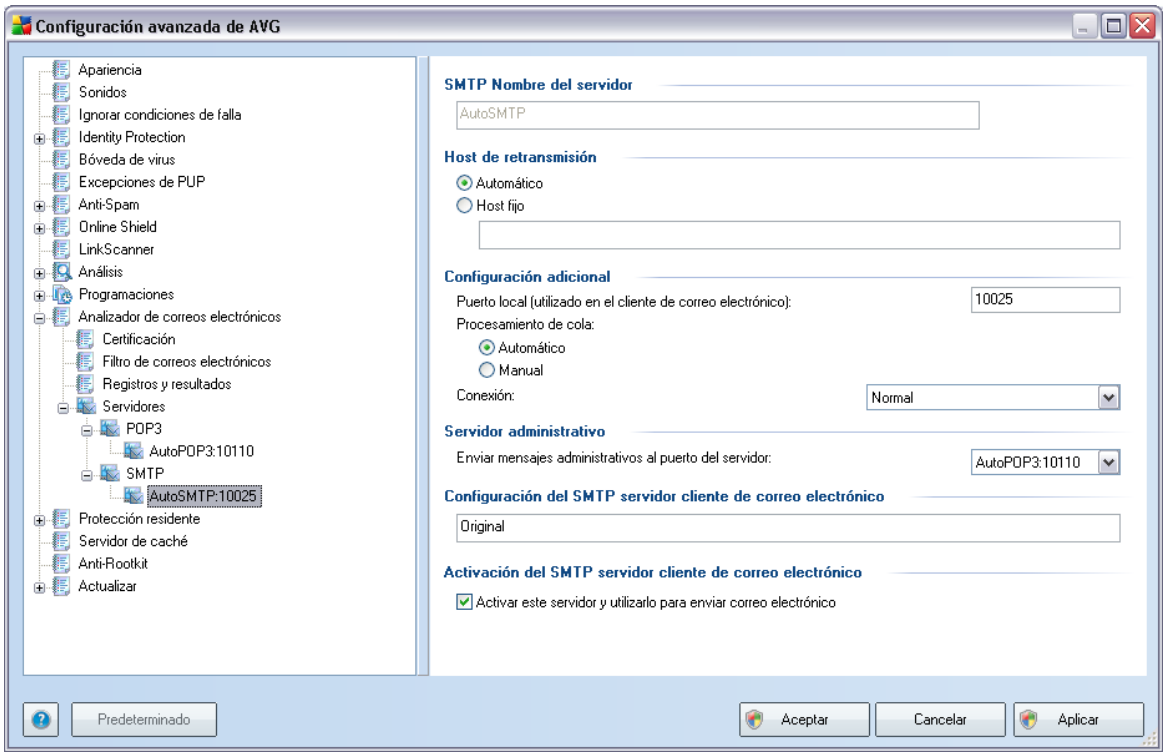
  - ***Utilizar APOP cuando esté disponible***: esta opción proporciona un inicio de sesión más seguro en el servidor de correo. Esto asegura que el ***Analizador de correos electrónicos*** utilice un método alternativo de enviar al servidor la contraseña de inicio de sesión de la cuenta del usuario no en un formato abierto, sino cifrada utilizando una cadena variable recibida desde el servidor. Naturalmente, esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.

  - ***Conexión***: en el menú desplegable, puede especificar la clase de conexión que desea utilizar (normal/SSL/SSL predeterminada). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.

- ***Configuración de servidor cliente POP3 de correo electrónico***: proporciona información breve sobre la configuración requerida para configurar de manera correcta su cliente de correo electrónico (para que el ***Analizador de correos electrónicos*** controle todo el correo entrante). Este es un resumen basado en los parámetros correspondientes especificados en este cuadro de diálogo y

otros cuadros de diálogo relacionados.

- ***Activación del servidor de cliente POP3 de correo electrónico***: seleccione o quite la marca de selección de este elemento para activar o desactivar el servidor POP3 especificado




En este diálogo (al que se obtiene acceso mediante ***Servidores/SMTP***) puede configurar un nuevo servidor ***Analizador de correos electrónicos*** utilizando el protocolo SMTP para el correo saliente:

- ***Nombre del servidor SMTP***: escriba el nombre del servidor o mantenga el nombre predeterminado AutoSMTP.

- ***Host de retransmisión***: define el método para determinar el servidor de correo empleado para el correo saliente:

  - ***Automático***: el inicio de sesión se efectuará automáticamente, según la configuración del cliente de correo electrónico.

- ***Host fijo***: en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (por ejemplo, smtp.acme.com) así como también una dirección IP (por ejemplo, 123.45.67.89). Si el servidor de correo utiliza un puerto no estándar, puede especificar este puerto poniéndolo a continuación del nombre del servidor con dos puntos como delimitador (por ejemplo, smtp.acme.com:8200). El puerto estándar para comunicaciones SMTP es 25.

- ***Configuración adicional***: especifica los parámetros con más detalle:

  - ***Puerto local***: especifica el puerto en el cual se espera recibir la comunicación de su aplicación de correo. Posteriormente deberá especificar en su aplicación de correo este puerto como puerto para la comunicación SMTP.

  - ***Procesamiento de cola***: determina el comportamiento del ***Analizador de correos electrónicos*** al procesar los requisitos de envío de mensajes de correo:

    - Automático: el correo saliente se entrega (envía) inmediatamente al servidor de correo de destino

    - Manual: el mensaje se inserta en la cola de los mensajes salientes y se envía más tarde

  - ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (normal/SSL/valor predeterminado de SSL). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible cuando el servidor de correo de destino la admite.

- ***Servidor administrativo***: muestra el número del puerto del servidor que se utilizará para el envío inverso de informes administrativos. Estos mensajes se generan, por ejemplo, cuando el servidor de correo de destino rechaza el mensaje saliente o cuando el servidor de correo no se encuentra disponible.

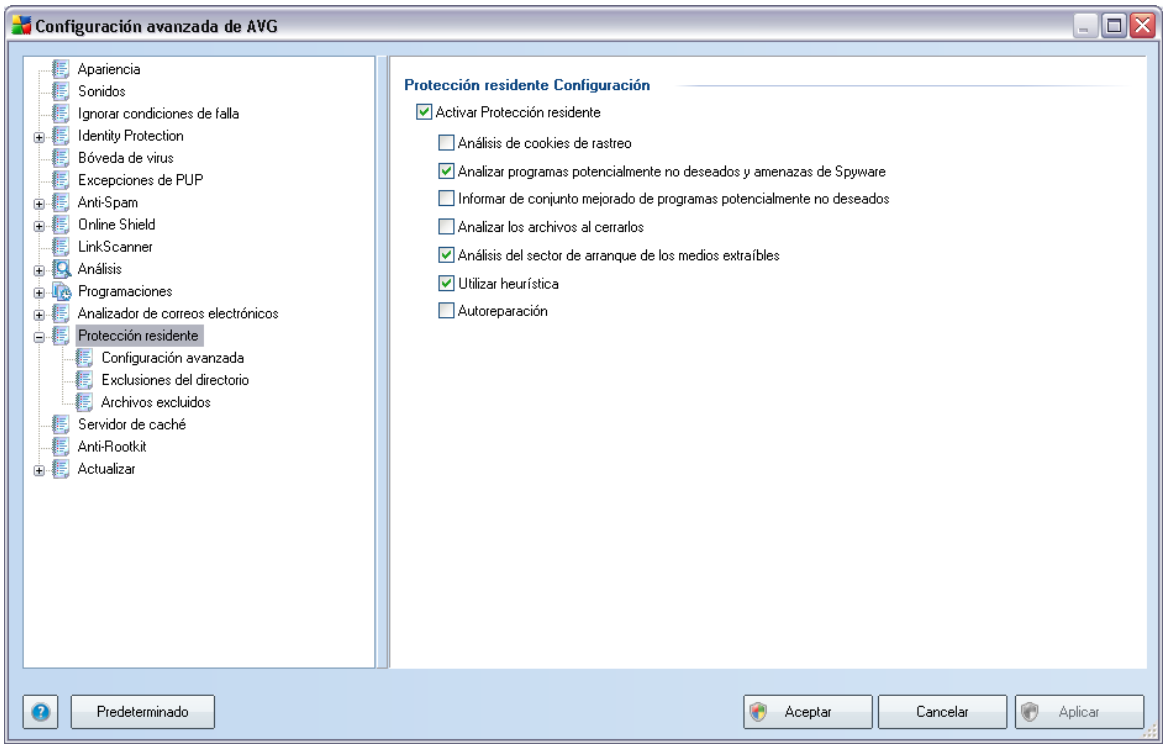
- ***Configuración del servidor cliente SMTP de correo electrónico***: proporciona información sobre cómo configurar la aplicación de correo del cliente para que los mensajes de correo salientes se analicen utilizando el servidor actualmente modificado para controlar el correo saliente. Este es un resumen basado en los parámetros correspondientes especificados en este cuadro de diálogo y otros cuadros de diálogo relacionados.

- ***Activación del servidor SMTP en el cliente de correo electrónico***: seleccione/quite la marca de selección de este elemento para activar o

desactivar el servidor SMTP especificado anteriormente

## 10.11. Protección residente

El componente ***Protección residente*** realiza la protección viva de archivos y carpetas contra virus, spyware y otro malware.




En el diálogo ***Configuración de Protección residente*** puede activar o desactivar la ***Protección residente*** por completo seleccionando o deseleccionando el elemento ***Activar Protección residente*** (*esta opción está seleccionada de modo predeterminado*). También puede seleccionar las funciones de ***Protección residente*** que deben activarse:

- ***Análisis de cookies de rastreo***: este parámetro define que se deben detectar las cookies durante el análisis. (*las cookies HTTP se utilizan para la autenticación, el seguimiento y el mantenimiento de información específica sobre los usuarios, como las preferencias de ubicación o el contenido de su carrito de compras electrónico.*)

- ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*seleccionada de modo predeterminado*): seleccione la opción para

activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo.

- ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware: programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

- ***Analizar los archivos al cerrarlos***: el análisis al cerrar garantiza que el programa AVG analiza los objetos activos (aplicaciones, documentos, etc.) cuando se abren y también cuando se cierran; esta función contribuye a proteger el equipo frente a algunos tipos de virus sofisticados.

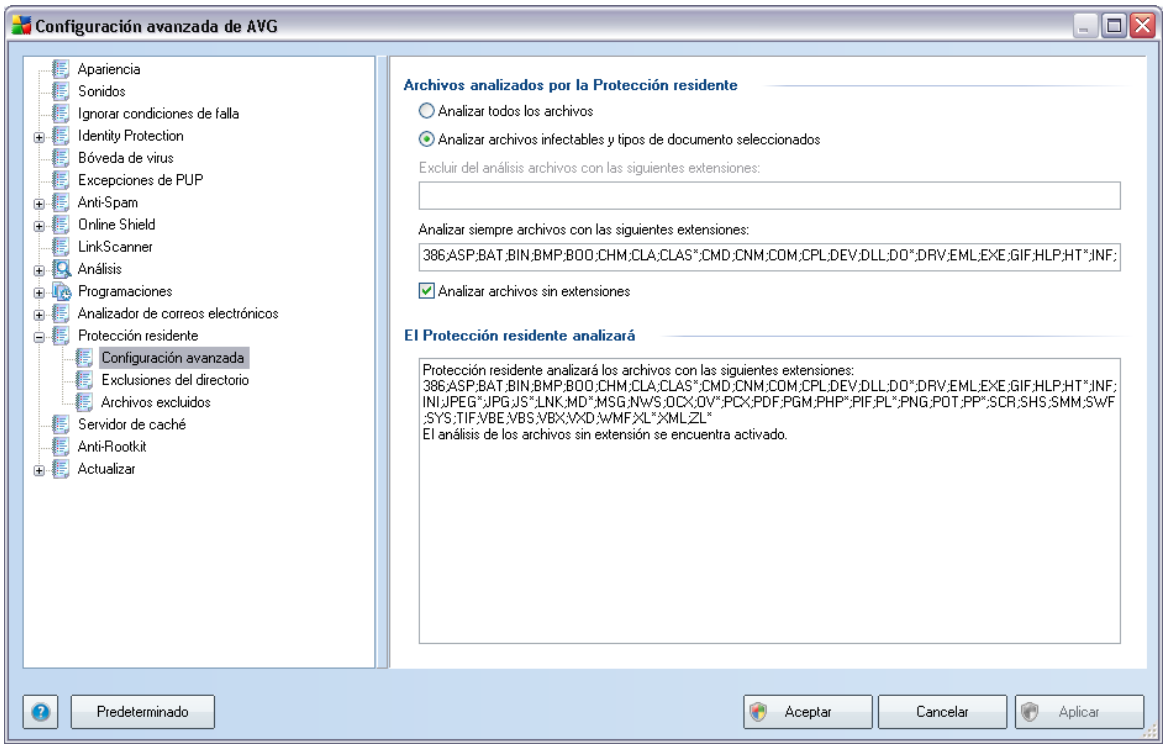
- ***Analizar sector de arranque de medios extraíbles***: (*opción seleccionada de modo predeterminado*).

- ***Utilizar método heurístico***: (*opción seleccionada de modo predeterminado*) se utilizará el análisis heurístico para la detección (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).

- ***Autoreparar***: se reparará automáticamente cualquier infección detectada si existe una cura disponible.

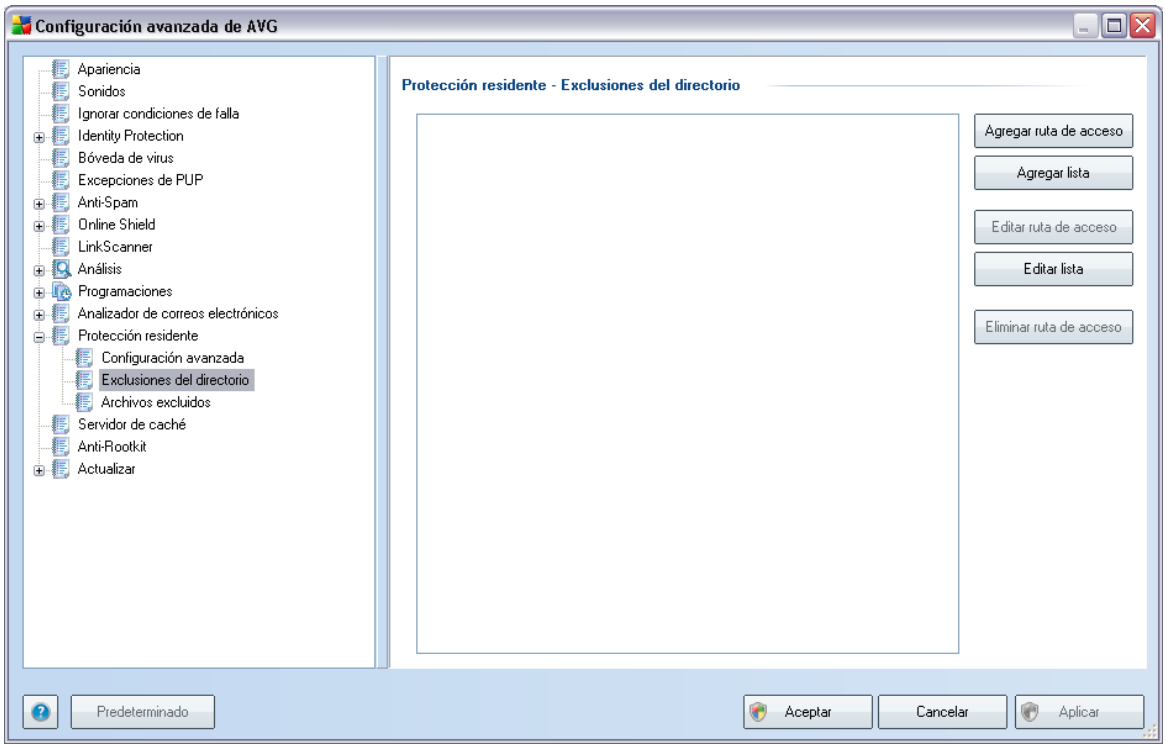
### 10.11.1. Configuración avanzada

En el cuadro de diálogo ***Archivos analizados mediante Protección residente*** es posible configurar qué archivos se van a analizar (*por medio de las extensiones específicas*):




Decida si desea que se analicen todos los archivos o sólo los archivos infectables; si escoge esta última opción, puede especificar una lista con las extensiones que definan los archivos que se deben excluir del análisis, así como una lista de las extensiones de los archivos que se deben analizar siempre.

## 10.11.2. Exclusiones de directorio




El diálogo ***Protección residente - Exclusiones de directorio*** ofrece la posibilidad de definir las carpetas en las que se debe ejecutar el análisis de la ***Protección residente.***

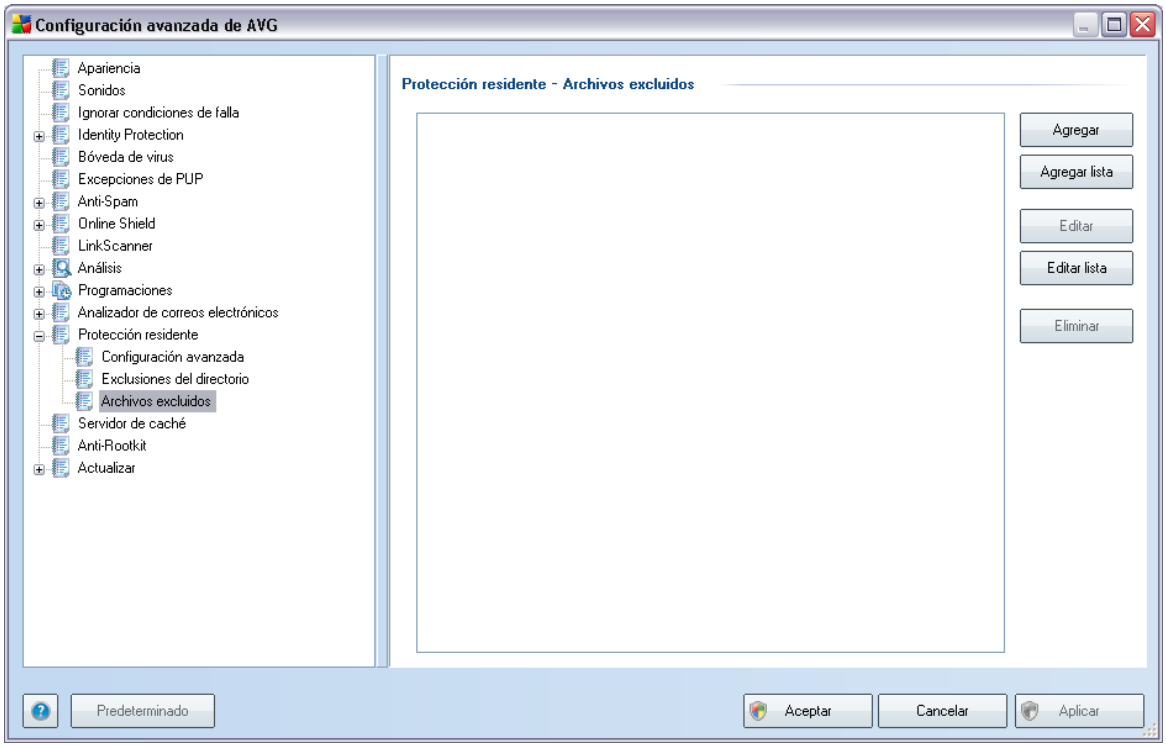
***Si no es absolutamente necesario, le recomendamos no excluir ningún directorio.***

El cuadro de diálogo proporciona los siguientes botones de control:

- ***Agregar ruta***: especifica los directorios que deben excluirse del análisis seleccionándolos uno por uno desde el árbol de navegación del disco local.
- ***Agregar lista***: le permite introducir una lista completa de directorios que desea excluir del análisis de la ***Protección residente***
- ***Editar ruta***: le permite editar la ruta de acceso especificada de una carpeta seleccionada
- ***Editar lista***: le permite editar la lista de carpetas

- ***Eliminar ruta***: le permite eliminar la ruta de acceso de una carpeta seleccionada.

### 10.11.3. Archivos excluidos




El cuadro de diálogo ***Protección residente - Archivos excluidos*** se comporta como el cuadro de diálogo descrito con anterioridad ***Protección residente - Exclusiones del directorio***pero en lugar de carpetas ahora puede definir archivos específicos que se deben excluir del análisis de la ***Protección residente.***

***Si no es absolutamente necesario, le recomendamos no excluir ningún archivo.***

El cuadro de diálogo proporciona los siguientes botones de control:

- ***Agregar***: especifique los archivos que deben excluirse del análisis seleccionándolos uno por uno en el árbol de navegación del disco local

- ***Agregar lista***: le permite introducir una lista completa de archivos que desea excluir del análisis de la ***Protección residente***

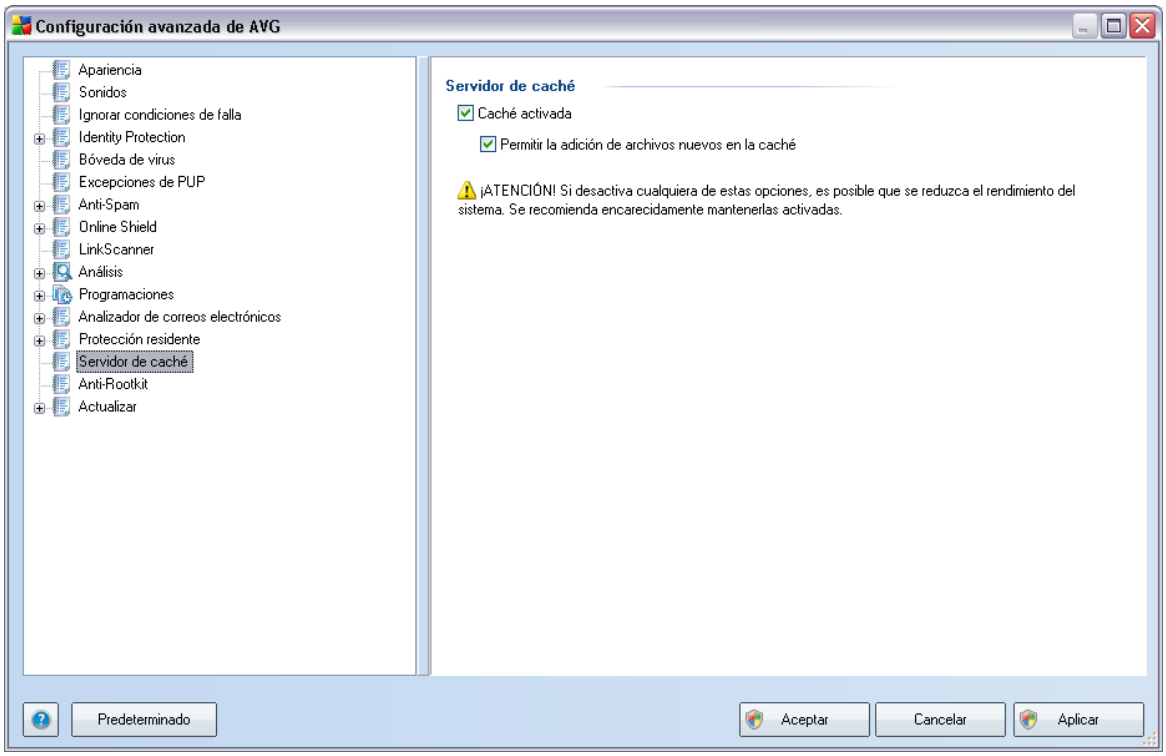
- ***Editar***: le permite editar la ruta de acceso especificada de un archivo

seleccionado

- ***Editar lista***: le permite editar la lista de archivos
- ***Eliminar***: le permite eliminar la ruta de acceso a un archivo seleccionado de la lista

## 10.12. Servidor de caché

El ***Servidor de caché*** es un proceso diseñado para acelerar cualquier análisis (*análisis a pedido, análisis programado de todo el equipo, análisis de Protección residente*). Reúne y mantiene información de los archivos confiables (*archivos de sistema con firma digital, etc.*): estos archivos se consideran seguros y se omiten durante el análisis.




