Anti-Virus AVG 9 más Firewall

Manual del usuario

Revisión del documento 90.6 (14.9.2009)

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 Requerimientos mínimos 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 13
4.4 Seleccionar tipo de licencia 14
4.5 Descargar archivos para instalar 15

5. Proceso de instalación de AVG 16

5.1 Ejecución de la instalación 16
5.2 Contrato de licencia 17
5.3 Verificando el estado del sistema 17
5.4 Seleccionar el tipo de instalación 18
5.5 Activar su licencia AVG 18
5.6 Instalación personalizada: carpeta de destino 20
5.7 Instalación personalizada: selección del componente 21
5.8 AVG DataCenter 22
5.9 Barra de herramientas AVG Security 23
5.10 Instalación de AVG 24
5.11 Programar análisis y actualizaciones automáticas 25
5.12 Selección de uso de equipo 25
5.13 Diseño de conexión en red de su equipo 26
5.14 La configuración de la protección AVG ha finalizado 27

6. Después de la instalación 28

6.1 Registro del producto 28
6.2 Acceso a la interfaz de usuario 28
6.3 Análisis de todo el equipo 28
6.4 Análisis Eicar 28

6.5 Configuración predeterminada de AVG 29

7. Interfaz del usuario de AVG 30

7.1 Menú del sistema 31
7.1.1 Archivo 31
7.1.2 Componentes 31
7.1.3 Historial 31
7.1.4 Herramientas 31
7.1.5 Ayuda 31
7.2 Información del estado de seguridad 34
7.3 Vínculos rápidos 35
7.4 Descripción general de los componentes 36
7.5 Estadísticas 37
7.6 Icono en la bandeja de sistema 37

8. Componentes de AVG 39

8.1 Antivirus 39
8.1.1 Antivirus Principios de 39
8.1.2 Interfaz de Antivirus 39
8.2 Anti-Spyware 41
8.2.1 Anti-Spyware Principios de 41
8.2.2 Interfaz de Anti-Spyware 41
8.3 Firewall 43
8.3.1 Principios de Firewall 43
8.3.2 Perfiles del Firewall 43
8.3.3 Interfaz de Firewall 43
8.4 Analizador de correos electrónicos 48
8.4.1 Principios del analizador de correos electrónicos 48
8.4.2 Interfaz del analizador de correos electrónicos 48
8.4.3 Detección del analizador de correos electrónicos 48
8.5 Licencia 52
8.6 Link Scanner 53
8.6.1 Principios de Link Scanner 53
8.6.2 Interfaz de Link Scanner 53
8.6.3 Protección de búsqueda AVG 53
8.6.4 Protección de navegación activa AVG 53
8.7 Web Shield 57
8.7.1 Principios de Web Shield 57

8.7.2 Interfaz de Web Shield *57*
8.7.3 Detección de Web Shield *57*
8.8 Protección residente 62
8.8.1 Protección residente Principios de *62*
8.8.2 Interfaz de protección residente *62*
8.8.3 Detección de protección residente *62*
8.9 Administrador de actualización 67
8.9.1 Principios de administrador de actualización *67*
8.9.2 Interfaz de administrador de actualización *67*
8.10 Barra de herramientas AVG Security 70
8.10.1 Barra de herramientas AVG Security Interfaz *70*
8.10.2 Opciones de la Barra de herramientas AVG Security *70*

9. Configuración avanzada de AVG 78

9.1 Apariencia 78
9.2 Sonidos 81
9.3 Ignorar condiciones de falla 82
9.4 Bóveda de Virus 83
9.5 Excepciones de PPND 84
9.6 Web Shield 87
9.6.1 Protección Web *87*
9.6.2 Mensajería instantánea *87*
9.7 Link Scanner 91
9.8 Análisis 92
9.8.1 Analizar todo el equipo *92*
9.8.2 Análisis de extensión de la shell *92*
9.8.3 Analizar carpetas o archivos específicos *92*
9.8.4 Análisis de dispositivos extraíbles *92*
9.9 Programaciones 99
9.9.1 Análisis programado *99*
9.9.2 Programación de actualización de la base de datos de virus *99*
9.9.3 Programación de actualización del programa *99*
9.10 Analizador de correos electrónicos 110
9.10.1 Certificación *110*
9.10.2 Filtro de correos electrónicos *110*
9.10.3 Registros y resultados *110*
9.10.4 Servidores *110*
9.11 Protección residente 118

9.11.1 Configuración avanzada *118*
9.11.2 Exclusiones de directorio *118*
9.11.3 Archivos excluidos *118*
9.12 Actualización 123
9.12.1 Proxy *123*
9.12.2 Conexión telefónica *123*
9.12.3 URL *123*
9.12.4 Administrar *123*

10. Configuración del Firewall 131

10.1 General 131
10.2 Seguridad 132
10.3 Perfiles de áreas y adaptadores 133
10.4 Registros 134
10.5 Perfiles 136
10.5.1 Información del perfil *136*
10.5.2 Redes definidas *136*
10.5.3 Aplicaciones *136*
10.5.4 Servicios del sistema *136*