El cuadro de diálogo de configuración presenta dos opciones:

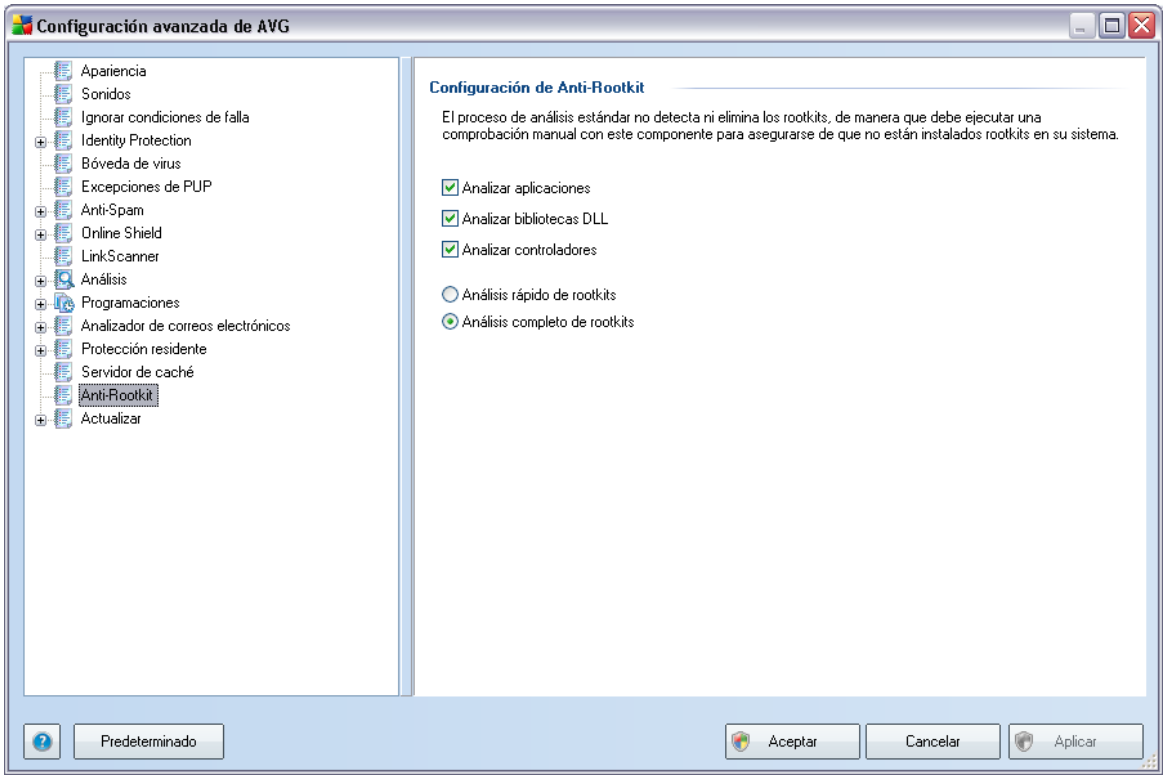
- ***Caché activada*** (*activada de forma predeterminada*): quite la marca de la casilla para desactivar el ***Servidor de caché*** y vacíe la memoria caché. Tenga en cuenta que el análisis puede ralentizar y reducir el rendimiento general de su

equipo, porque primero se analizarán todos y cada uno de los archivos en uso en busca de virus y spyware.

- ***Permitir la adición de archivos nuevos en la caché*** (*activada de forma predeterminada*): quite la marca de la casilla para dejar de agregar archivos en la memoria caché. Se guardarán y usarán todos los archivos ya almacenados en caché hasta que el almacenamiento en caché se desactive completamente o hasta la siguiente actualización de la base de datos de virus.

## 10.13. Anti-Rootkit

En este diálogo puede editar la configuración del componente ***Anti-Rootkit***:




También se puede tener acceso a la edición de todas las funciones del componente ***Anti-Rootkit***como se estipula dentro de este diálogo, directamente desde la ***interfaz del componente Anti-Rootkit***.

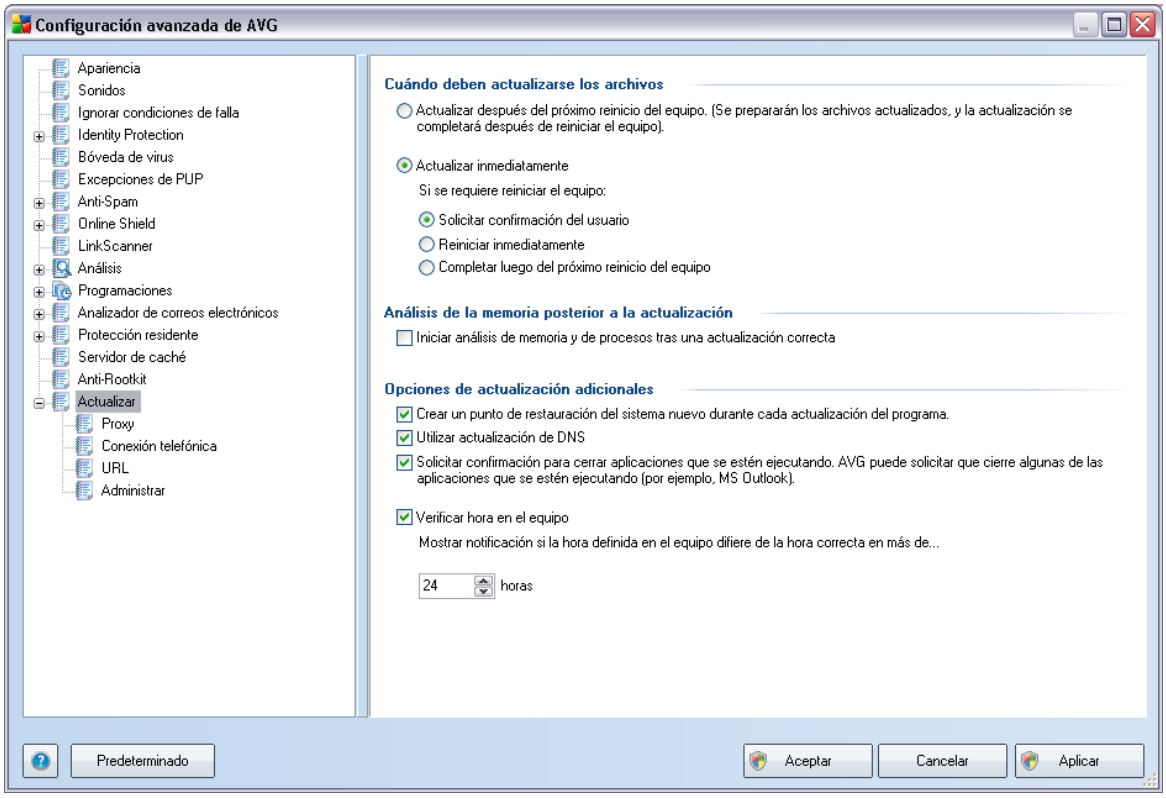
Marque las casillas de verificación respectivas para especificar los objetos que deben analizarse:

- ***Analizar aplicaciones***
- ***Analizar bibliotecas DLL***
- ***Analizar controladores***

También puede seleccionar el modo de análisis de rootkits:

- ***Análisis de rootkits rápido***: analiza todos los procesos en ejecución, los controladores cargados y la carpeta del sistema (*generalmente, c:\Windows*)
- ***Análisis de rootkits completo***: analiza todos los procesos en ejecución, los controladores cargados, la carpeta del sistema (*generalmente, c:\Windows*), así como todos los discos locales (*incluyendo el disco flash, pero excluyendo las unidades de disco flexible/CD*)

## 10.14. Actualización




El elemento de navegación ***Actualizar*** abre un nuevo diálogo en el que puede especificar los parámetros generales relacionados con la actualización de AVG:

## Cuándo deben actualizarse los archivos

En esta sección, puede seleccionar entre dos opciones alternativas: actualizar, que se puede programar para el siguiente reinicio del equipo o puede ejecutar actualizar inmediatamente. De manera predeterminada, está seleccionada la opción de actualización inmediata, dado que de esta forma AVG puede garantizar el máximo nivel de seguridad. La programación de una actualización para el siguiente reinicio del equipo sólo se puede recomendar si está seguro de que el equipo se reiniciará regularmente, al menos diariamente.

Si decide mantener la configuración predeterminada y ejecuta el proceso de actualización inmediatamente, puede especificar las circunstancias bajo las cuales se debe llevar a cabo un posible reinicio requerido.

- ***Solicitar confirmación del usuario***: se le pedirá que apruebe un reinicio del equipo, necesario para finalizar el proceso de actualización

- ***Reiniciar inmediatamente***: el equipo se reiniciará inmediatamente de forma automática después de que elproceso de actualización haya finalizado, no será necesaria la aprobación del usuario.

- ***Completar luego del próximo reinicio del equipo*** : la finalización del proceso de actualización se pospondrá hasta el siguiente reinicio del equipo. Nuevamente, tenga en cuenta que esta opción sólo se recomienda si puede estar seguro de que el equipo se reinicia regularmente, al menos diariamente.

## Análisis de la memoria posterior a la actualización

Seleccione esta casilla de verificación para especificar que desea ejecutar un nuevo análisis de la memoria después de cada actualización completada correctamente. La última actualización descargada podría contener definiciones de virus nuevas, y éstas podrían aplicarse en el análisis de forma inmediata.

## Opciones de actualización adicionales

- ***Crear un nuevo punto de restauración del equipo después de cada actualización del programa***: antes de iniciar cada actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Se puede obtener acceso a esta opción mediante Inicio/Todos los programas/Accesorios/

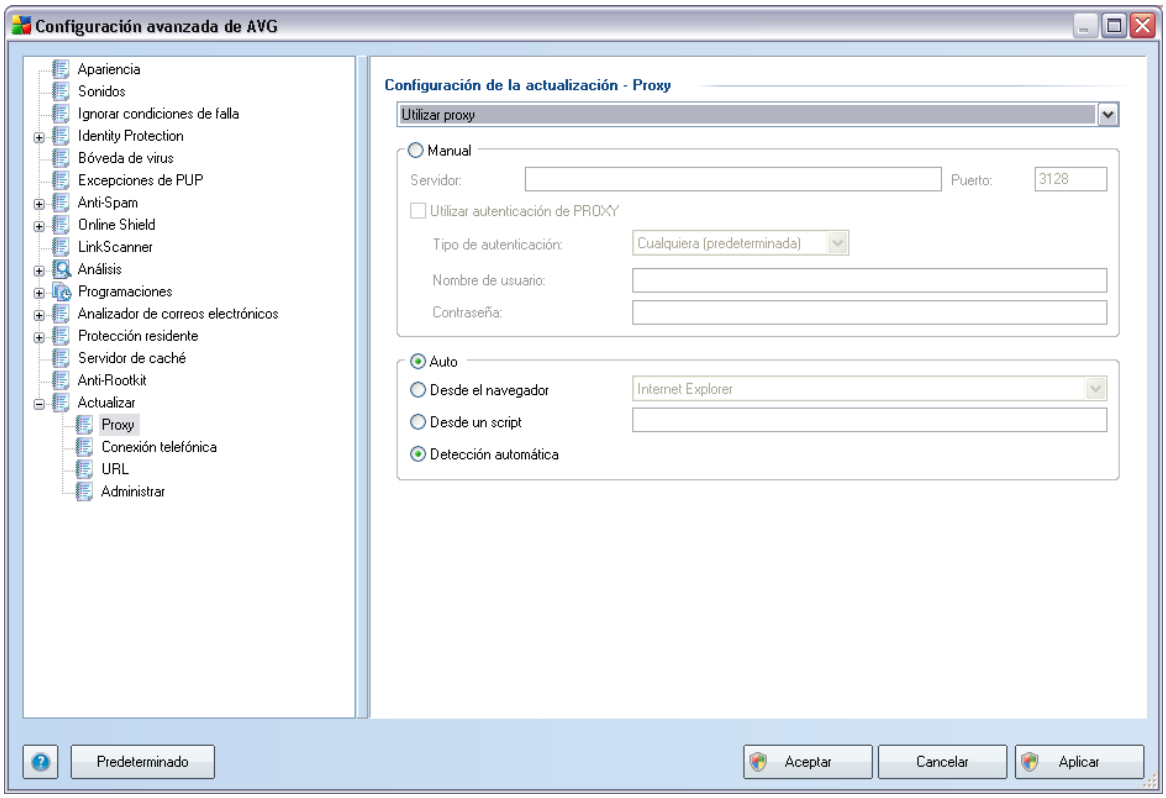
Herramientas del sistema/Restaurar sistema, pero se recomienda que sólo los usuarios experimentados realicen cambios. Mantenga esta casilla seleccionada si desea hacer uso de esta funcionalidad.

- ***Utilizar actualización de DNS***: marque esta casilla para confirmar que desea utilizar el método de detección de los archivos de actualización que elimina la cantidad de datos transferidos entre el servidor de actualización y el cliente AVG;

- ***Solicitar confirmación para cerrar aplicaciones que se estén ejecutando*** (*activado de forma predeterminada*): con este elemento tendrá la seguridad de que ninguna aplicación actualmente en ejecución se cerrará sin su permiso, si se requiere para que el proceso de actualización finalice;

- ***Verificar hora del equipo***: marque esta opción para declarar que desea recibir una notificación en caso de que la hora del equipo difiera por más horas de las especificadas de la hora correcta.

## 10.14.1. Proxy



El servidor proxy es un servidor independiente o un servicio que funciona en el equipo, que garantiza la conexión más segura a Internet. De acuerdo con las reglas de red especificadas, puede acceder a Internet bien directamente o a través del servidor proxy; ambas posibilidades pueden darse al mismo tiempo. A continuación, en el primer elemento del diálogo ***Configuración de la actualización - Proxy*** debe seleccionar en el menú del cuadro combinado si desea:

- ***Utilizar proxy***
- ***No utilizar servidor proxy***: configuración predeterminada
- ***Intentar conectarse utilizando proxy, y si esto falla, conectarse directamente***

Si selecciona alguna opción que utiliza el servidor proxy, deberá especificar varios datos adicionales. La configuración del servidor se puede llevar a cabo manual o automáticamente.

## Configuración manual

Si selecciona la configuración manual (marque *la opción **Manual** para activar la sección del diálogo correspondiente*) deberá especificar los elementos siguientes:

- ***Servidor***: especifique la dirección IP del servidor o el nombre del servidor.
- ***Puerto***: especifique el número del puerto que hace posible el acceso a Internet (*el valor predeterminado es 3128 pero se puede definir otro; en caso de duda, póngase en contacto con el administrador de la red*).

El servidor proxy también puede tener reglas específicas configuradas para cada usuario. Si el servidor proxy está configurado de este modo, seleccione la opción ***Utilizar autenticación de PROXY*** para verificar que el nombre de usuario y la contraseña sean válidos para la conexión a Internet mediante el servidor proxy.

## Configuración automática

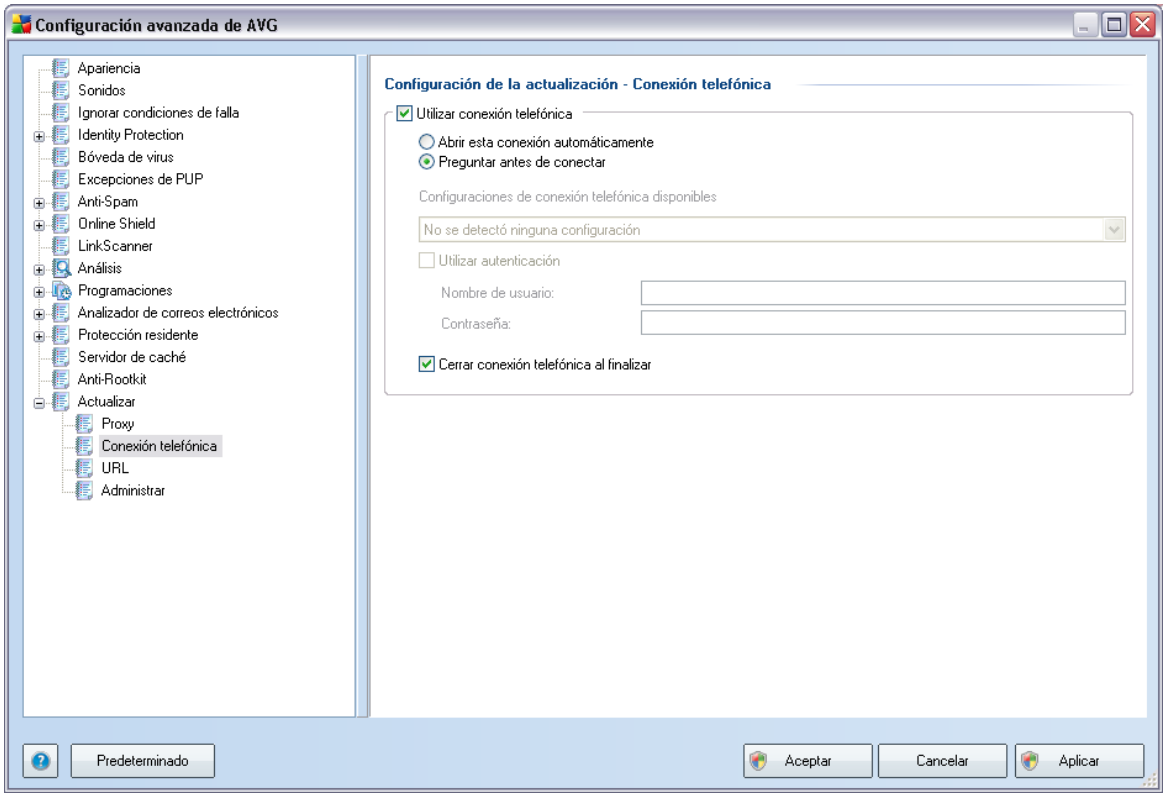
Si selecciona la configuración automática *(marque la opción **Auto** para activar la sección del cuadro de diálogo correspondiente*), a continuación, seleccione de dónde debe obtenerse la configuración de proxy:

- ***Desde el navegador***: la configuración se obtendrá del navegador de Internet predeterminado

- ***Desde el script***: la configuración se leerá de un script descargado con la dirección de proxy como valor de retorno de la función.

- ***Detección automática***: la configuración se detectará automáticamente desde el servidor proxy

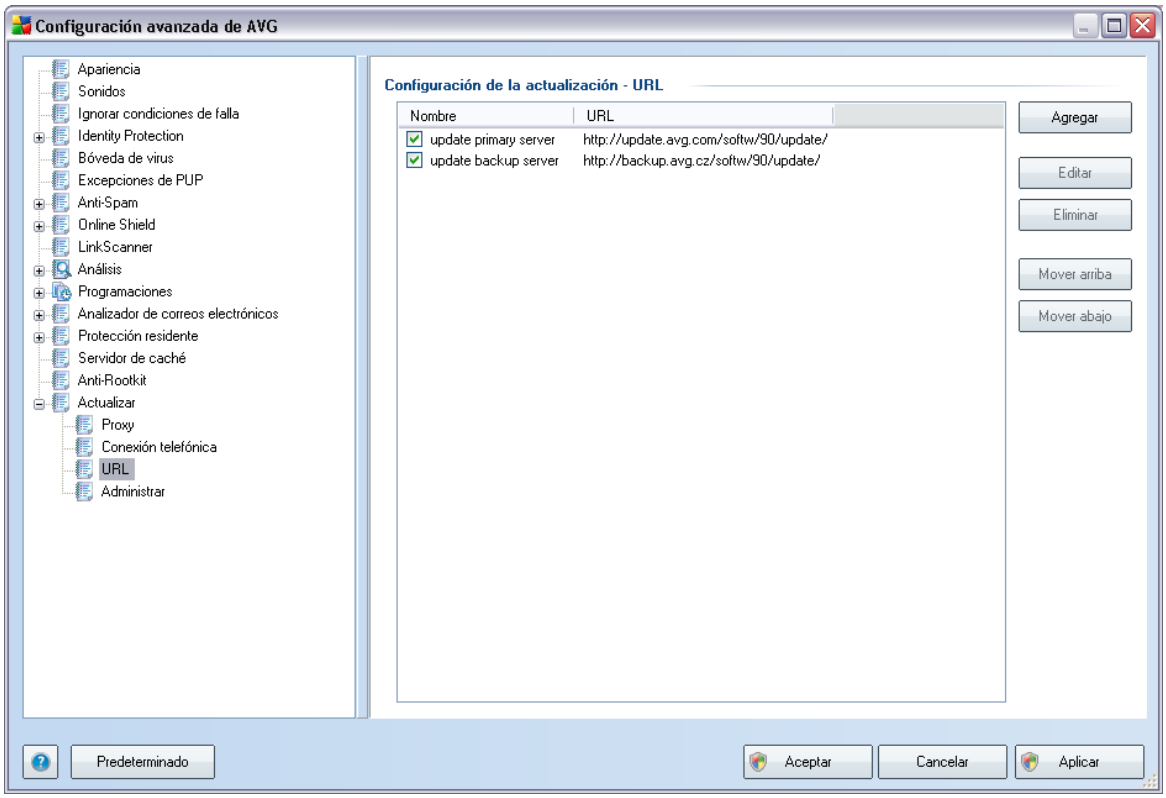
## 10.14.2. Conexión telefónica




Todos los parámetros definidos de modo opcional en el diálogo ***Actualizar configuración - Conexión telefónica*** hacen referencia a la conexión telefónica a Internet. Los campos del diálogo están inactivos hasta que se selecciona la opción ***Utilizar conexión telefónica***, que los activa.

Especifique si desea conectarse a Internet automáticamente (***Abrir esta conexión automáticamente***) o desea confirmar cada vez la conexión manualmente (***Preguntar antes de conectarse***). Para la conexión automática, debe seleccionar también si la conexión se cerrará una vez finalizada la actualización (***Cerrar la conexión telefónica cuando finalice***).

## 10.14.3. URL

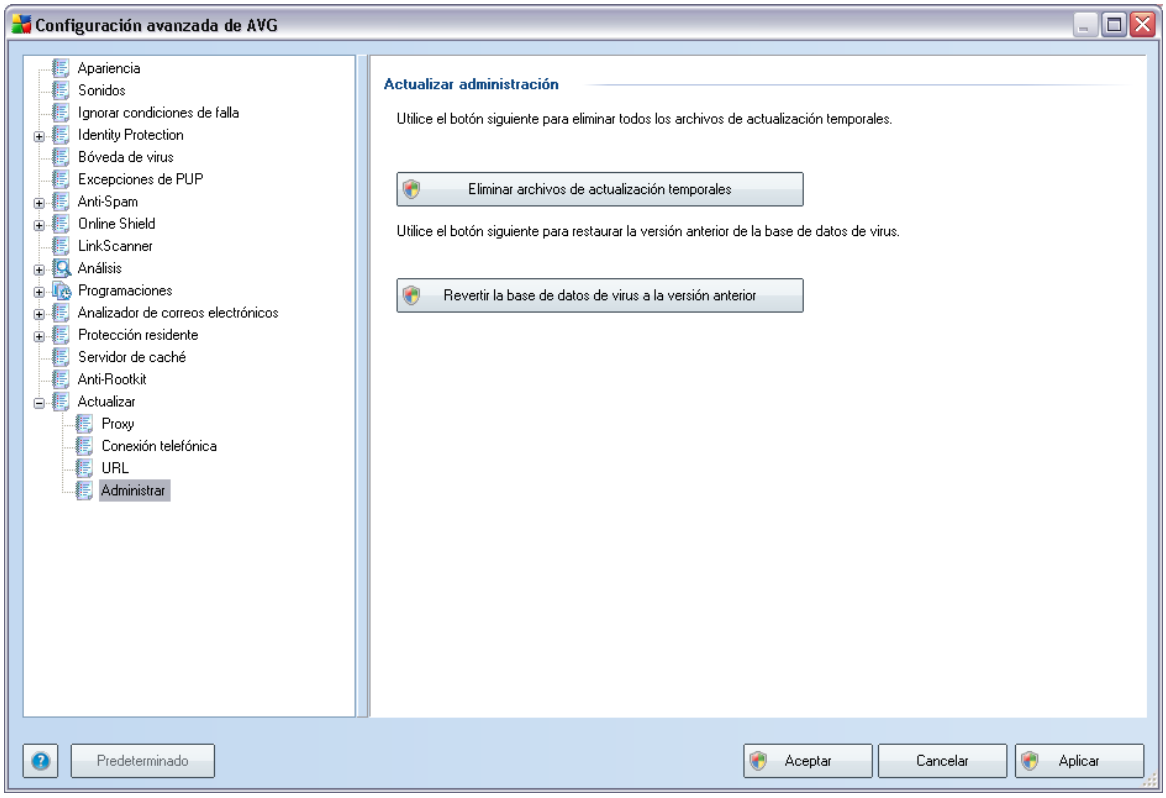



El diálogo ***URL*** ofrece una lista de direcciones de Internet desde las que se pueden descargar los archivos de actualización. La lista y los elementos se pueden modificar por medio de los siguientes botones de control:

- ***Agregar***: abre un diálogo donde puede especificar una nueva dirección URL para agregarla a la lista.
- ***Editar***: abre un diálogo donde puede editar los parámetros de URL seleccionados.
- ***Eliminar***: elimina la dirección URL seleccionada de la lista.
- ***Mover arriba***: mueve la dirección URL seleccionada una posición arriba de la lista.
- ***Mover abajo***: mueve la dirección URL seleccionada una posición abajo de la lista.

### 10.14.4. Administrar

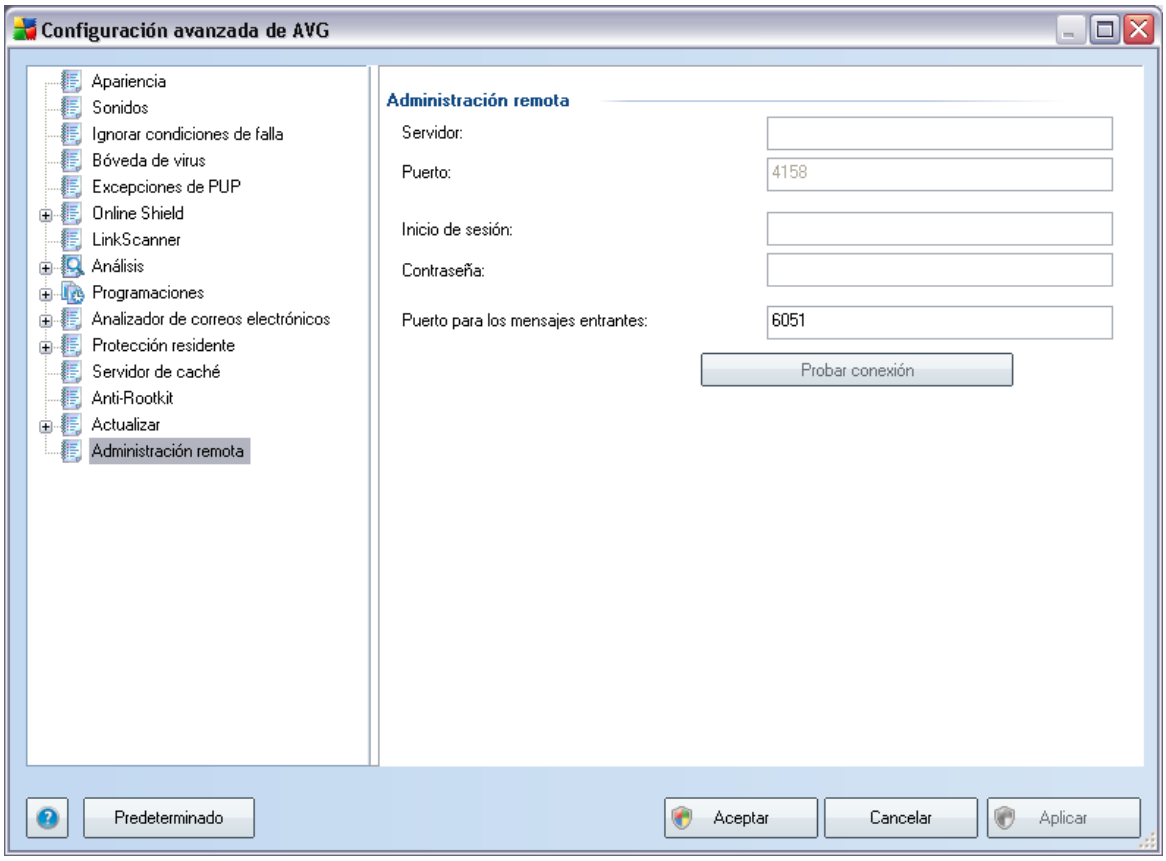
El diálogo ***Administrar*** ofrece dos opciones accesibles mediante dos botones:




- ***Eliminar archivos de actualización temporales***: presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada estos archivos se guardan durante 30 días*)

- ***Revertir la base de datos de virus a la versión anterior***: presione este botón para eliminar la última versión de la base de datos de virus del disco duro y volver a la versión anterior guardada (*la nueva versión de la base de datos de virus será parte de la siguiente actualización*).

## 10.15. Administración remota




La configuración de ***Administración remota*** hace referencia a la conexión de la estación cliente AVG con el sistema de administración remota. Si tiene previsto conectar la estación correspondiente con el sistema de administración remota, especifique los parámetros siguientes:

- ***Servidor***: nombre del servidor (o dirección IP del servidor) donde está instalado el Servidor de AVG Admin.
- ***Puerto***: indique el número del puerto en que el cliente AVG se comunica con el Servidor de AVG Admin (*el número de puerto 4158 se considera predeterminado; si utiliza este número de puerto, no es necesario que lo especifique explícitamente*).
- ***Inicio de sesión***: si la comunicación entre el cliente AVG y el Servidor de AVG Admin está definida como segura, indique el nombre de usuario...

- ***Contraseña***: especifique la contraseña.
- ***Puerto de mensajes entrantes***: número del puerto en que el cliente AVG acepta los mensajes entrantes del Servidor de AVG Admin.

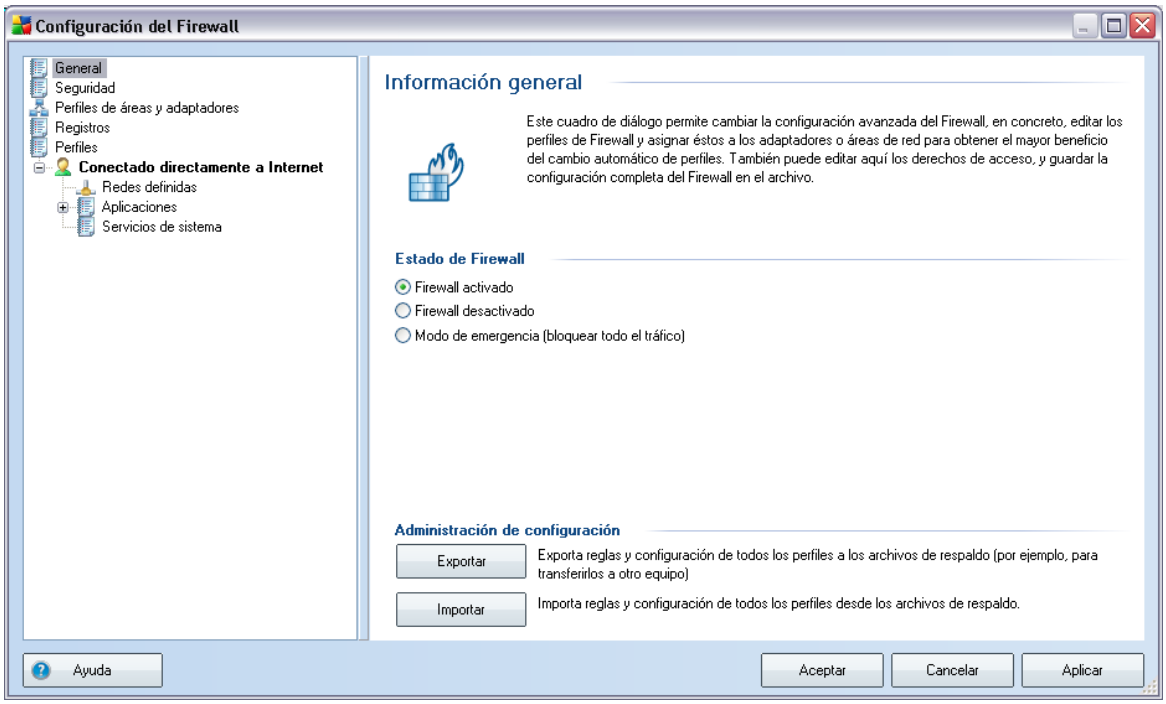
El botón ***Probar conexión*** le ayuda a verificar que todos los datos establecidos anteriormente están disponibles y se pueden utilizar para conectarse de manera exitosa al DataCenter.

***Nota:*** *para ver una descripción detallada de la administración remota, consulte la documentación de AVG - Edición para redes.*

# 11. Configuración del Firewall

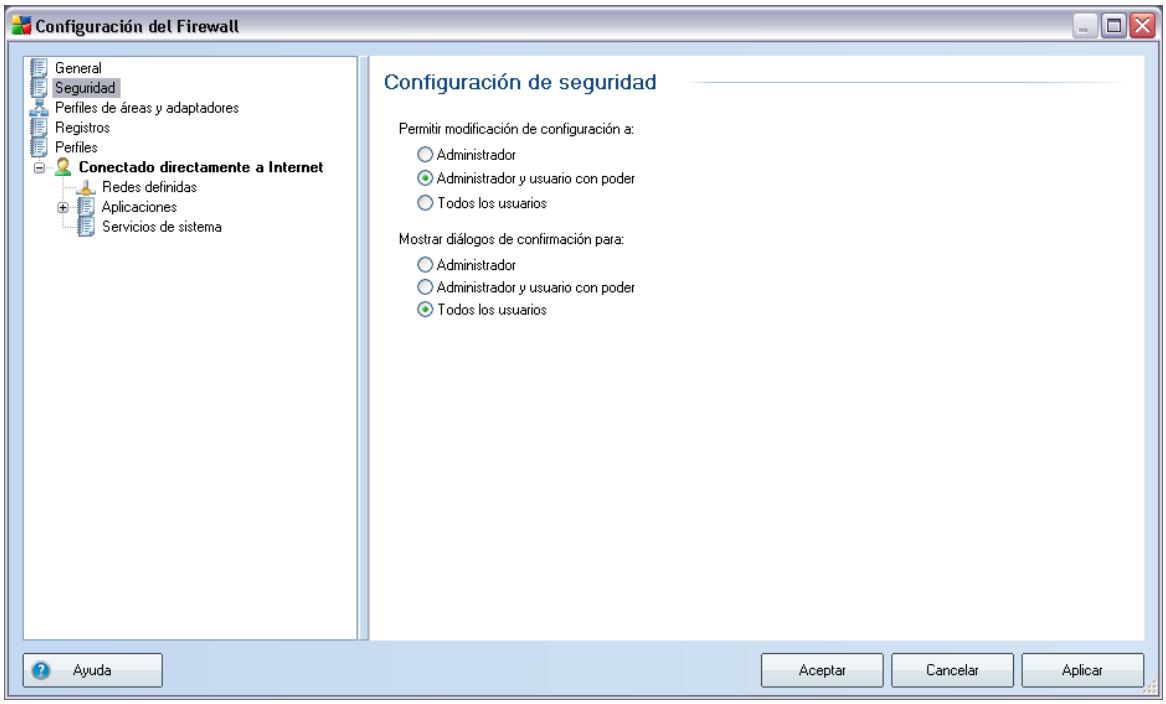
La configuración del ***Firewall*** se abre en una nueva ventana donde se pueden establecer parámetros muy avanzados del componente en varios cuadros de diálogo. ***Sin embargo, la edición de la configuración avanzada sólo está pensada para expertos y usuarios con experiencia.***

## 11.1. General




En ***Información general***, puede ***Exportar***/***Importar*** la configuración del ***Firewall***; por ejemplo exportar las reglas definidas y la configuración del ***Firewall*** a los archivos de copia de seguridad o, por otro lado, importar todo el archivo de copia de seguridad.

## 11.2. Seguridad




En el diálogo ***Configuración de seguridad*** puede definir las reglas generales del comportamiento del ***Firewall*** sin importar el perfil seleccionado:

- ***Permitir la modificación de la configuración a*** - especifique a quién le está permitido cambiar la configuración del ***Firewall***

- ***Mostrar el diálogo de confirmación para***: especifique a quién se deben mostrar los diálogos de confirmación (*diálogos solicitando una decisión en una situación no cubierta por una regla definida del* ***Firewall***)

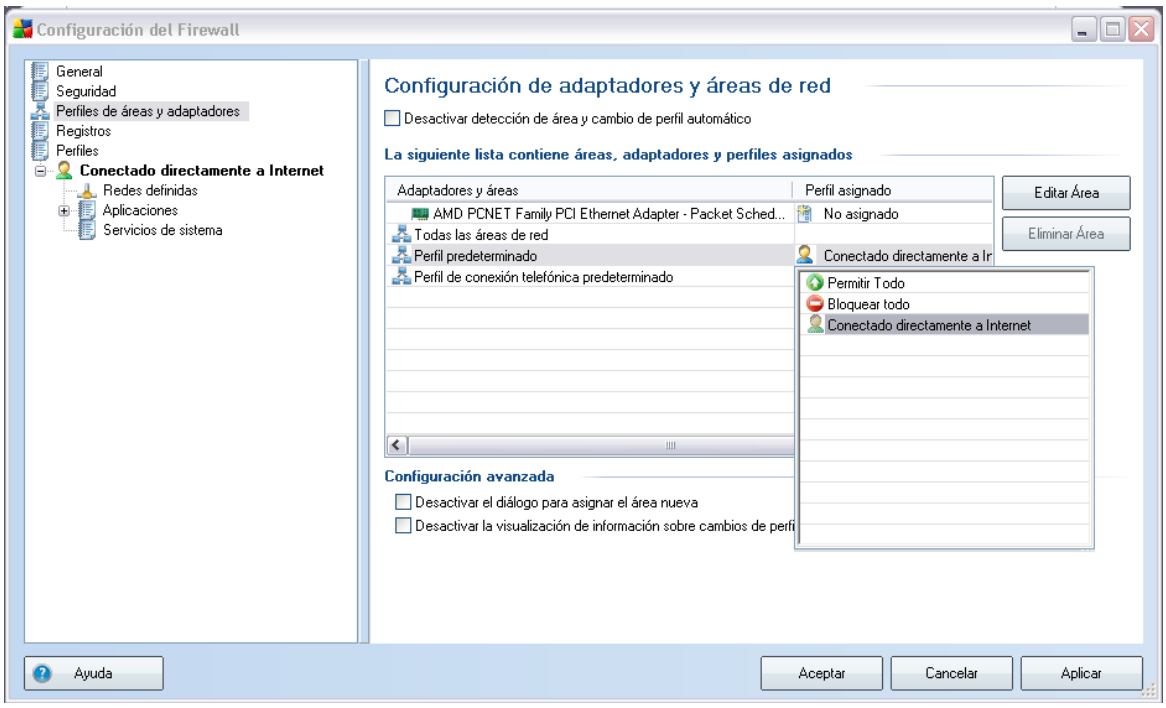
En ambos casos puede asignar el derecho específico a uno de los siguientes grupos de usuarios:

  - ***Administrador***: controla el equipo por completo y tiene derecho a asignar a cada usuario a grupos con autoridades específicamente definidas

  - ***Administrador y usuario con poder*** el administrador puede asignar a cualquier usuario a un grupo especificado (*Usuario con poder*) y definir las autoridades de los integrantes del grupo

- ***Todos los usuarios***:otros usuarios no asignados a ningún grupo específico

## 11.3. Perfiles de áreas y adaptadores




En los diálogos de ***Configuración de adaptadores y áreas de red*** puede editar la configuración relacionada con la asignación de perfiles definidos a adaptadores específicos y referentes a sus redes respectivas:

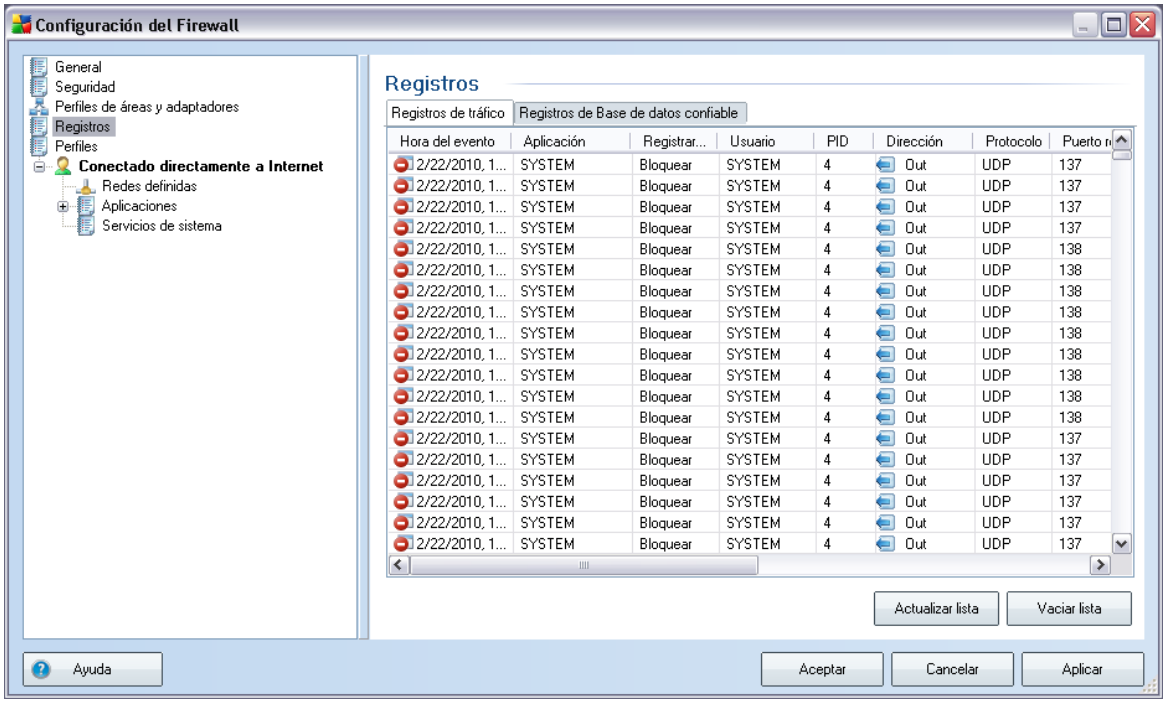
- ***Deshabilitar la detección de área y el cambio automático de perfiles***: uno de los perfiles definidos puede asignarse a cada tipo de interfaz de red, de forma respectiva a cada área. Si desea definir perfiles específicos, se utilizará un perfil común definido según la selección de uso del equipo y diseño de conexión en red del equipo durante el ***proceso de instalación***. Sin embargo, si decide diferenciar los perfiles y asignarlos a áreas y adaptadores específicos, y después, por alguna razón, desea cambiar esta configuración de forma temporal, haga clic en la opción ***Deshabilitar la detección de área y el cambio automático de perfiles***.

- ***Lista de adaptadores, áreas y perfiles asignados***: en esta lista puede encontrar una descripción general de los adaptadores y áreas detectados. Para

cada uno de ellos, puede asignar un perfil específico en el menú de perfiles definidos. Para abrir este menú, haga clic en el elemento respectivo en la lista de adaptadores, y seleccione el perfil.

- ***Configuración avanzada***: al marcar la opción respectiva desactivará la característica de mostrar un mensaje de información.

## 11.4. Registros




El cuadro de diálogo ***Registros*** permite revisar la lista de todas las acciones y eventos registrados del ***Firewall*** con una descripción detallada de los parámetros relevantes (*la hora del evento, el nombre de la aplicación, la acción de registro correspondiente, el nombre de usuario, el PID, la dirección de tráfico, el tipo de protocolo, los números de los puertos remotos y locales, etc.*) en dos pestañas:

- ***Registros de tráfico***: ofrece información acerca de la actividad de todas las aplicaciones que han intentado conectarse a la red.

- ***Registros de Base de datos confiable***: la *Base de datos confiable* es la base de datos interna de AVG que recopila información acerca de aplicaciones certificadas y confiables a las que siempre se les puede permitir comunicarse en línea. La primera vez que una nueva aplicación intenta conectarse a la red (

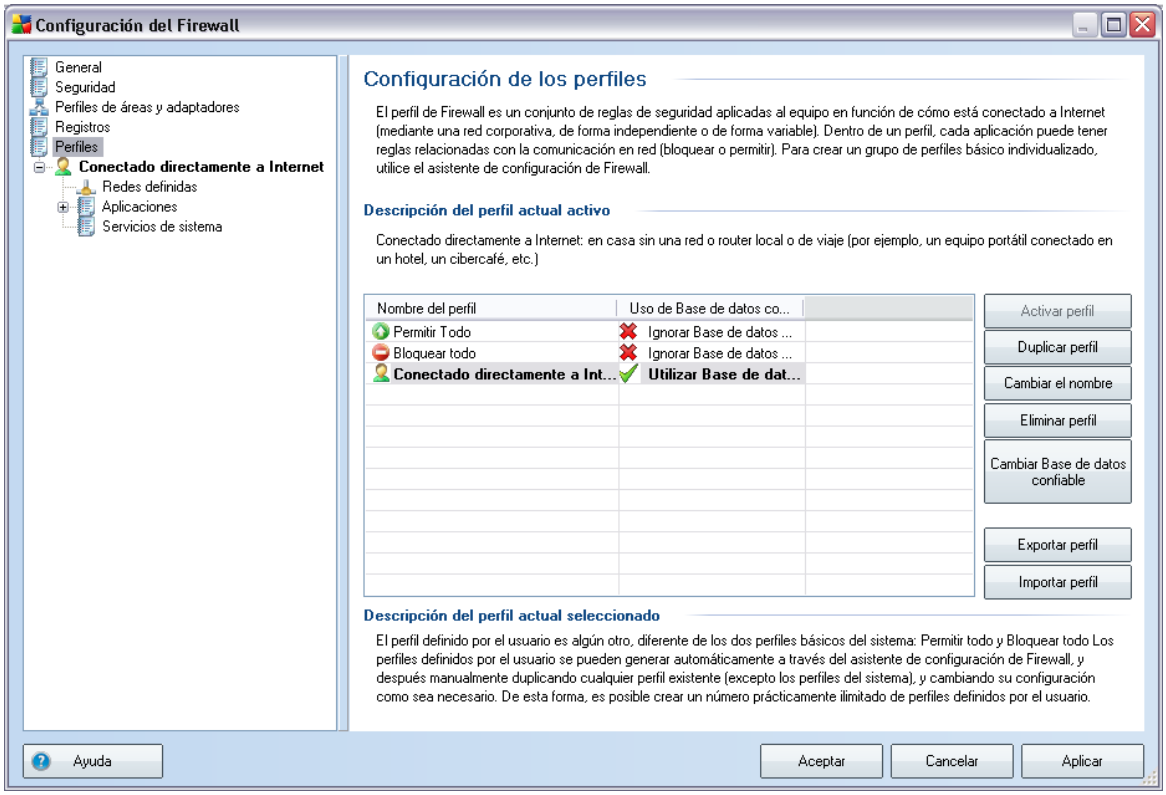
*es decir, aún no existen reglas del firewall especificadas para esta aplicación*), es necesario determinar si se le debe permitir la comunicación con la red. Primero, AVG busca en la *Base de datos confiable* y, si la aplicación se encuentra en la lista, se le concederá automáticamente acceso a la red. Sólo después de que se comprueba que no existe información disponible acerca de la aplicación en la base de datos, se le preguntará en un cuadro de diálogo independiente si desea permitir que la aplicación obtenga acceso a la red.

## Botones de control

- ***Ayuda***: abre los archivos de ayuda relacionados con el cuadro de diálogo activo.
- ***Actualizar lista*** : todos los parámetros registrados se pueden organizar de acuerdo al atributo seleccionado: cronológicamente (*fechas*) o alfabéticamente (*otras columnas*): sólo haga clic en el encabezado de la columna respectiva. Utiliceel botón ***Actualizar lista*** para actualizar la información actualmente mostrada.
- ***Vaciar lista***: elimina todas las entradas en la tabla.

## 11.5. Perfiles

Puede encontrar una lista de todos los perfiles disponibles en el diálogo ***Configuración del perfil***




Todos los demás perfilesdel sistema pueden editarse en este mismo diálogo utilizando los siguientes botones de control:

- ***Activar perfil***: este botón establece el perfil seleccionado como activo, lo cual significa que el ***Firewall*** utilizará el perfil seleccionado para controlar el tráfico de la red.
- ***Duplicar perfil***: crea una copia idéntica del perfil seleccionado; posteriormente es posible editar y cambiar el nombre de la copia para crear un perfil nuevo basado en el original duplicado
- ***Cambiar el nombre del perfil***: permite definir un nombre nuevo para un perfil seleccionado

- ***Eliminar perfil***: : elimina el perfil seleccionado de la lista

- ***Cambiar la Base de datos confiable***: para el perfil seleccionado puede elegir utilizar la información de la *Base de datos confiable* (*la Base de datos confiable es una base de datos interna de AVG que recopila información acerca de las aplicaciones confiables y certificadas a las cuales siempre se puede permitir la comunicación en línea.*)

- ***Exportar perfil***: registra la configuración del perfil seleccionado en un archivo que se guardará para utilizarse en el futuro

- ***Importar perfil***: configura el perfil seleccionado basándose en la información exportada en un archivo de copia de seguridad de la configuración

- ***Ayuda***: abre el archivo de ayuda relacionado con el diálogo activo

En la sección inferior del diálogo puede encontrar la descripción de un perfil que está seleccionado en la lista de arriba.

La estructura del menú de navegación izquierdo cambiará de acuerdo con el número de perfiles definidos mencionados en la lista dentro del diálogo ***Perfil***. Cada perfil definido crea una rama específica bajo el elemento ***Perfil***. Los perfiles específicos pueden editarse en los diálogos siguientes (*que son idénticos para todos los perfiles*):

## 11.5.1. Información del perfil

El cuadro de diálogo ***Información del perfil*** es el primero de una sección donde puede editar la configuración de cada perfil en cuadros de diálogo distintos y hacer referencia a los parámetros específicos del perfil.

- ***Utilizar base de datos confiable para este perfil*** (*seleccionada de modo predeterminado*): seleccione la opción para activar la *base de datos confiable* (*es decir, la base de datos interna de AVG que recopila información acerca de comunicaciones en línea confiables y certificadas. Si aún no existe una regla especificada para la aplicación, es necesario averiguar si se puede otorgar a la aplicación acceso a Internet. AVG busca primero en la Base de datos confiable y, si la aplicación se encuentra en la lista, se considerará segura y se le permitirá la comunicación a través de la red. En caso contrario, se le solicitará que decida si se debe permitir a la aplicación comunicarse a través de la red* ) con el perfil correspondiente.

- ***Activar red de puente de equipos virtuales*** (*desactivado de manera*

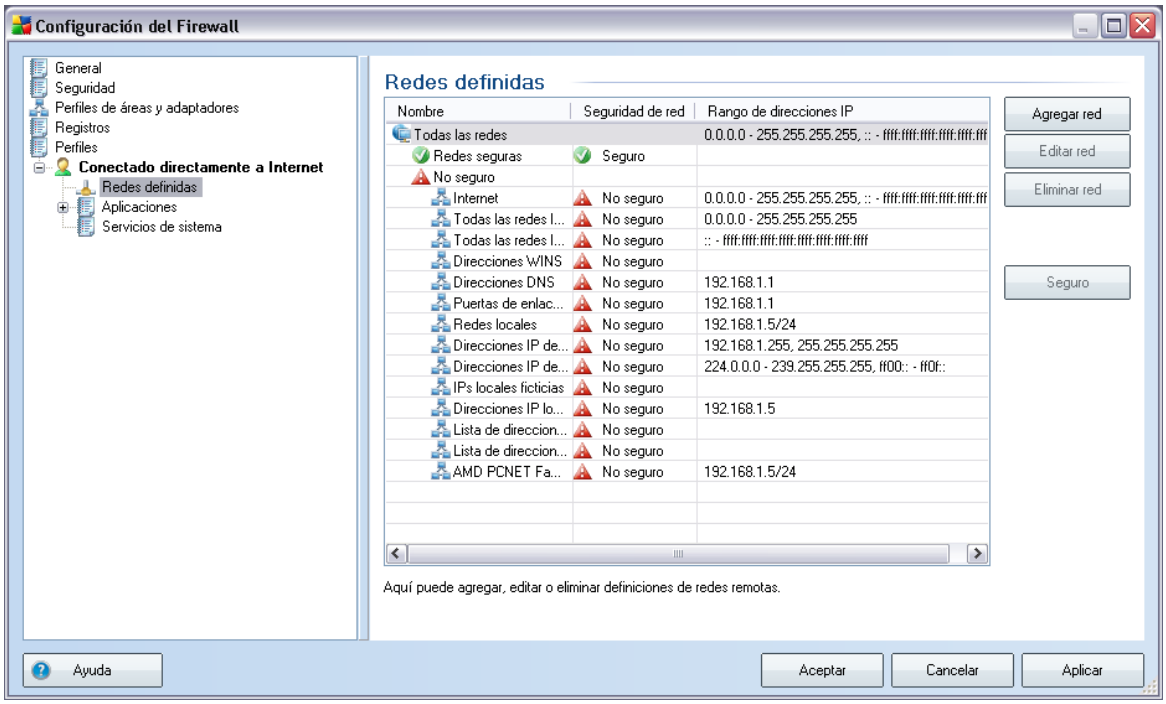
*predeterminada*): seleccione este elemento para permitir que las máquinas virtuales de VMware se conecten directamente a la red.

### Configuración del modo de juego

En la sección ***Configuración del modo de juego*** puede decidir y confirmar seleccionando cada elemento si desea que se muestren mensajes de información del ***Firewall***incluso cuando haya aplicaciones de pantalla completa en ejecución en el equipo (*por lo general éstos son juegos, pero se aplican a cualquier aplicación, por ejemplo, presentaciones PPT*). Dado que los mensajes de información pueden causar interrupciones.

Si selecciona el elemento ***Desactivar notificaciones de Firewall al jugar***, en el menú desplegable seleccione la acción que se debe realizar en caso de que una nueva aplicación para la que no se hayan especificado reglas intente comunicarse a través de la red (*aplicaciones que normalmente mostrarían un cuadro de diálogo de confirmación*), todas estas aplicaciones pueden permitirse o bloquearse.

## 11.5.2. Redes definidas



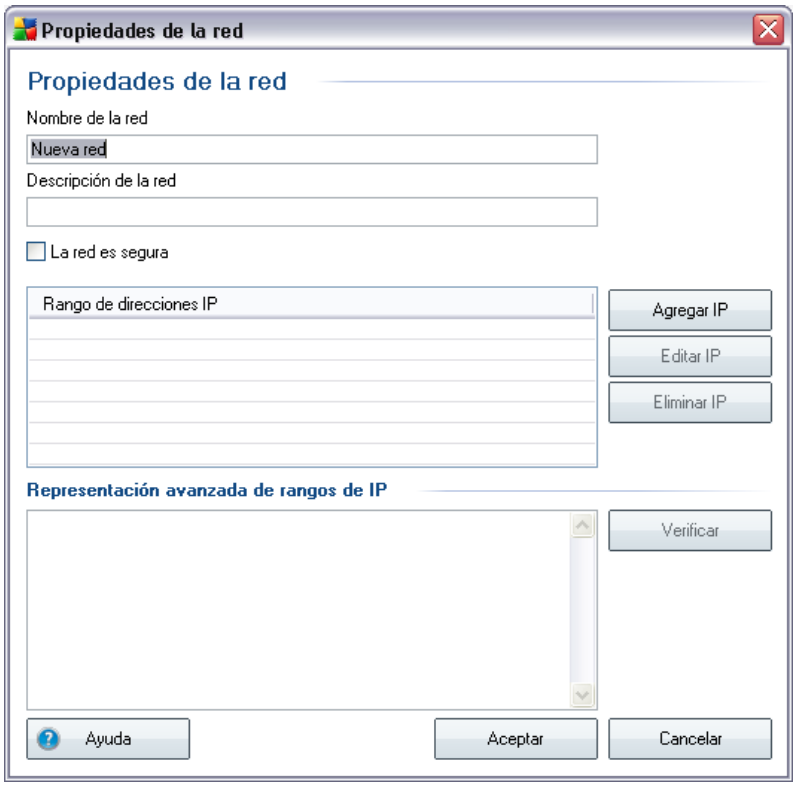

El diálogo ***Redes definidas*** ofrece una lista de todas las redes a las que está

conectada su equipo. De cada red detectada se proporciona la siguiente información:

- ***Redes*** : lista de los nombres de todas las redes a las que está conectado el equipo
- ***Seguridad de red***: de forma predeterminada, todas las redes se consideran no seguras, y sólo si está seguro de que la red es segura, puede asignarle dicho valor (*haga clic en el elemento de la lista que haga referencia a la red mencionada y seleccione Segura en el menú contextual*); todas las redes seguras se incluirán en el grupo de redes que se pueden comunicar con el grupo de reglas establecido para Permitir seguras
- ***Rango de dirección IP***: cada red se detectará de forma automática y se especificará como un rango de direcciones IP

## Botones de control

- ***Agregar red***: abre el diálogo ***Propiedades de red***, donde puede editar parámetros de la nueva red definida:




Dentro de este diálogo, puede especificar el ***Nombre de la red***, dar la ***Descripción de red*** y posiblemente asignar la red como segura. La nueva red puede definirse de forma manual en un cuadro de diálogo independiente que se abre mediante el botón ***Agregar IP*** (de forma alternativa, ***Editar IP*** /***Eliminar IP***); dentro de este cuadro de diálogo puede especificar la red utilizando su rango o máscara IP.

Para establecer varias redes que deben definirse como parte de una red creada recientemente, puede utilizar la opción de ***Representación avanzada de rango IP***: introduzca la lista de todas las redes en el campo de texto respectivo (*es compatible con cualquier formato estándar* y presione el botón ***Comprobar*** para asegurarse de que se pueda reconocer el formato. A continuación, presione ***Aceptar*** para confirmar y guardar la información.

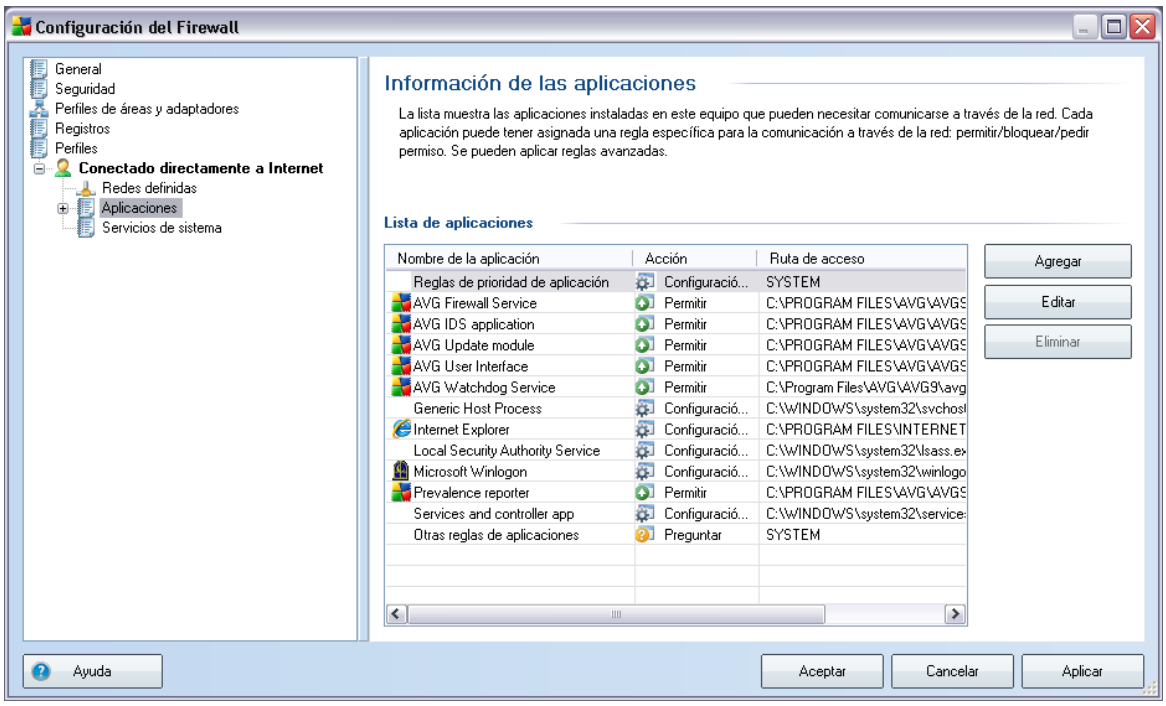
- ***Editar red***: abre la ventana del diálogo ***Propiedades de red*** (*ver arriba*), donde puede editar los parámetros de una red ya definida (*el diálogo es idéntico al diálogo para agregar una red nueva, consulte la descripción en el párrafo anterior*)

- ***Eliminar red***: elimina la nota de una red seleccionada de una lista de redes

- ***Marcar como segura***: de forma predeterminada, todas las redes se consideran no seguras, y sólo debe utilizar este botón para asignar el estado de segura a una red si está seguro de que la red lo es (*y viceversa, una vez que la red tiene asignado el estado de segura, el texto del botón cambia a "Marcar como no segura"*).

- ***Ayuda***: abre el archivo de ayuda relacionado con el diálogo activo

## 11.5.3. Aplicaciones




El cuadro de diálogo ***Información de las aplicaciones*** lista todas las aplicaciones instaladas que pueden necesitar comunicarse utilizando una red, y los iconos para la acción asignada:

- Permitir la comunicación para todas las redes

- Permitir la comunicación sólo para las redes definidas como Seguras

- Bloquear comunicación

- Mostrar cuadro de diálogo de pregunta (*el usuario podrá decidir en ese momento si desea permitir o bloquear la comunicación*)

- Configuración avanzada definida

Las aplicaciones de la lista se detectaron en su equipo (*y se les asignaron acciones respectivas*) ya sea durante la búsqueda del ***Asistente de configuración del Firewall*** o, en el caso de una aplicación desconocida o de reciente instalación, en un momento posterior.

***Nota: sólo se pueden detectar las aplicaciones ya instaladas, por lo que, si instala una aplicación nueva en el futuro, deberá definir las reglas de Firewall para ésta. De manera predeterminada, cuando la aplicación nueva intenta conectarse a través de la red por primera vez, el Firewall crea una regla automáticamente de acuerdo con la Base de datos confiable o le solicita que confirme si desea permitir o bloquear la comunicación. En el segundo caso, podrá guardar la respuesta como regla permanente (que se mostrará entonces en este cuadro de diálogo).***

Por supuesto, también puede definir reglas para la nueva aplicación de forma inmediata: en este cuadro de diálogo, presione ***Agregar*** e introduzca los detalles de la aplicación.

Además de las aplicaciones, la lista también contiene dos elementos especiales:

- ***Las reglas prioritarias de aplicaciones*** (*en la parte superior de la lista*) son preferenciales y siempre se aplican antes que las reglas específicas de las aplicaciones.

- ***Otras reglas de aplicaciones*** (*en la parte inferior de la lista*) se utilizan como "último recurso" cuando no se aplican reglas específicas para la aplicación, por ejemplo, para una aplicación desconocida e indefinida.

***Estos elementos tienen diferentes opciones de configuración para aplicaciones comunes y sólo deben utilizarlos los usuarios experimentados. Se recomienda encarecidamente no modificar la configuración***

## Botones de control

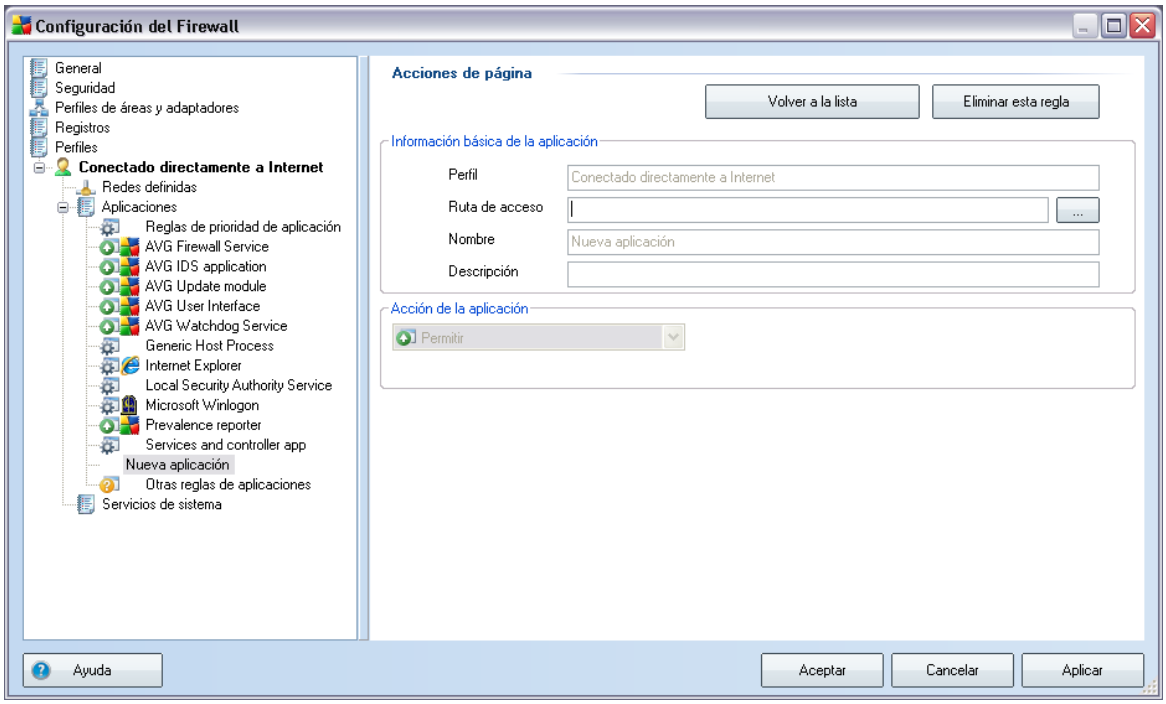
La lista puede editarse utilizando los siguientes botones de control:

- ***Agregar***: abre un cuadro de diálogo ***Acciones de página*** vacío para definir nuevas reglas de aplicación

- ***Editar***: abre el mismo cuadro de diálogo ***Acciones de página*** con datos proporcionados para editar el conjunto de reglas de una aplicación existente

- ***Eliminar*** : elimina la aplicación seleccionada de la lista

- ***Ayuda***: abre el archivo de ayuda relacionado con el diálogo activo




En este cuadro de diálogo, puede definir la configuración detallada para la aplicación respectiva.

## Acciones de página

- ***El botón Volver a la lista*** mostrará la descripción general de todas las reglas de aplicaciones definidas.

- ***El botón Eliminar esta regla*** borrará la regla de aplicación mostrada. Tenga en cuenta que esta acción no puede revertirse.

## Información básica de la aplicación

En esta sección, complete el campo ***Nombre*** con la aplicación y, de forma opcional, el campo ***Descripción*** (*un breve comentario para su información*). En el campo ***Ruta***, introduzca la ruta completa de la aplicación (*el archivo ejecutable*) en el disco; de forma alternativa, puede localizar la aplicación en la estructura de árbol al presionar el botón "***...***".

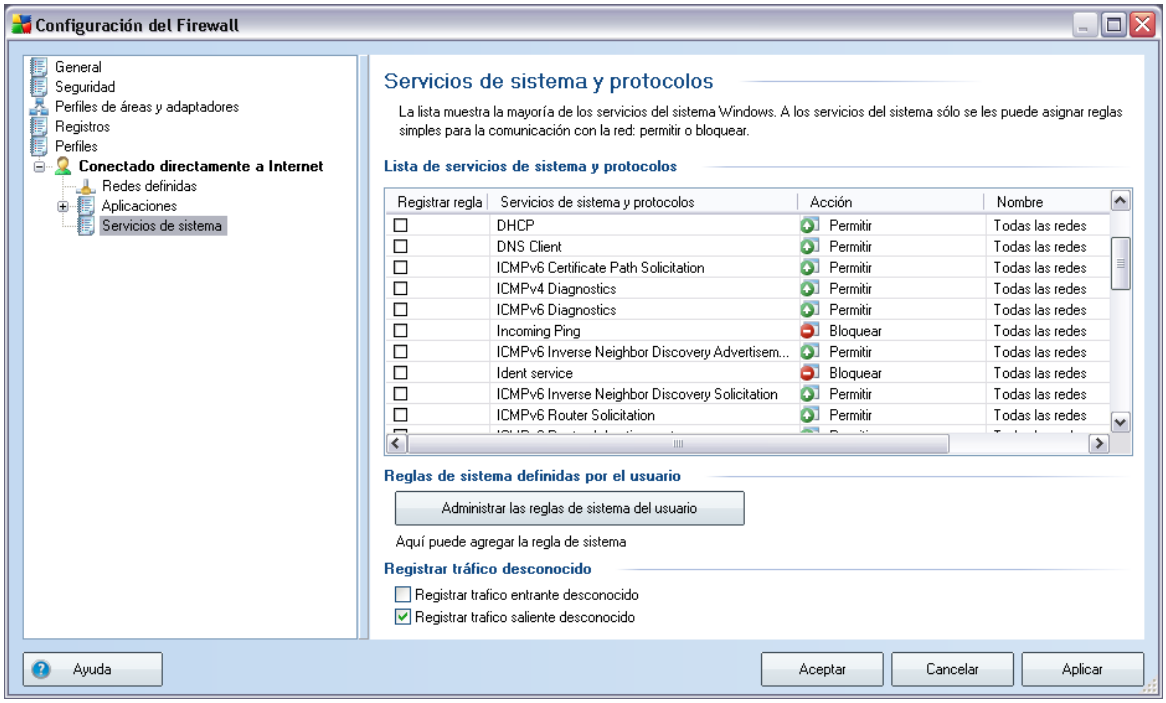
## Acción de la aplicación

En el menú desplegable, puede seleccionar la regla de Firewall para la aplicación, por ejemplo, lo que el Firewall debe hacer cuando la aplicación intenta comunicarse mediante la red:

- ***Permitir*** permitirá que la aplicación que se comunique utilizando todas las redes y adaptadores definidos sin limitaciones.
- ***Permitir seguras*** sólo permitirá que la aplicación se comunique utilizando redes definidas como Seguras (confiables).
- ***Bloquear*** prohibirá la comunicación automáticamente; la aplicación no podrá comunicarse utilizando ninguna red.
- ***Preguntar*** mostrará un diálogo que le permitirá decidir si desea permitir o bloquear el intento de comunicación en ese momento.
- ***Configuración avanzada*** muestra opciones de configuración más extensivas y detalladas en la parte inferior del cuadro de diálogo, en la sección ***Reglas de detalles de la aplicación***. Los detalles se aplicarán de acuerdo con el orden establecido en la lista, por lo que puede ***Mover arriba*** o ***Mover abajo*** las reglas en la lista para establecer su precedencia. Después de hacer clic en una regla específica de la lista, se mostrará la descripción general de los detalles de regla en la parte inferior del cuadro de diálogo. Cualquier valor en color azul subrayado puede modificarse haciendo clic en el cuadro de diálogo de configuración respectivo. Para eliminar la regla resaltada, presione ***Eliminar***. Si desea definir una regla nueva, utilice el botón ***Agregar*** para abrir el cuadro de diálogo ***Cambiar detalle de regla*** y especificar todos los detalles necesarios.

## 11.5.4. Servicios del sistema

***Se recomienda que sólo los usuarios expertos realicen cambios en el cuadro de diálogo Servicios y protocolos de sistema.***




El cuadro de diálogo ***Servicios y protocolos de sistema*** muestra los servicios y protocolos estándar de Windows que pueden necesitar comunicarse a través de la red. La tabla tiene las siguientes columnas:

- ***Registrar regla***: esta casilla permite activar la grabación de cada aplicación de la regla en los registros.
- ***Servicios y protocolos de sistema***: esta columna muestra el nombre del servicio de sistema respectivo.
- ***Acción***: esta columna muestra un icono para la acción asignada:
  - o Permitir la comunicación para todas las redes
  - o Permitir la comunicación sólo para las redes definidas como Seguras

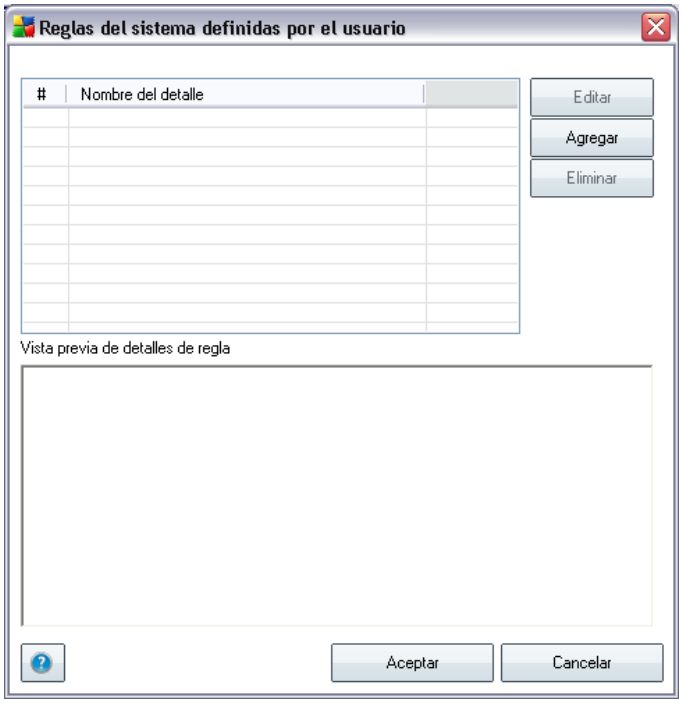
o Bloquear comunicación

- ***Redes***: esta columna establece las redes específicas en las que se aplica la regla de sistema.

La lista (*incluidas las acciones asignadas*) puede editarse mediante los siguientes botones:

- Para editar la configuración de cualquier elemento de la lista (*incluidas las acciones asignadas*), haga clic con el botón secundario en el elemento y seleccione ***Editar***.

- Para abrir un cuadro de diálogo nuevo y definir su propia regla de servicio de sistema (*consulte la siguiente imagen*), presione el botón ***Administrar las reglas de sistema del usuario***. La parte superior del cuadro de diálogo ***Reglas del sistema definidas por el usuario*** muestra una descripción general de los detalles de la regla del sistema que se está editando; la sección inferior muestra el detalle seleccionado. Los detalles de la regla definida por el usuario pueden editarse, agregarse o eliminarse mediante el botón correspondiente; los detalles de la regla definida por el fabricante sólo pueden editarse:



***Advertencia:*** *tenga en cuenta que esta configuración de detalle de regla es avanzada y está diseñada principalmente para los administradores de red que necesitan un control total sobre la configuración del Firewall. Si no está familiarizado con los tipos de protocolos de comunicación, los números de puertos de red, las definiciones de dirección IP, etc. no modifique esta configuración! Si realmente necesita cambiar la configuración, consulte los archivos de ayuda del cuadro de diálogo correspondiente para ver información específica.*

## Registrar tráfico desconocido

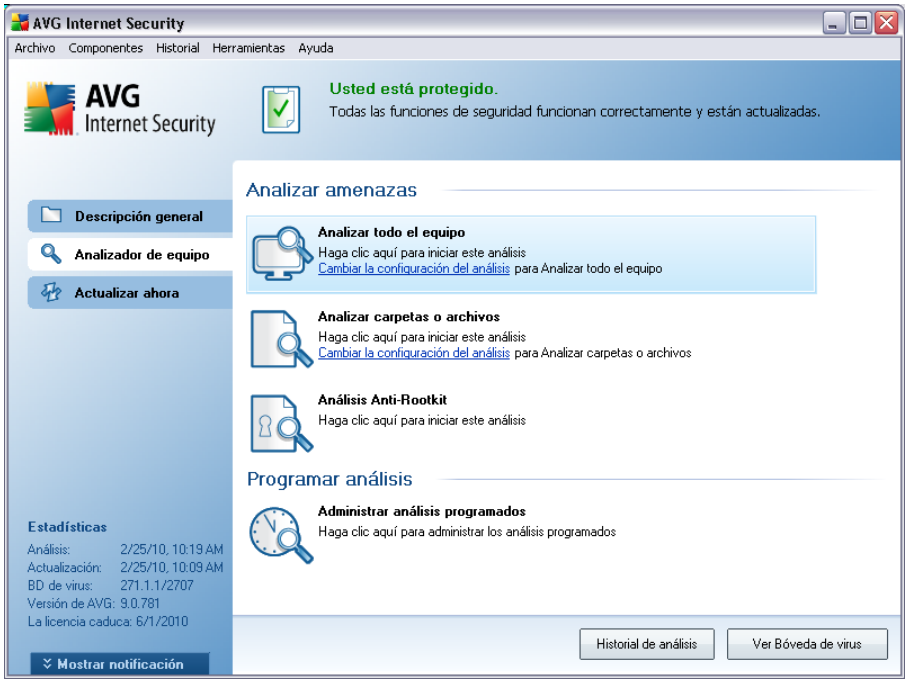
- ***Registrar tráfico entrante desconocido***: marque la casilla para guardar en los Registros cualquier intento desconocido para conectarse a su equipo desde fuera.

- ***Registrar tráfico saliente desconocido***: seleccione la casilla para guardar en los Registros cada intento desconocido para conectarse a su equipo desde fuera.

# 12. Análisis de AVG

El análisis es una parte crucial de la funcionalidad de **Anti-Virus AVG 9 más Firewall**. Puede realizar análisis a petición o programarlos para que se ejecuten periódicamente en los momentos apropiados.

## 12.1. Interfaz de análisis




Se puede obtener acceso a la interfaz de análisis de AVG mediante el vínculo rápido ***Analizador del equipo****. Haga clic en este vínculo para ir al diálogo ***Analizar en busca de amenazas***. En este diálogo encontrará las siguientes secciones:

- Descripción general de los análisis predefinidos: existen tres tipos de análisis definidos por el proveedor de software para su uso inmediato a pedido o programados:
  - ***Analizar todo el equipo***
  - ***Analizar carpetas o archivos específicos***
  - ***Análisis Anti-Rootkit***

- Sección de programación de análisis: en ella puede definir nuevos análisis y crear nuevas programaciones según convenga.

### Botones de control

Los botones de control disponibles en la interfaz de análisis son:

- ***Historial de análisis***: muestra el diálogo Descripción general de los resultados del análisis con todo el historial de análisis.
- ***Ver Bóveda de Virus***: abre una nueva ventana con la Bóveda de Virus, un espacio donde se ponen en cuarentena las infecciones detectadas.

## 12.2. Análisis predefinidos

Una de las funciones principales de **Anti-Virus AVG 9 más Firewall** es el análisis a pedido. Los análisis a pedido están diseñados para analizar varias partes de su equipo cuando existen sospechas de una posible infección de virus. De todas formas, se recomienda llevar a cabo dichos análisis con regularidad aun si no cree que se vayan a detectar virus en su equipo.

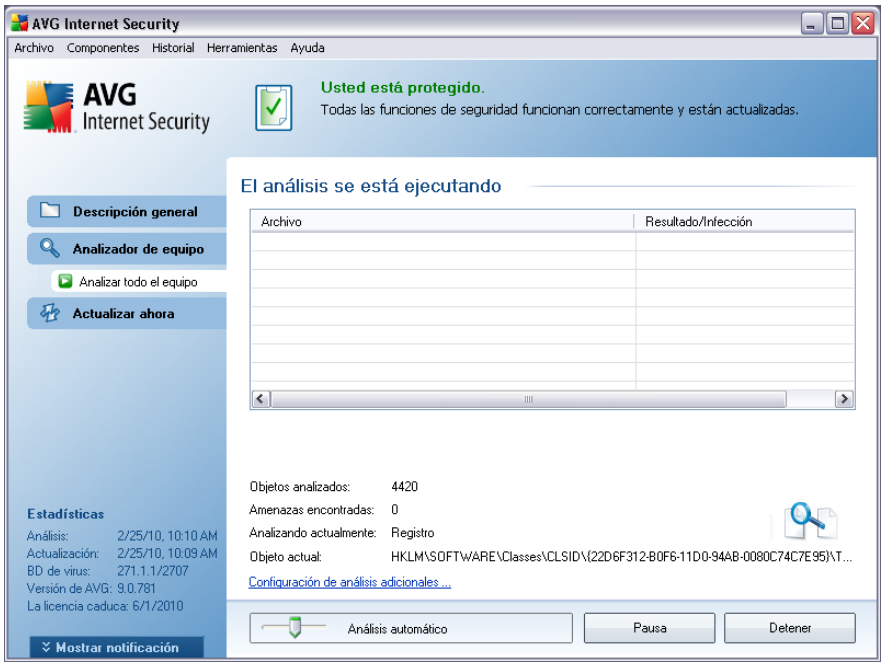
En **Anti-Virus AVG 9 más Firewall** encontrará dos tipos de análisis predefinidos por el proveedor del software:

### 12.2.1. Analizar todo el equipo

***Analizar todo el equipo***: analiza todo el equipo en busca de posibles infecciones o programas potencialmente no deseados. Este análisis analizará todos los discos duros del equipo y detectará y reparará los virus encontrados o eliminará la infección detectada a la ***Bóveda de Virus***. Se recomienda programar el análisis de todo el equipo en una estación de trabajo al menos una vez a la semana.

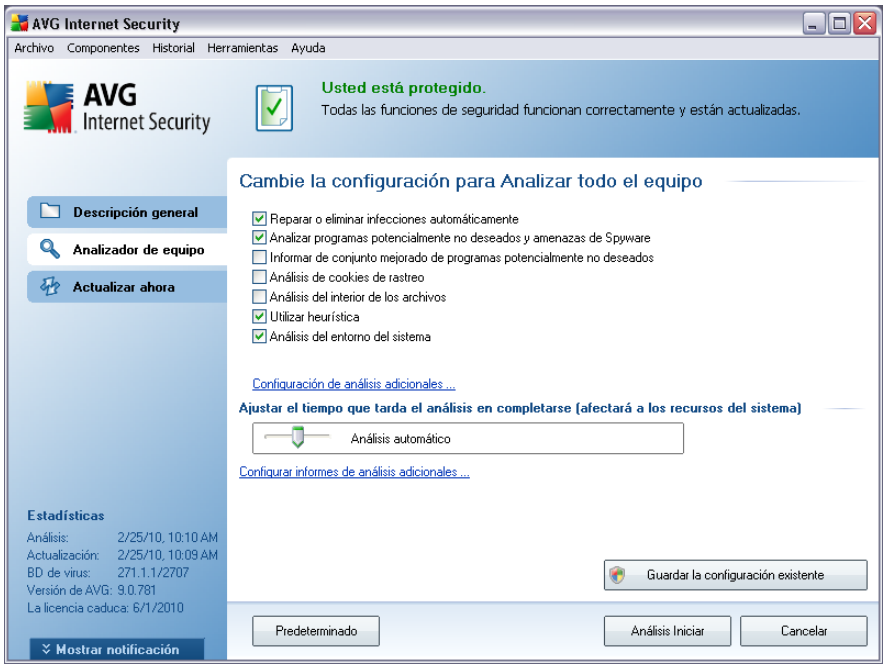
### Ejecución de análisis

El ***análisis de un equipo completo*** se puede ejecutar directamente desde la interfaz de análisis haciendo clic en el icono de análisis. No se deben configurar más parámetros específicos para este tipo de análisis; el análisis empezará inmediatamente en el cuadro de diálogo ***El análisis se está ejecutando*** (*consulte la captura de pantalla*). El análisis puede interrumpirse temporalmente (***Pausa***) o se puede cancelar (***Detener***) si es necesario.



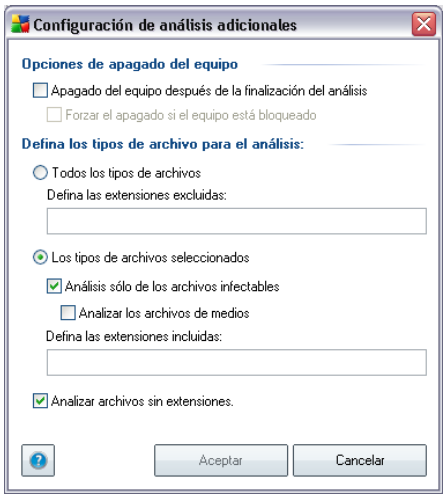

## Edición de la configuración de análisis

Tiene la opción de editar la configuración predeterminada predefinida de ***Análisis de todo el equipo***. Presione el vínculo ***Cambiar la configuración del análisis*** para ir al cuadro de diálogo ***Cambiar configuración del análisis de todo el equipo. Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.***




- ***Parámetros del análisis***: en la lista de parámetros de análisis puede activar o desactivar parámetros según sea necesario. La mayoría de los parámetros están seleccionados de modo predeterminado y se utilizarán automáticamente durante el análisis.

- ***Configuración de análisis adicional***: el vínculo abre un nuevo cuadro de diálogo ***Configuración de análisis adicional***, donde puede especificar los siguientes parámetros:




- ***Opciones de apagado del equipo***: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

- ***Defina los tipos de archivo para el análisis***: debe decidir si desea analizar:

  - ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;

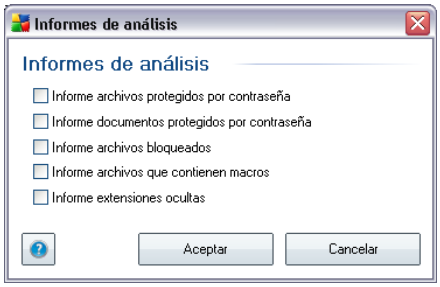
  - ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

  - En forma opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que

tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

- ***Prioridad del proceso de análisis***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De forma predeterminada, la prioridad se establece al nivel medio (*Análisis automático*), que optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

- ***Configurar informes de análisis adicionales***: el vínculo abre un nuevo cuadro de diálogo ***Informes de análisis***, donde puede seleccionar de qué tipos de posibles hallazgos se debería informar:




***Advertencia:*** *estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo* ***Análisis de AVG/Programación de análisis/Cómo analizar****. Si decide cambiar la configuración predeterminada de* ***Analizar todo el equipo****, puede guardar la nueva configuración como la predeterminada que se usará para posteriores análisis del equipo completo.*

## 12.2.2. Analizar carpetas o archivos específicos

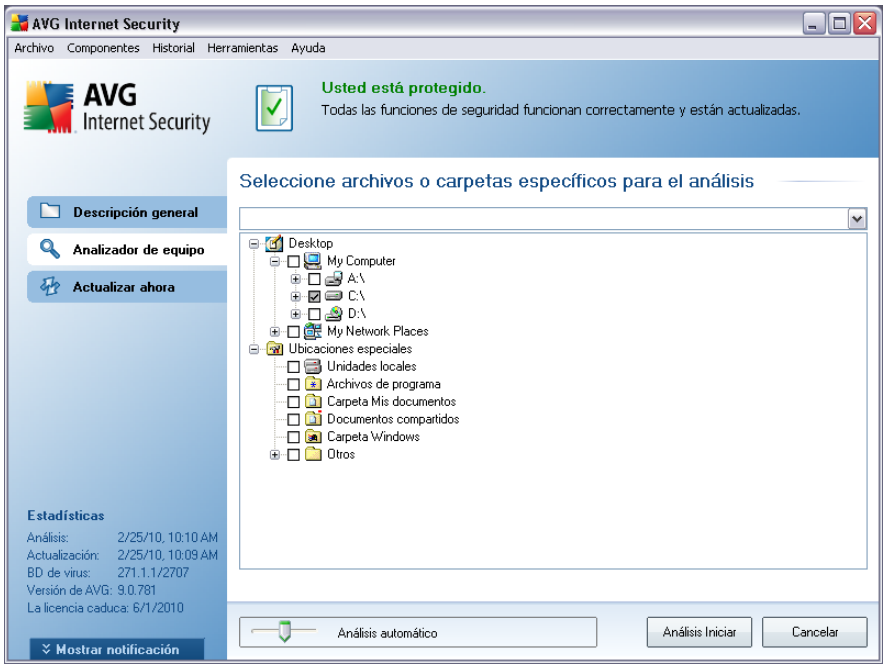
***Analizar carpetas o archivos específicos***: analiza únicamente las áreas del equipo que ha seleccionado que se analicen *(carpetas, discos duros, discos flexibles, CD, etc.)*). El procedimiento de análisis en caso de detección de virus y su tratamiento es el mismo que se realiza con el análisis de todo el equipo: los virus encontrados se reparan o eliminan a la ***Bóveda de Virus***. Puede emplear el análisis de archivos o carpetas específicos para configurar sus propios análisis y programas en función de sus necesidades.

### Ejecución de análisis

El ***análisis de archivos o carpetas específicos*** se puede ejecutar directamente desde la interfaz de análisis haciendo clic en el icono de análisis. Se abre un nuevo diálogo denominado ***Selección de archivos o carpetas específicos para el análisis***. En la estructura de árbol del equipo, seleccione aquellas carpetas que desea analizar. La ruta a cada carpeta seleccionada se genera automáticamente y aparece en el cuadro de texto de la parte superior de este diálogo.

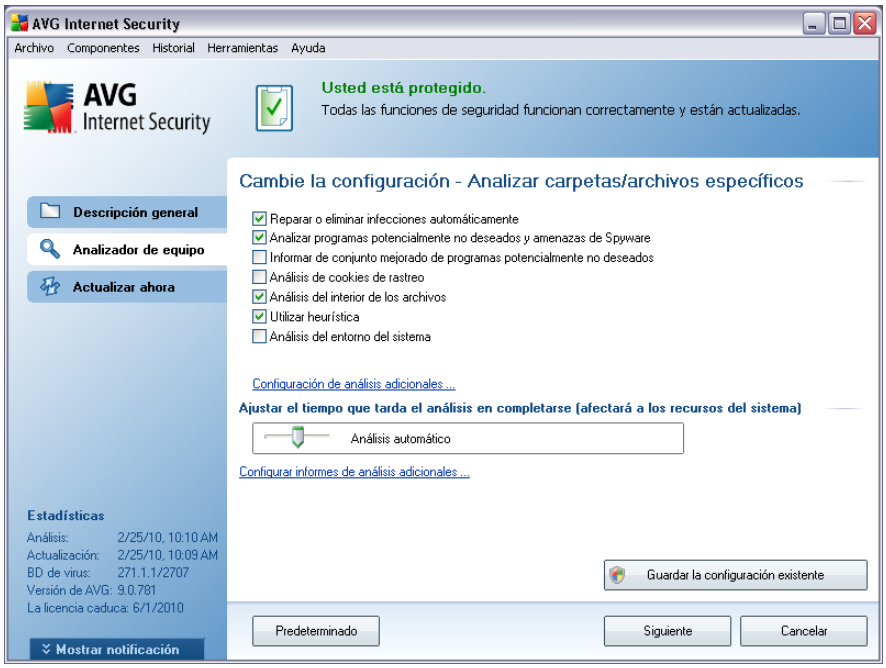
También existe la posibilidad de analizar una carpeta determinada y, a la vez, excluir de este análisis sus subcarpetas; para ello, escriba un signo menos "**-**" delante de la ruta generada automáticamente (*consulte la captura de pantalla*). Para excluir toda la carpeta del análisis utilice el signo de admiración "!" parámetro.

Finalmente, para iniciar el análisis, presione el botón ***Iniciar análisis***; el proceso de análisis es básicamente idéntico al análisis de todo un equipo.



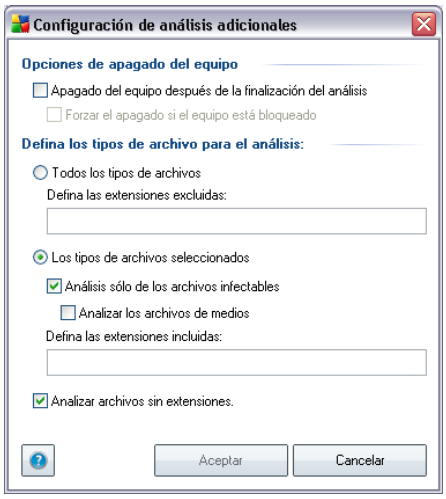

## Edición de la configuración de análisis

Tiene la opción de editar la configuración predeterminada predefinida de ***Análisis de archivos o carpetas específicos***. Presione el vínculo ***Cambiar la configuración del análisis*** para ir al diálogo ***Cambiar configuración de análisis de archivos o carpetas específicos***. ***Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.***




- ***Parámetros de análisis***: en la lista de parámetros de análisis puede activar o desactivar parámetros según sea necesario (*para obtener una descripción detallada de estos parámetros, consulte el capítulo Configuración avanzada de AVG/Análisis/Analizar carpetas o archivos específicos*).

- ***Configuración de análisis adicional***: el vínculo abre un nuevo cuadro de diálogo Configuración de análisis adicional, donde puede especificar los siguientes parámetros:




- ***Opciones de apagado del equipo***: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

- ***Defina los tipos de archivo para el análisis***: será conveniente decidir si desea analizar:

  - ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;

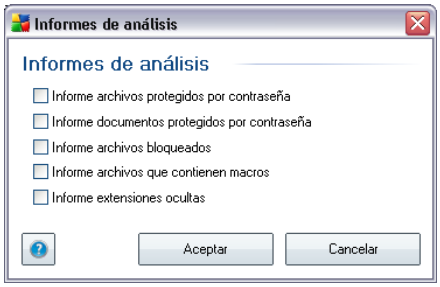
  - ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

  - En forma opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que

tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

- ***Prioridad del proceso de análisis***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De forma predeterminada, la prioridad se establece al nivel medio (*Análisis automático*), que optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

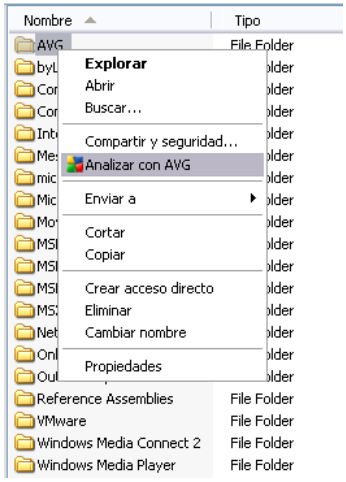
- ***Configurar informes de análisis adicionales***: el vínculo abre un nuevo diálogo de ***Informes de análisis***, donde puede seleccionar de qué tipos de posibles hallazgos se debería informar:




***Advertencia:*** *estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo* ***Análisis de AVG/Programación de análisis/Cómo analizar****. Si decide cambiar la configuración predeterminada de* ***Análisis de archivos o carpetas específicos*** *puede guardar la nueva configuración como la predeterminada que se usará para todos los análisis de archivos o carpetas específicos posteriores. Asimismo, esta configuración se utilizará como plantilla para todos los nuevos análisis programados (todos los análisis personalizados se basan en la configuración actual del análisis de archivos o carpetas específicos).*

## 12.3. Análisis en el Explorador de Windows

Además de los análisis predefinidos ejecutados para todo el equipo o sus áreas seleccionadas, **Anti-Virus AVG 9 más Firewall** también ofrece la opción de análisis rápido de un objeto específico directamente en el entorno del Explorador de Windows. Si desea abrir un archivo desconocido y no está seguro de su contenido, puede pedir que se compruebe. Siga estos pasos:




- Dentro del Explorador de Windows, resalte el archivo (o la carpeta) que desea comprobar.
- Haga clic con el botón secundario de su ratón sobre el objeto para abrir el menú de contexto.
- Seleccione la opción ***Analizar con AVG*** para que el archivo se analice con AVG

## 12.4. Análisis de línea de comandos

En **Anti-Virus AVG 9 más Firewall** existe la opción de realizar el análisis desde la línea de comandos. Puede utilizar esta opción, por ejemplo, en servidores, o bien al crear un script por lotes que se ejecutará automáticamente una vez reiniciado el equipo. Desde la línea de comandos, puede ejecutar el análisis con la mayoría de los parámetros ofrecidos en la interfaz gráfica de usuario de AVG.

Para ejecutar el análisis de AVG desde la línea de comandos, ejecute el siguiente comando en la carpeta donde se encuentra instalado AVG:

- ***avgscanx*** para SO de 32 bits
- ***avgscanx*** para SO de 64 bits

### Sintaxis del comando

La sintaxis del comando es la siguiente:

- ***avgscanx /parámetro*** ... p. ej., ***avgscanx /comp*** para analizar todo el equipo

- ***avgscanx /parámetro /parámetro*** .. con varios parámetros, estos deben alinearse en una fila y separarse mediante un espacio y un signo de barra

- si un parámetro requiere que se proporcione un valor específico (p. ej., el parámetro ***/scan*** requiere información sobre qué áreas seleccionadas del equipo se deben analizar, por lo que debe proporcionar una ruta de acceso exacta hasta la sección seleccionada), los valores se separan mediante punto y coma, por ejemplo: ***avgscanx /scan=C:\;D:***

### Parámetros del análisis

Para mostrar una descripción completa de los parámetros disponibles, escriba el comando respectivo junto con el parámetro /? o /HELP (por ejemplo, ***avgscanx /?***). El único parámetro obligatorio es /SCAN para especificar cuáles áreas del equipo se deben analizar. Para obtener una explicación más detallada de las opciones, consulte la descripción general de los parámetros de la línea de comandos.

Para ejecutar el análisis, presione ***Intro***. Durante el análisis, puede detener el proceso mediante ***Ctrl+C*** o ***Ctrl+Pausa***.

### Análisis de CMD iniciado desde la interfaz gráfica

Cuando ejecuta su equipo en el modo seguro de Windows, existe también la posibilidad de iniciar el análisis de la línea de comandos desde la Interfaz gráfica de usuario. El análisis en sí mismo se iniciará desde la línea de comandos, el diálogo ***Compositor de línea de comandos*** sólo le permite especificar la mayoría de los parámetros de análisis en la interfaz gráfica práctica.

Debido a que sólo se puede tener acceso a este diálogo dentro del modo seguro de Windows, para obtener la descripción detallada de este diálogo consulte el archivo de ayuda que se abre directamente desde el diálogo.

## 12.4.1. Parámetros del análisis de CMD

A continuación figura una lista de todos los parámetros disponibles para el análisis de la línea de comandos:

- ***/SCAN*** Analizar carpetas o archivos específicos /SCAN=ruta de acceso;ruta de acceso (por ejemplo /SCAN=C:\;D:\)

- ***/COMP*** Analizar todo el equipo
- ***/HEUR*** Utilizar análisis heurístico***
- ***/EXCLUDE*** Excluir ruta de acceso o archivos del análisis
- ***/@*** Archivo de comandos /nombre de archivo/
- ***/EXT*** Analizar estas extensiones /por ejemplo EXT=EXE,DLL/
- ***/NOEXT*** No analizar estas extensiones /por ejemplo NOEXT=JPG/
- ***/ARC*** Analizar archivos
- ***/CLEAN*** Borrar automáticamente
- ***/TRASH*** Mover los archivos infectados a la bóveda de virus***
- ***/QT*** Análisis rápido
- ***/MACROW*** Notificar macros
- ***/PWDW*** Notificar archivos protegidos por contraseña
- ***/IGNLOCKED*** Omitir archivos bloqueados
- ***/REPORT*** Informar a archivo /nombre de archivo/
- ***/REPAPPEND*** Anexar al archivo de reporte
- ***/REPOK*** Notificar archivos no infectados como correctos
- ***/NOBREAK*** No permitir la anulación de CTRL-BREAK
- ***/BOOT*** Activar la comprobación de MBR/BOOT
- ***/PROC*** Analizar los procesos activos
- ***/PUP*** Informar "Programas potencialmente no deseados"
- ***/REG*** Analizar registro
- ***/COO*** Analizar cookies
- ***/?*** Mostrar ayuda sobre este tema

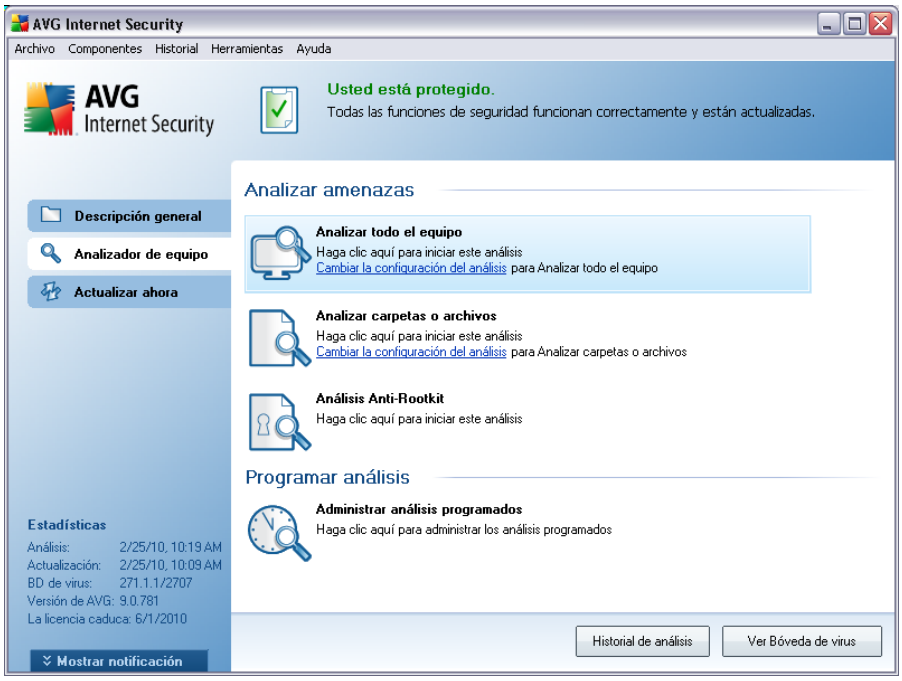
- ***/HELP*** Visualizar ayuda sobre este tema
- ***/PRIORITY*** Establecer prioridad de análisis /Baja, Automática, Alta/ (consulte Configuración avanzada / Análisis)
- ***/SHUTDOWN*** Apagado del equipo después de la finalización del análisis
- ***/FORCESHUTDOWN*** Forzar el apagado del equipo tras la finalización del análisis
- ***/ADS*** Analizar flujo de datos alternos (sólo NTFS)

## 12.5. Programación de análisis

Con **Anti-Virus AVG 9 más Firewall** puede ejecutar el análisis a pedido (por ejemplo cuando sospecha que se ha arrastrado una infección a su equipo) o según un plan programado. Es muy recomendable ejecutar el análisis basado en una programación: de esta manera puede asegurarse de que su equipo está protegido contra cualquier posibilidad de infección, y no tendrá que preocuparse de si y cuándo ejecutar el análisis.

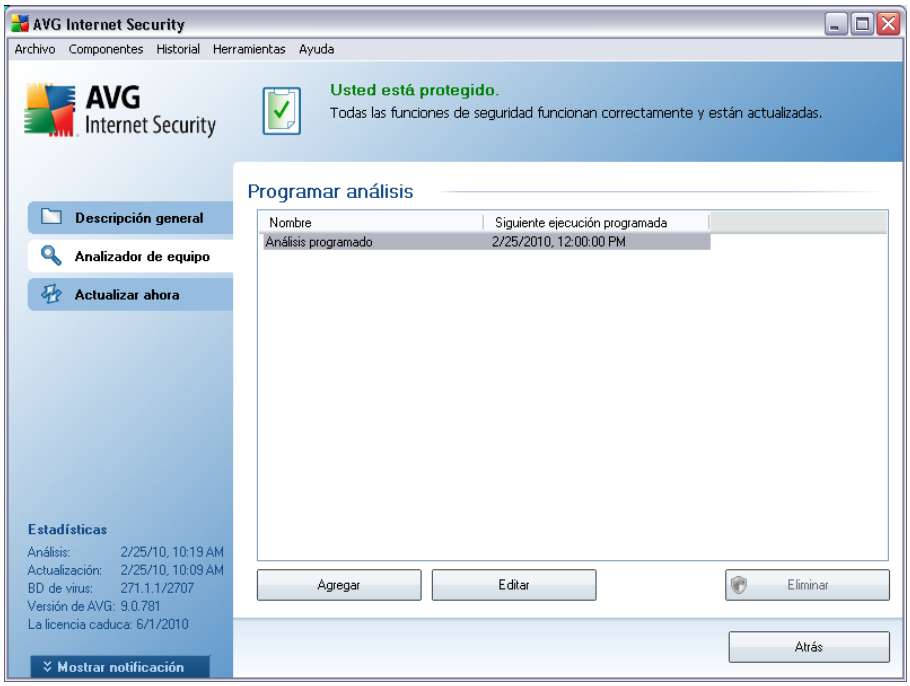
Se debe ejecutar el ***Análisis de todo el equipo*** periódicamente, al menos una vez a la semana. Sin embargo, si es posible, ejecute el análisis de todo su equipo diariamente, como está establecido en la configuración predeterminada de programación del análisis.Si el equipo siempre está encendido, se pueden programar los análisis fuera del horario de trabajo . Si el equipo algunas veces está apagado, se puede programar que los análisis ocurran durante un arranque del equipo, cuando no tenga tareas.

Para crear nuevas programaciones de análisis, consulte la interfaz de análisis de AVG y encuentre la sección en la parte inferior llamada ***Programación de análisis***:




## Programar análisis

Haga clic en el icono gráfico dentro de la sección ***Programar análisis*** para abrir un nuevo cuadro de diálogo ***Programar análisis*** donde podrá encontrar una lista de todos los análisis programados actualmente:




Puede editar o agregar análisis utilizando los siguientes botones de control:

- ***Agregar programación de análisis***: el botón abre el diálogo ***Configuración del análisis programado*** , pestaña***Configuración de programación***. En este diálogo puede especificar los parámetros del análisis recientemente definido.

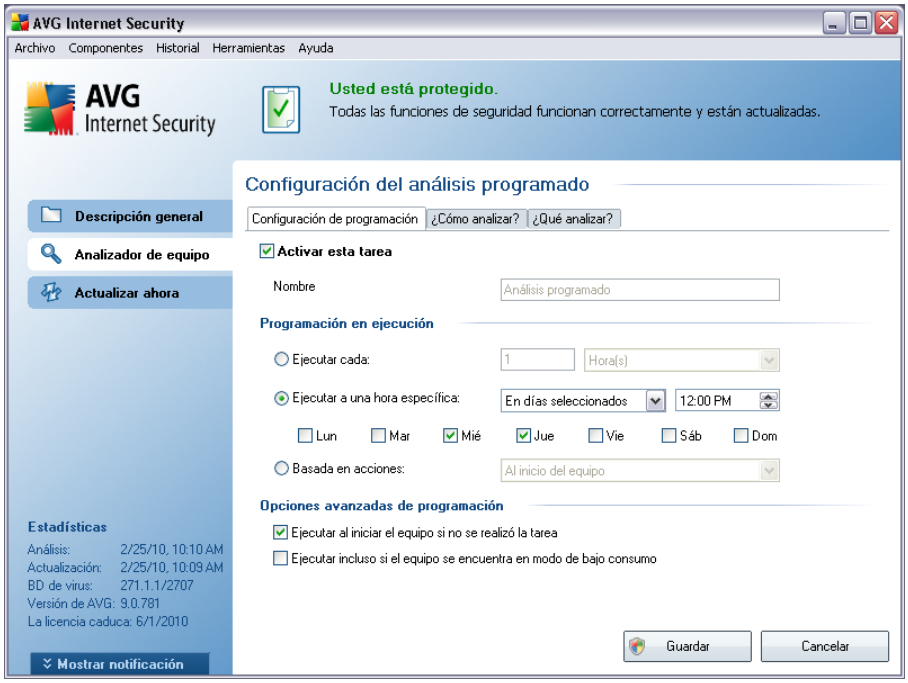
- ***Editar la programación de análisis***: este botón sólo se puede emplear si ha seleccionado previamente un análisis existente en la lista de análisis programados. En ese caso el botón aparece como activo y puede hacer clic en él para cambiar al diálogo ***Configuración del análisis programado***, pestaña ***Configuración de programación***. Los parámetros del análisis seleccionado ya están especificados aquí y se pueden editar.

- ***Eliminar la programación de análisis***: este botón también está activo si ha seleccionado previamente un análisis existente en la lista de análisis programados. Este análisis se puede eliminar de la lista presionando el botón de control. Sin embargo, sólo puede eliminar sus propios análisis; la ***Programación de análisis de todo el equipo*** predefinida dentro de la programación predeterminada nunca se puede eliminar.

- ***Atrás***: permite volver a la interfaz de análisis de AVG

### 12.5.1. Configuración de programación

Si desea programar un nuevo análisis y su ejecución periódica, vaya al cuadro de diálogo ***Configuración del análisis programado*** (*haga clic en el botón* ***Agregar programación de análisis*** *en el cuadro de diálogo* ***Programar análisis***). El cuadro de diálogo está dividido en tres pestañas: ***Configuración de programación****: consulte la imagen siguiente* (*la pestaña predeterminada a la que se le enviará automáticamente* ), ***¿Cómo analizar?*** y ***¿Qué analizar?***.




En la pestaña ***Configuración de programación*** puede seleccionar o cancelar la selección del elemento ***Activar esta tarea*** para desactivar el análisis programado de forma temporal, y volverlo a activar cuando sea necesario.

A continuación, dé un nombre al análisis que está a punto de crear y programar. Escriba el nombre en el campo de texto mediante el elemento***Nombre***. Intente utilizar nombres cortos, descriptivos y adecuados para los análisis a fin de distinguirlos después fácilmente.

***Ejemplo:****no es adecuado llamar al análisis por el nombre "Nuevo análisis" o "Mi análisis" ya que estos nombres no hacen referencia a lo que el análisis realmente verifica. En cambio, un ejemplo de un buen nombre descriptivo sería "Análisis de áreas del sistema", etc. Además, no es necesario especificar en el nombre del análisis si es el análisis de todo el sistema o solo de archivos o carpetas seleccionados; sus*

*propios análisis siempre serán una versión específica del análisis de archivos o carpetas seleccionados.*

En este diálogo puede definir con más detalle los siguientes parámetros del análisis:

- ***Ejecución de la programación***: especifique los intervalos de tiempo de la ejecución del análisis recién programada. El tiempo se puede definir con la ejecución repetida del análisis tras un período de tiempo determinado ( ***Ejecutar cada...***), estableciendo una fecha y una hora exactas (***Ejecutar en un momento específico...***) o estableciendo un evento al que debe estar asociada la ejecución de análisis (***Acción basada en el inicio del equipo***).

- ***Opciones de programación avanzada***: esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

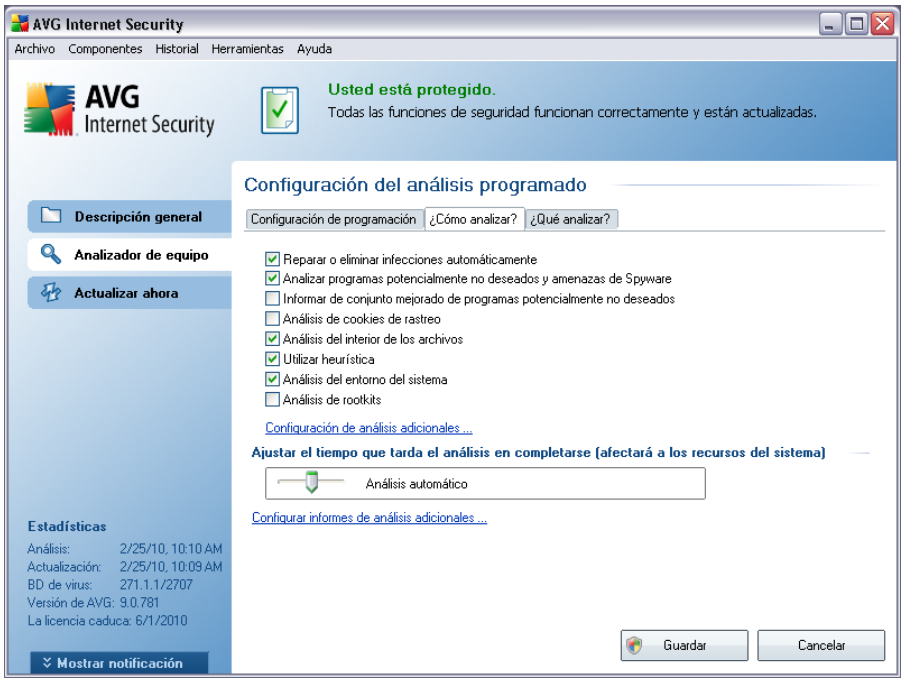
## Botones de control del diálogo Configuración del análisis programado.

Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo ***Configuración del análisis programado*** (***Configuración de programación***, ***¿Cómo analizar?*** y ***¿Qué analizar?***), y tienen el mismo funcionamiento sin importar en qué pestaña se encuentre:

- ***Guardar***: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después que haya especificado todos los requisitos.

- ***Cancelar***: cancela los cambios efectuados en esta pestaña o en cualquier otra pestaña de este diálogo y vuelve al diálogo predeterminado de la interfaz de análisis de AVG.

## 12.5.2. Cómo analizar




En la pestaña ***Cómo analizar*** se encontrará una lista de parámetros de análisis que de manera opcional se pueden activar/desactivar. De manera predeterminada, la mayoría de los parámetros están activados y su funcionamiento se aplicará durante el análisis. A menos que se cuente con una razón válida para cambiar esta configuración recomendamos mantenerla:

- ***Reparar o eliminar infecciones automáticamente*** (*activada de manera predeterminada*): si se identifica un virus durante el análisis, éste se puede reparar automáticamente si hay una vacuna disponible. Si no se puede reparar automáticamente el archivo infectado o decide desactivar esta opción, cada vez que se detecte un virus se le avisará y tendrá que decidir qué hacer con la infección detectada. El método recomendado consiste en eliminar el archivo infectado a la ***Bóveda de virus***.

- ***Analizar programas potencialmente no deseados y amenazas de Spyware*** (*activada de forma predeterminada*): seleccione esta opción para activar el motor ***Anti-Spyware*** y analizar en busca de spyware así como de virus. El spyware representa una categoría de malware dudoso: aunque normalmente significa un riesgo de seguridad, puede que algunos de estos programas se instalen a propósito. Recomendamos mantener esta función activada, ya que incrementa la seguridad del equipo

- ***Informar de conjunto mejorado de programas potencialmente no deseados***: si la opción anterior está activada, también puede seleccionar esta casilla para detectar un paquete extendido de spyware, es decir, programas que son totalmente correctos e inofensivos cuando se adquieren directamente del fabricante, pero que pueden emplearse con fines maliciosos posteriormente. Se trata de una medida adicional que aumenta aún más la seguridad de su equipo, pero que puede llegar a bloquear programas legales, por lo que de forma predeterminada está desactivada.

- ***Analizar cookies de rastreo*** (*activado de manera predeterminada*): este parámetro del componente ***Anti-Spyware*** define que deben detectarse cookies durante el análisis (*las cookies HTTP se utilizan para autenticar, rastrear y mantener información específica acerca de los usuarios, como los sitios que prefieren o los contenidos de sus carritos de compra electrónicos*);

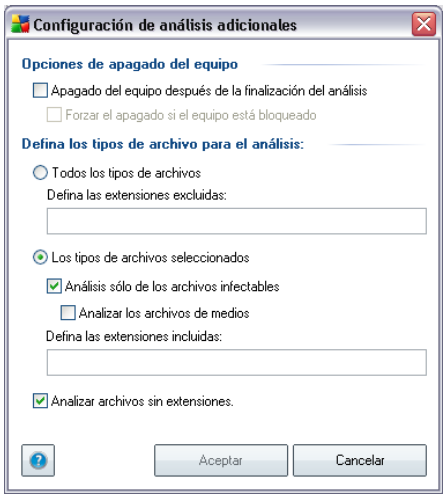
- ***Análisis del interior de los archivos*** (*activado, de manera predeterminada*): este parámetro defíne que el análisis debe comprobar todos los archivos, incluso aquellos que se encuentran comprimidos dentro de algún tipo de archivo, por ejemplo ZIP, RAR, ...

- ***Utilizar método heurístico*** (*activado, de manera predeterminada*): la emulación dinámica del análisis heurístico (*de las instrucciones del objeto analizadoen el entorno virtual del equipo*) será uno de los métodos empleados para la detección de virus durante el análisis;

- ***Analizar el entorno del sistema*** : (*activado, de manera predeterminada*): el análisis también comprobará las áreas del sistema del equipo;

A continuación, puede cambiar la configuración de análisis de la siguiente manera:

- ***Configuración de análisis adicional***: el vínculo abre un nuevo cuadro de diálogo ***Configuración de análisis adicional***, donde puede especificar los siguientes parámetros:




- ***Opciones de apagado del equipo***: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de análisis en ejecución. Después de haber confirmado la opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite que el equipo se apague aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

- ***Defina los tipos de archivo para el análisis***: debe decidir si desea analizar:

  - ***Todos los tipos de archivos*** con la posibilidad de definir excepciones al análisis proporcionando una lista de extensiones de archivo separadas por comas que no deben ser analizadas;

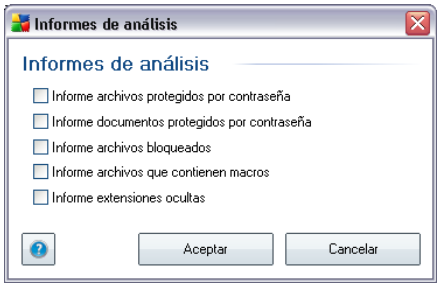
  - ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos que pueden resultar infectados (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos multimedia (*archivos de video, audio; si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis debido a que estos archivos normalmente son muy grandes y no son muy propensos a infecciones por virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

  - En forma opcional, puede decidir si desea ***Analizar archivos sin extensiones***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que

tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

- ***Prioridad del proceso de análisis***: puede utilizar el control deslizante para cambiar la prioridad del proceso de análisis. De forma predeterminada, la prioridad se establece al nivel medio (*Análisis automático*), que optimiza la velocidad del proceso de análisis y el uso de los recursos del sistema. De forma alternativa, puede ejecutar el proceso de análisis más lento, lo que significa que la carga de recursos del sistema se minimizará (*útil cuando se tiene que trabajar en el equipo pero no importa cuánto dure el análisis*) o más rápido con mayores requisitos de recursos del sistema (*p. ej. cuando el equipo está temporalmente desatendido*).

- ***Configurar informes de análisis adicionales***: el vínculo abre un nuevo cuadro de diálogo ***Informes de análisis***, donde puede seleccionar de qué tipos de posibles hallazgos se debería informar:




***Nota:*** *de manera predeterminada, la configuración del análisis está programado para un rendimiento óptimo. A menos que se tenga una razón válida para cambiar la configuración del análisis, se recomienda encarecidamente que se mantenga la configuración predefinida. Sólo los usuarios experimentados pueden llevar a cabo cualquier cambio en la configuración. Para las opciones adicionales de configuración del análisis, consulte el diálogo* ***Configuración avanzada*** *disponible través del elemento del menú del sistema* ***Archivo/Configuración avanzada*** *.*

## Botones de control

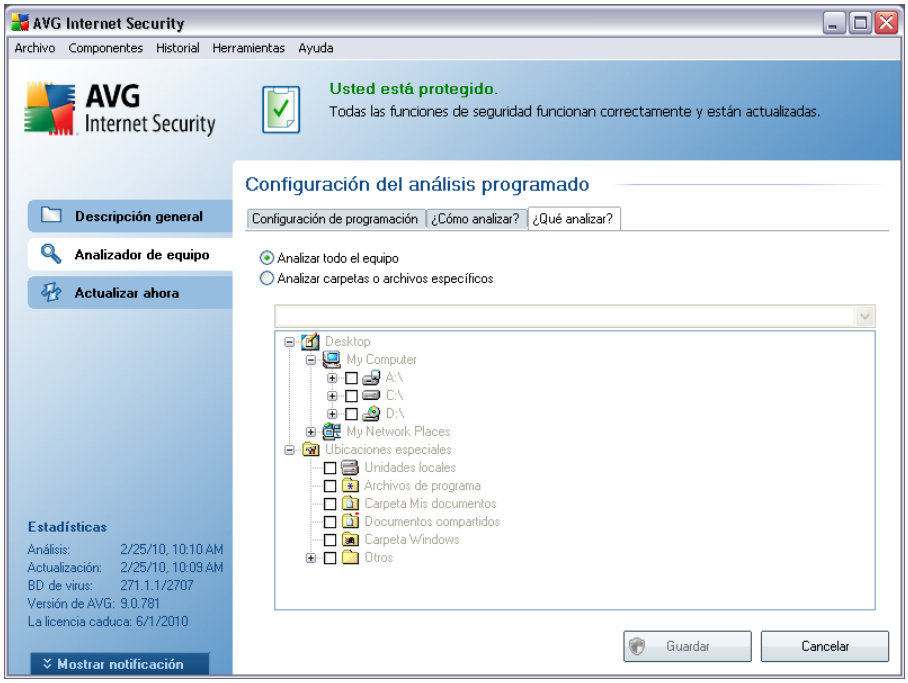
Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo ***Configuración del análisis programado*** (***Configuración de programación***, ***¿Cómo analizar?*** y ***¿Qué analizar?***) y tienen el mismo funcionamiento sin importar en cuál pestaña se encuentre:

- ***Guardar***: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al cuadro de diálogo

predeterminado de la interfaz de análisis de AVG. Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después que haya especificado todos los requisitos.

- ***Cancelar***: cancela los cambios efectuados en esta pestaña o en cualquier otra pestaña de este diálogo y vuelve al diálogo predeterminado de la interfaz de análisis de AVG.

### 12.5.3. Qué analizar




En la pestaña ***Qué analizar***puede definir si desea programar el análisis de todo el equipo o el análisis de archivos o carpetas específicos.

Si selecciona analizar archivos o carpetas específicos, en la parte inferior de este cuadro de diálogo se activará la estructura de árbol visualizada y podrá especificar las carpetas que se analizarán (*expanda los elementos haciendo clic en el nodo "más" hasta que encuentre la carpeta que desea analizar*). Puede seleccionar varias carpetas, seleccionando las casillas respectivas. Las carpetas seleccionadas aparecerán en el campo de texto en la parte superior del diálogo, y el menú desplegable mantendrá el historial de análisis seleccionados para uso posterior. De manera alternativa, puede introducir manualmente la ruta de acceso completa a la carpeta deseada (*si introduce varias rutas de acceso, es necesario separarlas con punto y coma, sin espacios*).

En la estructura de árbol también puede ver una rama denominada ***Ubicaciones especiales***. A continuación encontrará una lista de ubicaciones que se analizarán si se marca la casilla de verificación correspondiente:

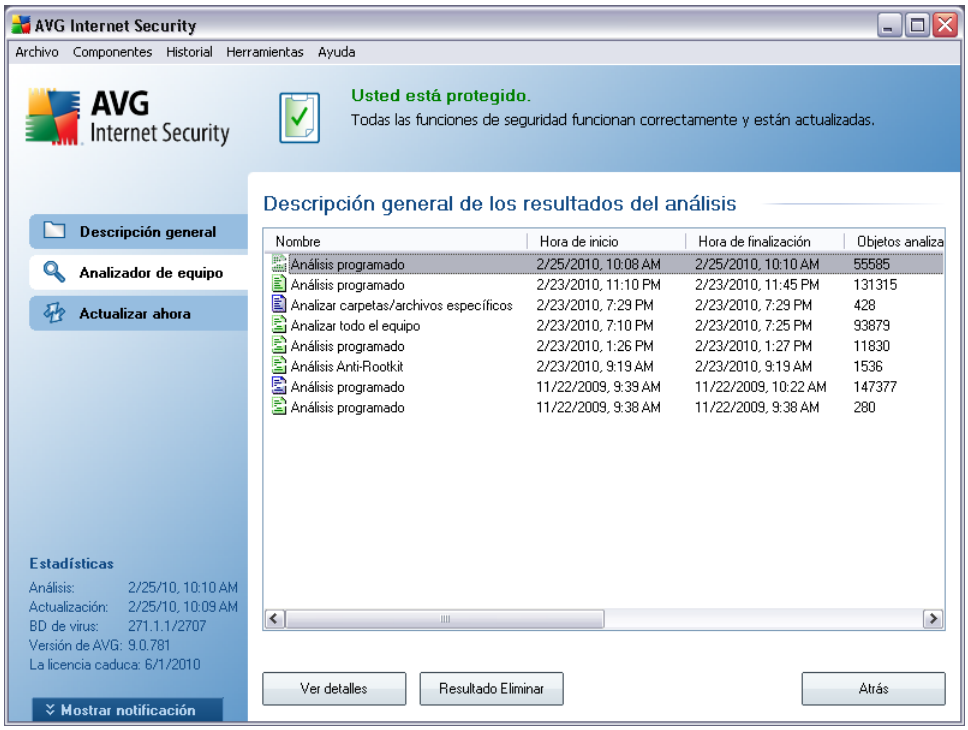
- ***Unidades locales***: todas las unidades de disco duro de su equipo
- ***Archivos de programa***: C:\Archivos de programa\
- ***Carpeta Mis documentos***: C:\Documents and Settings\User\Mis documentos\
- ***Documentos compartidos***: C:\Documents and Settings\All Users\Documents\
- ***Carpeta Windows***: C:\Windows\
- ***Otros***
    - *Unidad del sistema*: el disco duro en el cual está instalado el sistema operativo (normalmente C:)
    - *Carpeta de sistema*: Windows/System32
    - *Carpeta de archivos temporales*: Documents and Settings/User/Local Settings/Temp
    - *Carpeta de archivos temporales de Internet*: Documents and Settings/User/Local Settings/Temporary Internet Files

## Botones de control del diálogo Configuración del análisis programado.

Hay dos botones de control en cada una de las tres pestañas del cuadro de diálogo ***Configuración del análisis programado*** (***Configuración de programación***, ***¿Cómo analizar?*** y ***¿Qué analizar?***, y tienen el mismo funcionamiento sin importar en qué pestaña se encuentre:

- ***Guardar***: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este cuadro de diálogo y vuelve al cuadro de diálogo predeterminado de la interfaz de análisis de AVG. Por lo tanto, si desea configurar los parámetros de análisis en todas las pestañas, presione el botón para guardarlos sólo después que haya especificado todos los requisitos.
- ***Cancelar***: cancela los cambios efectuados en esta pestaña o en cualquier otra pestaña de este diálogo y vuelve al diálogo predeterminado de la interfaz de análisis de AVG.

## 12.6. Descripción general de los resultados del análisis




El diálogo ***Descripción general de los resultados del análisis*** está disponible desde la interfaz de análisis de AVGa través del botón***Historial de análisis*** El diálogo proporciona una lista de todos los análisis ejecutados anteriormente y la información de sus resultados:

- ***Nombre***: designación del análisis; puede ser el nombre de uno de los análisis predefinidos o un nombre que le haya dado a su propio análisis programado. Cada nombre incluye un icono que indica el resultado del análisis.

  - el icono verde indica que durante el análisis no se detectó ninguna infección

  - el icono azul indica que durante el análisis se detectó una infección, pero que el objeto infectado se eliminó automáticamente

  - el icono rojo indica que durante el análisis se detectó una infección y que no se pudo eliminar

  Cada icono puede ser sólido o cortado a la mitad: los iconos sólidos

representan un análisis que se completó y finalizó adecuadamente; el icono cortado a la mitad significa que el análisis se canceló o se interrumpió.

***Nota***: *para obtener información detallada sobre cada análisis, consulte el diálogo* ***Resultados del análisis*** *disponible a través del botón* ***Ver detalles*** *(en la parte inferior de este diálogo).*

- ***Hora de inicio***: fecha y hora en que se inició el análisis
- ***Hora de finalización***: fecha y hora en que finalizó el análisis
- ***Objetos analizados***: número de objetos que se verificaron durante el análisis
- ***Infecciones***: número de infecciones de virus detectadas/eliminadas
- ***Spyware*** : número de spyware detectados/eliminados
- ***Advertencias***: número de objetos sospechosos detectados
- ***Rootkits***: número de rootkits detectados
- ***Información de registros del análisis*** : información relacionada con el curso y el resultado del análisis (normalmente sobre su finalización o interrupción)

**Botones de control**

Los botones de control para el diálogo ***Descripción general de los resultados del análisis*** son:

- ***Ver detalles***: presione este botón para pasar al cuadro de diálogo ***Resultados del análisis*** para ver la información detallada sobre el análisis seleccionado
- ***Eliminar resultado***: presione este botón para eliminar el elemento seleccionado de la descripción general de resultados
- ***Atrás***: regresa al diálogo predeterminado de la interfaz de análisis de AVG

## 12.7. Detalles de los resultados del análisis

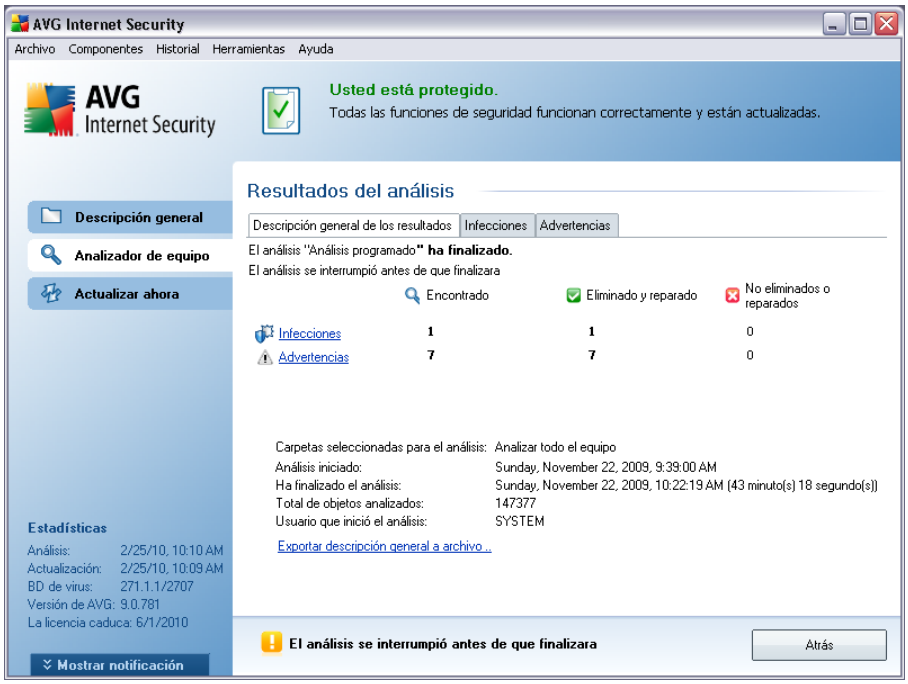
Si en el diálogo ***Descripción general de los resultados del análisis*** se selecciona un análisis específico, puede a continuación hacer clic en el botón ***Ver detalles*** para cambiar al diálogo ***Resultados del análisis***, que proporciona datos detallados sobre el

curso y resultado del análisis seleccionado.

El diálogo está dividido en varias pestañas:

- ***Descripción general de los resultados***: esta pestaña se visualiza en todo momento y proporciona los datos estadísticos que describen el progreso del análisis.
- ***Infecciones***: esta pestaña se visualiza sólo si durante el análisis se detectó una infección de virus.
- ***Spyware***: esta pestaña se visualiza sólo si durante el análisis se detectó un spyware.
- ***Advertencias***: esta pestaña se muestra si, por ejemplo, se detectaron cookies durante el análisis
- ***Información:*** esta pestaña se visualiza sólo si se detectaron algunas amenazas potenciales pero no se pudieron clasificar en ninguna de las categorías anteriores; entonces la pestaña proporciona un mensaje de advertencia del hallazgo. También se mostrará información sobre objetos que no pudieron analizarse (por ejemplo, archivos protegidos por contraseña).

## 12.7.1. Pestaña Descripción general de los resultados




En la pestaña ***Resultados del análisis*** puede consultar estadísticas detalladas con información sobre:

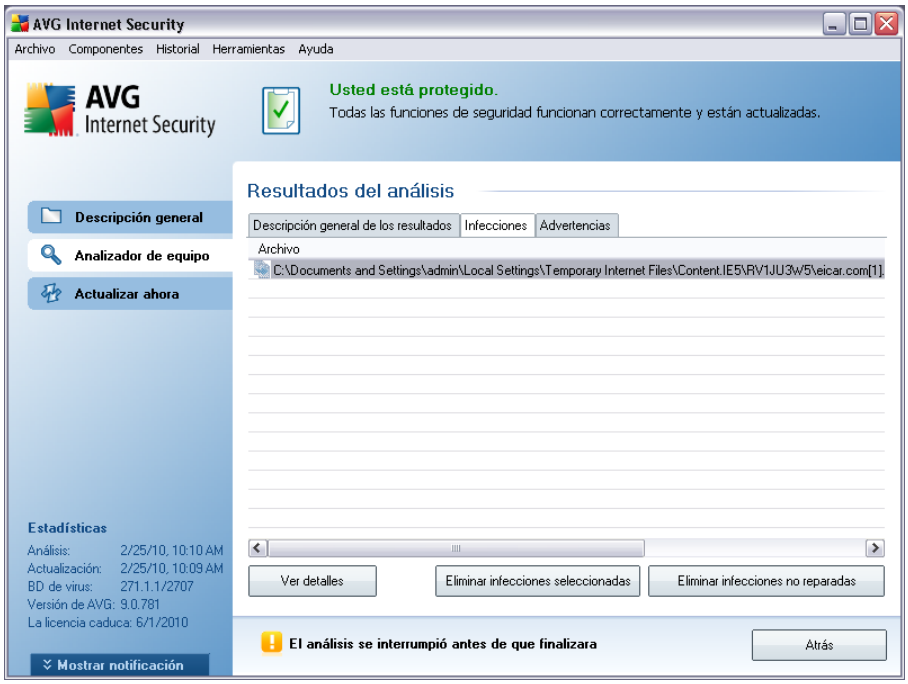
- Infecciones de virus/spyware detectadas
- Infecciones de virus/spyware eliminadas
- El número de infecciones de virus/spyware que no se han podido eliminar ni reparar

También encontrará información sobre la fecha y la hora exactas de la ejecución del análisis, el número total de objetos analizados, la duración del análisis y el número de errores que se han producido durante el análisis.

### Botones de control

En este diálogo, solo hay un botón de control disponible. El botón ***Cerrar resultados*** permite volver al diálogo ***Descripción general de los resultados del análisis***.

## 12.7.2. Pestaña Infecciones




La pestaña ***Infecciones*** sólo se muestra en el diálogo ***Resultados del análisis*** si durante el análisis se detecta una infección de virus. La pestaña se divide en tres secciones que facilitan la información siguiente:

- ***Archivo***: ruta completa de la ubicación original del objeto infectado.
- ***Infecciones***: nombre del virus detectado (*para obtener detalles sobre virus específicos, consulte la Enciclopedia de Virus en línea*).
- ***Resultado***: define el estado actual del objeto infectado detectado durante el análisis:
  - ***Infectado***: el objeto infectado se ha detectado y se ha dejado en su ubicación original (por ejemplo, si tiene *desactivada la opción de reparación automática**** en una configuración de análisis específica).
  - ***Reparado***: el objeto infectado se ha reparado automáticamente y se ha dejado en su ubicación original.
  - ***Movido a la Bóveda de Virus***: el objeto infectado se ha movido a la ***Bóveda de Virus***donde está en cuarentena.

- ***Eliminado***: el objeto infectado se ha eliminado.

- ***Agregado a excepciones de PPND***: el hallazgo se ha evaluado como una excepción y se ha agregado a la lista de excepciones de PPND ( *configurada en el diálogo* ***Excepciones PPND*** *en configuración avanzada*)

- ***Archivo bloqueado, no analizado*** : el objeto correspondiente está bloqueado, por lo que el programa AVG no puede analizarlo

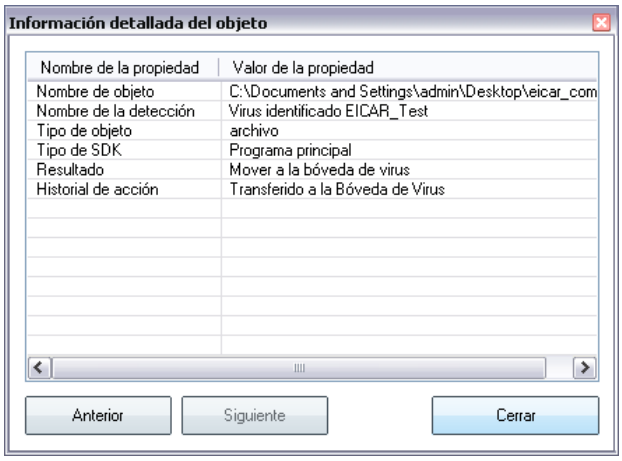
- ***Objeto potencialmente peligroso*** : el objeto se ha detectado como potencialmente peligroso pero no infectado (*puede que, por ejemplo, contenga macros*); la información es sólo una advertencia

- ***Para finalizar la acción, es necesario reiniciar el equipo***: el objeto infectado no se puede eliminar; para eliminarlo es preciso reiniciar el equipo.

## Botones de control

Hay tres botones de control disponibles en este diálogo:

- ***Ver detalles***: el botón abre una nueva ventana de diálogo denominada ***Información detallada de resultados del análisis***:




En este diálogo puede encontrar información sobre la ubicación del objeto infeccioso detectado (***Nombre de propiedad***). Mediante los botones ***Anterior***/***Siguiente*** puede ver información sobre hallazgos concretos. Utilice el botón ***Cerrar*** para cerrar este diálogo.

- ***Eliminar las infecciones seleccionadas***: utilice este botón para mover el hallazgo seleccionado a la ***Bóveda de Virus.***

- ***Eliminar todas las infecciones sin reparar***: este botón elimina todos los hallazgos que no se pueden reparar o mover a la ***Bóveda de Virus.***

- ***Cerrar resultados***: termina la vista general de información detallada y permite volver al diálogo ***Descripción general de los resultados del análisis***.

### 12.7.3. Pestaña Spyware

La pestaña ***Spyware*** solo se visualiza en el diálogo ***Resultados del análisis*** si se ha detectado spyware durante el análisis. La pestaña se divide en tres secciones que facilitan la información siguiente:

- ***Archivo***: ruta completa de la ubicación original del objeto infectado.

- ***Infecciones***: nombre del spyware detectado (*para obtener detalles sobre virus específicos, consulte la* ***Enciclopedia de Virus*** *en línea*).

- ***Resultado***: define el estado actual del objeto detectado durante el análisis:

  - ***Infectado***: el objeto infectado se ha detectado y se ha dejado en su ubicación original (por ejemplo, si tiene desactivada la opción de reparación automática en una configuración de análisis específica).

  - ***Reparado***: el objeto infectado se ha reparado automáticamente y se ha dejado en su ubicación original.

  - ***Movido a la Bóveda de Virus***: el objeto infectado se ha movido a la ***Bóveda de Virus*** donde está en cuarentena.

  - ***Eliminado***: el objeto infectado se ha eliminado.

  - ***Agregado a excepciones de PPND***: el hallazgo se ha evaluado como una excepción y se ha agregado a la lista de excepciones de PPND ( *configurada en el diálogo* ***Excepciones PPND*** *de la configuración avanzada*)

  - ***Archivo bloqueado, no analizado***: el objeto correspondiente está bloqueado, por lo que el programa AVG no puede analizarlo.

  - ***Objeto potencialmente peligroso***: el objeto se ha detectado como potencialmente peligroso pero no infectado (por ejemplo, puede contener

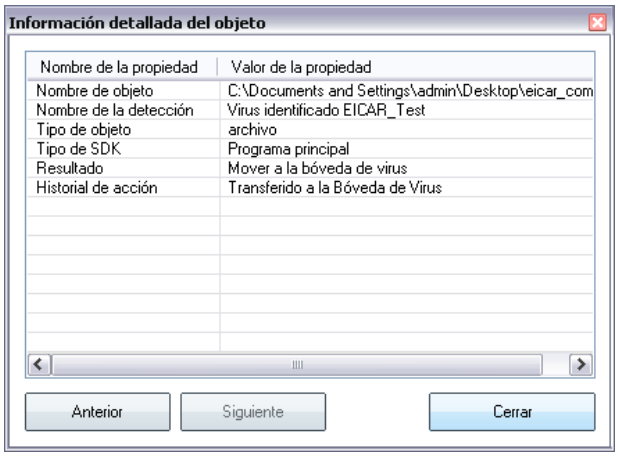
macros); la información es solo una advertencia.

- ***Para finalizar la acción, es necesario reiniciar el equipo***: el objeto infectado no se puede eliminar; para eliminarlo es preciso reiniciar el equipo.

## Botones de control

Hay tres botones de control disponibles en este diálogo:

- ***Ver detalles***: el botón abre una nueva ventana de diálogo denominada ***Información detallada de resultados del análisis***:




  En este diálogo puede encontrar información sobre la ubicación del objeto infeccioso detectado (***Nombre de propiedad***). Mediante los botones ***Anterior***/***Siguiente*** puede ver información sobre hallazgos concretos. Utilice el botón ***Cerrar*** para salir de este diálogo.

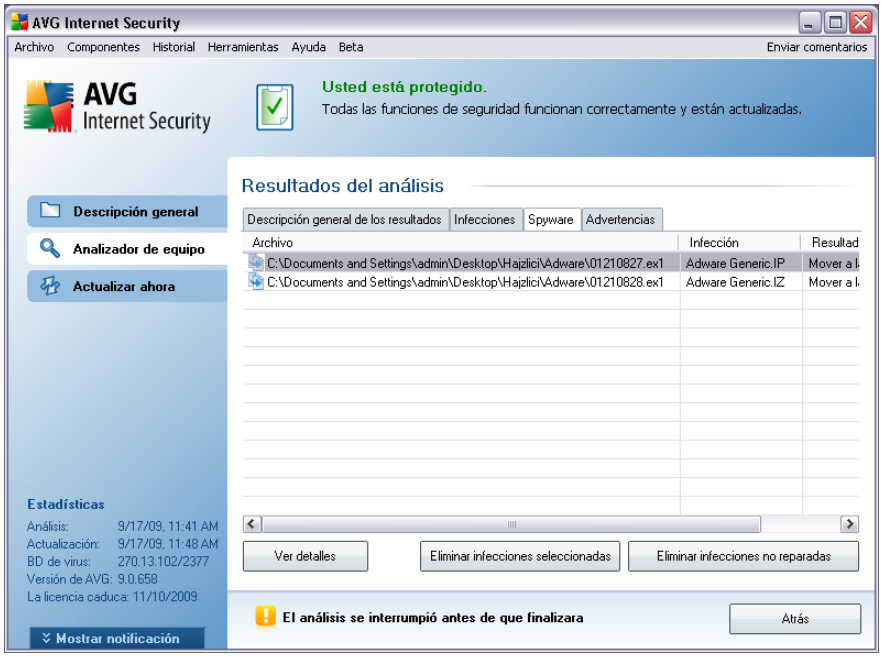
- ***Eliminar las infecciones seleccionadas***: utilice este botón para mover el hallazgo seleccionado a la ***Bóveda de Virus.***

- ***Eliminar todas las infecciones sin reparar***: este botón elimina todos los hallazgos que no se pueden reparar o mover a la ***Bóveda de Virus.***

- ***Cerrar resultados***: termina la vista general de información detallada y permite volver al diálogo ***Descripción general de los resultados del análisis***.

## 12.7.4. Pestaña Advertencias

La pestaña ***Advertencias*** muestra información sobre los objetos "sospechosos" ( *normalmente archivos*) detectados durante el análisis. Una vez detectados por la ***Protección residente***, se bloquea el acceso a estos archivos. Son ejemplos típicos de este tipo de hallazgos los archivos ocultos, las cookies, las claves de registro sospechosas, los documentos o archivos protegidos mediante contraseñas, etc.Estos archivos no presentan ninguna amenaza directa a su equipo o a su seguridad. La información acerca de estos archivos es generalmente útil en caso de que se detecte un adware o un spyware en el equipo. Si sólo hay advertencias detectadas por un análisis de AVG, no es necesaria ninguna acción.




Esta es una breve descripción de los ejemplos más comunes de tales objetos:

- ***Archivos ocultos***: de manera predeterminada, los archivos ocultos no son visibles en Windows, y algunos virus y otras amenazas pueden intentar evitar su detección almacenando sus archivos con este atributo. Si AVG informa acerca de un archivo oculto que sospecha que es malicioso, puede moverlo a la ***Bóveda de virus AVG***.

- ***Cookies***: las cookies son archivos de texto sin formato que utilizan los sitios Web para almacenar información específica del usuario, que posteriormente se utiliza para cargar el diseño personalizado del sitio Web, rellenar previamente el nombre de usuario, etc.

- ***Claves de registro sospechosas***: algunos malware almacenan su información en el registro de Windows, con el fin de asegurarse de que se cargan al iniciar el equipo o para prolongar su efecto en el sistema operativo.

### 12.7.5. Pestaña Rootkits

La pestaña ***Rootkits*** muestra información sobre los rootkits detectados durante el análisis si ejecutó el ***Análisis Anti-Rootkit*** o agregó manualmente la opción de análisis anti-rootkit a ***Análisis de todo el equipo*** (*esta opción se encuentra desactivada de manera predeterminada*).

Un ***rootkit*** es un programa diseñado para tomar el control fundamental de un sistema informático, sin la autorización de los propietarios ni de los administradores legítimos del sistema. Raramente se precisa acceso al hardware, ya que un rootkit está pensado para tomar el control del sistema operativo que se ejecuta en el hardware. Normalmente, los rootkits ocultan su presencia en el sistema mediante la subversión o evasión de los mecanismos de seguridad estándar del sistema operativo. A menudo, también son troyanos, con lo que engañan a los usuarios y les hacen creer que son seguros de ejecutar en los sistemas. Las técnicas empleadas para lograrlo pueden consistir en ocultar los procesos en ejecución a los programas de supervisión o esconder archivos o datos del sistema al sistema operativo.

La estructura de esta pestaña es básicamente la misma que la de la ***pestaña Infecciones*** o la ***pestaña Spyware***.

### 12.7.6. Pestaña Información

La pestaña ***Información*** contiene datos sobre los "hallazgos" que no se pueden clasificar como infecciones, spyware, etc. No se pueden etiquetar positivamente como peligrosos pero, sin embargo, merecen su atención. El análisis de AVG puede detectar archivos que quizás no están infectados pero que son sospechosos. Estos archivos se notifican como ***Advertencia*** o como ***Información***.

La ***Información*** de severidad se puede notificar por uno de los siguientes motivos:

- ***Tiempo de ejecución comprimido***: el archivo fue comprimido con uno de los empaquetadores de tiempo de ejecución menos comunes, algo que puede indicar un intento de evitar el análisis de dicho archivo. No obstante, no todos los reportes de dicho archivo indican la existencia de un virus.

- ***Tiempo de ejecución comprimido recursivo***: parecido al anterior, pero menos frecuente en software común. Estos archivos son sospechosos y se debería tener en cuenta la posibilidad de eliminarlos o someterlos a un análisis.

- ***Archivo o documento protegido por contraseña***: AVG no puede analizar los

archivos protegidos por contraseña (*ni cualquier otro programa anti-malware en general*).

- ***Documento con macros***: el documento notificado contiene macros, que pueden ser maliciosos.

- ***Extensión oculta***: los archivos con la extensión oculta pueden aparentar que son, por ejemplo, imágenes, pero en realidad son archivos ejecutables (*por ejemplo, imagen.jpg.exe*). La segunda extensión no es visible en Windows de forma predeterminada, y AVG reporta estos archivos para prevenir que se abran accidentalmente.

- ***Ruta de acceso del archivo incorrecta***: si algún archivo importante del sistema se ejecuta desde otra ruta de acceso que no sea la predeterminada ( *por ejemplo, si winlogon.exe se ejecuta desde otra carpeta que no sea Windows*), AVG notifica esta discrepancia. En algunos casos, los virus utilizan nombres de procesos estándar del sistema para hacer que su presencia sea menos aparente en el sistema.

- ***Archivo bloqueado***: el archivo notificado está bloqueado, por lo que AVG no puede analizarlo. Esto suele significar que el sistema utiliza un archivo constantemente (*por ejemplo, un archivo swap*).

## 12.8. Bóveda de virus

***Bóveda de Virus*** es un entorno seguro para administrar los objetos sospechosos/ infectados que se han detectado durante los análisis de AVG. Una vez que se detecta un objeto infectado durante el análisis, y AVG no puede repararlo de inmediato, se le pide que decida qué hacer con el objeto sospechoso. La solución recomendada es mover el objeto a la ***Bóveda de virus*** para tratarlo allí. El objetivo principal de la ***Bóveda de virus*** es conservar cualquier archivo eliminado durante un cierto periodo de tiempo, para que pueda asegurarse de que ya no necesita el archivo en la ubicación original. Si la ausencia de un archivo provoca problemas, puede enviar dicho archivo a análisis, o bien restaurarlo a su ubicación original.

La interfaz de la ***Bóveda de Virus*** se abre en una ventana aparte y ofrece una visión general de información sobre los objetos infectados en cuarentena:

- ***Severidad***: información del tipo de infección (*basada en el nivel de infección; todos los objetos enumerados pueden estar infectados o potencialmente infectados*)

- ***Nombre del virus***: especifica el nombre de la infección detectada conforme a la Enciclopedia de Virus (en línea).

- ***Ruta al archivo***: ruta completa de la ubicación original del archivo infeccioso detectado.

- ***Nombre del objeto original***: todos los objetos detectados listados en la tabla se han etiquetado con el nombre estándar dado por AVG durante el proceso de análisis. Si el objeto tenia un nombre original específico que es conocido (*por ejemplo el nombre de un dato adjunto de correo electrónico que no responde al contenido real del dato adjunto*), se proporcionará en esta columna.

- ***Fecha de almacenamiento***: fecha y hora en que se ha detectado el archivo sospechoso y se ha eliminado a la ***Bóveda de Virus.***

## Botones de control

Se puede tener acceso a los botones de control siguientes desde la interfaz de la ***Bóveda de Virus***:

- ***Restaurar***: devuelve el archivo infectado a su ubicación original en el disco.

- ***Restaurar como***: si decide mover el objeto infeccioso detectado de la ***Bóveda de virus*** hacia una carpeta seleccionada, utilice este botón. El objeto sospechosos y detectado se guardará con su nombre original. Si el nombre original no se conoce, se utilizará el nombre estándar.

- ***Detalles***: este botón sólo se aplica a las amenazas detectadas por ***Identity Protection***. Al hacer clic, aparece una descripción general de los detalles de la amenaza (*archivos o procesos que se han visto afectados, características del proceso, etc.*). Observe que para los elementos que no hayan sido detectados por IDP, este botón aparece en gris y está inactivo!

- ***Eliminar***: elimina el archivo infectado de la ***Bóveda de virus*** de forma total e irreversible.

- ***Vaciar la Bóveda de virus***: elimina todo el contenido de la ***Bóveda de virus*** permanentemente. Al eliminar los archivos de la Bóveda de virus, estos archivos se borran del disco de forma irreversible (no se transfieren a la Papelera de reciclaje).

# 13. Actualizaciones de AVG

**Mantener AVG actualizado es crucial para asegurar que todos los virus recién descubiertos se detecten tan pronto sea posible.**

Durante el proceso de instalación de AVG, se le solicitó que especificara la frecuencia con la que desea actualizar AVG. Las opciones disponibles son ***Cada 4 horas*** o ***Cada día*** (vea el cuadro de diálogo ***Programar análisis y actualizaciones automáticas***). Debido a que las actualizaciones de AVG no se publican de acuerdo con una programación fija, sino como reacción a la cantidad y severidad de las nuevas amenazas, se recomienda buscar actualizaciones al menos una vez al día. El buscar actualizaciones cada 4 horas garantizará que **Anti-Virus AVG 9 más Firewall** también estará actualizado durante el día.

## 13.1. Niveles de actualización

AVG permite seleccionar dos niveles de actualización:

- ***Actualización de definiciones*** contiene los cambios necesarios para una protección anti-virus, confiable. Por lo general, no incluye cambios del código y sólo actualiza la base de datos de definiciones. Esta actualización se debe aplicar tan pronto como esté disponible.

- ***Actualización del programa*** contiene diferentes modificaciones, arreglos y mejoras del programa.

Al programar una actualización, es posible seleccionar qué nivel de prioridad se descargará y se aplicará.

***Nota:*** *si coinciden una actualización programada y un análisis programado al mismo tiempo, el proceso de actualización tendrá más prioridad, y por consiguiente se interrumpirá el proceso de análisis.*

## 13.2. Tipos de actualización

Puede distinguir dos tipos de actualización:

- ***La actualización a pedido*** es una actualización inmediata de AVG que se puede realizar en cualquier momento en que sea necesaria.

- ***Actualización programada***: en AVG también se puede predefinir un plan de actualización. La actualización planificada se realiza entonces de manera periódica de acuerdo con la configuración establecida. Siempre que haya nuevos archivos de actualización en la ubicación especificada, se descargan ya sea directamente de Internet o desde el directorio de red. Cuando no hay

actualizaciones más recientes disponibles, nada sucede.

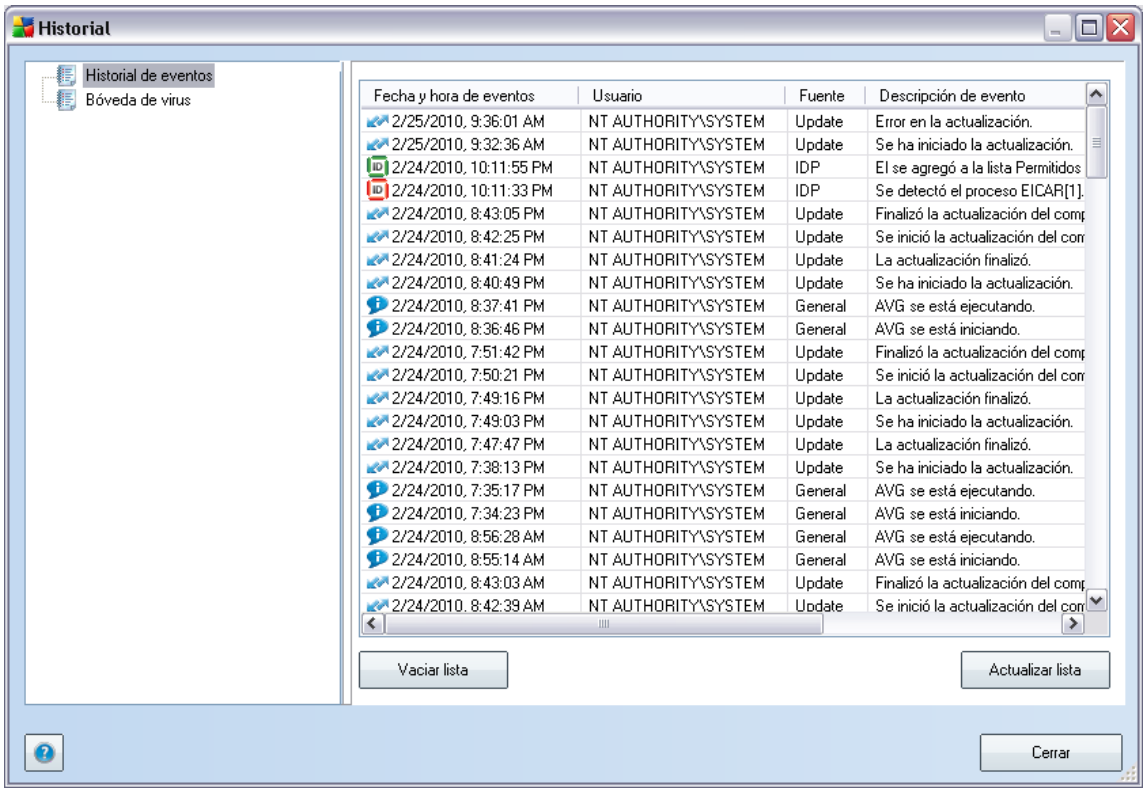
## 13.3. Proceso de actualización

El proceso de actualización se puede iniciar inmediatamente cuando se necesite, mediante el vínculo rápido ***Actualizar ahora***. Este vínculo está disponible en todo momento desde cualquier diálogo de la Interfaz del usuario de AVG . Sin embargo, es altamente recomendable llevar a cabo las actualizaciones regularmente como se establece en la programación de actualización editable dentro del componente Administrador de actualizaciones .

Una vez que se inicia la actualización, AVG verificará primero si hay nuevos archivos de actualización disponibles. De ser así, AVG empieza su descarga e inicia el proceso de actualización por sí mismo. Durante el proceso de actualización, se le enviará a la interfaz de ***Actualización***, en donde puede ver una representación gráfica del progreso del proceso, así como una descripción general de los parámetros estadísticos relevantes (*tamaño del archivo actualizado, datos recibidos, velocidad de descarga, tiempo transcurrido, etc.*).

***Nota**: antes del inicio de la actualización del programa AVG se crea un punto de restauración del sistema. Si el proceso de actualización falla y su sistema operativo se bloquea, podrá restaurar su sistema operativo a su configuración original desde este punto. Puede obtener acceso a esta opción mediante Inicio / Todos los programas / Accesorios / Herramientas del sistema / Restaurar sistema. Recomendado sólo para usuarios avanzados.*

# 14. Historial de eventos




Se puede tener acceso al cuadro de diálogo ***Historial de eventos*** desde el menú del sistema mediante el elemento ***Historial/Registro de historial de eventos***. En este cuadro de diálogo puede encontrar un resumen de los eventos importantes que se han producido durante el funcionamiento de **Anti-Virus AVG 9 más Firewall**. El ***Historial de eventos*** registra los siguientes tipos de eventos:

- Información sobre las actualizaciones de la aplicación AVG
- Comienzo, finalización o interrupción del análisis (incluidos los análisis realizados automáticamente)
- Eventos relacionados con la detección de virus (por Protección residente o durante el análisis), con la ubicación del evento incluida.
- Otros eventos importantes

## Botones de control

- ***Lista vacía***: elimina todas las entradas de la lista de eventos.
- ***Lista de actualizaciones***: actualiza todas las entradas de la lista de eventos.

# 15. Preguntas frecuentes y soporte técnico

Si se produce algún problema con AVG, ya sea comercial o técnico, consulte la sección ***Preguntas frecuentes*** del sitio Web de AVG (http://www.avg.com/).

Si no logra encontrar ayuda de esta manera, póngase en contacto con el servicio de soporte técnico a través del correo electrónico. Utilice el formulario de contacto, disponible en el menú del sistema a través de ***Ayuda/Obtener ayuda en línea***.