11. Análisis de AVG 148

11.1 Interfaz de análisis 148
11.2 Análisis predefinidos 149
11.2.1 Analizar todo el equipo *149*
11.2.2 Analizar carpetas o archivos específicos *149*
11.3 Análisis en el Explorador de Windows 157
11.4 Análisis de línea de comandos 158
11.4.1 Parámetros del análisis de CMD *158*
11.5 Programación de análisis 161
11.5.1 Configuración de programación *161*
11.5.2 Cómo analizar *161*
11.5.3 Qué analizar *161*
11.6 Descripción general de los resultados del análisis 171
11.7 Detalles de los resultados del análisis 173
11.7.1 Pestaña Descripción general de los resultados *173*
11.7.2 Pestaña Infecciones *173*
11.7.3 Pestaña Spyware *173*
11.7.4 Pestaña Advertencias *173*

11.7.5 Pestaña Información *173*
11.8 Bóveda de virus 181
12. Actualizaciones de AVG 183
12.1 Niveles de actualización 183
12.2 Tipos de actualización 183
12.3 Proceso de actualización 183
13. Historial de eventos 185
14. Preguntas frecuentes y soporte técnico 187

1. Introducción

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

Enhorabuena 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. Como con todo los productos de AVG **Anti-Virus AVG 9 más Firewall** ha sido completamente rediseñado, desde la base, para entregar la protección de seguridad renombrada y acreditada de AVG en una forma nueva, más agradable y eficiente para el usuario.

Su nuevo **Anti-Virus AVG 9 más Firewall** producto 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. Requerimientos mínimos de hardware

Los siguientes son los requisitos mínimos de hardware del **Anti-Virus AVG 9 más Firewall**:

- Equipo Intel Pentium de 1.2 GHz
- 250 MB de espacio libre en el disco duro (para la instalación)
- 256 MB de memoria RAM

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 que estará instalando 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 seleccionar el archivo de instalación adecuado.

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 simple que le permite seleccionar el archivo de instalación adecuado para 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 (SP2 y posteriores), Windows Vista (todas las ediciones).*

Administrador de descargas de AVG está disponible para 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 el 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 establecer una conexión a Internet para 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 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. Seleccionar tipo de licencia

En este paso, se le solicitará que elija el tipo de licencia del producto que desea descargar. La descripción provista le permitirá seleccionar el que mejor le convenga:

- ***Versión completa*** : por ejemplo ***AVG Anti-Virus***, ***AVG Anti-Virus más Firewall***, o ***AVG Internet Security***
- ***Versión de prueba***: le permite utilizar todas las funciones del producto completo de AVG durante un tiempo limitado de 30 días.
- ***Versión gratuita***: proporciona protección gratuita para los usuarios domésticos, sin embargo, las funciones de la aplicación son limitadas. Además, la versión gratuita sólo incluye algunas de las funciones disponibles en el producto pagado.

4.5. Descargar archivos para instalar

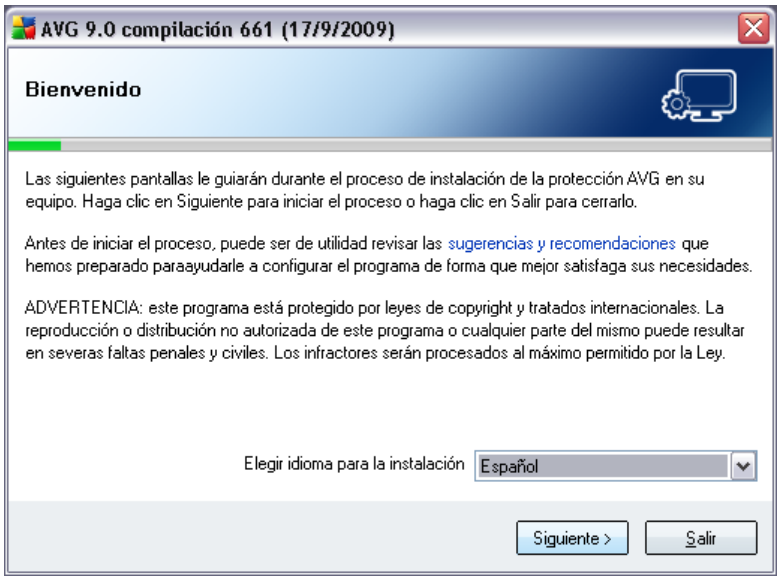
Ahora ha proporcionado toda la información necesaria para que **Administrador de descargas de AVG** inicie la descarga del paquete de instalación e inicie el proceso de instalación. A continuación, avance hacia el proceso de instalación de AVG.

5. Proceso de instalación de AVG

Para instalar en su equipo, necesita obtener el archivo de instalación más reciente. **Anti-Virus AVG 9 más Firewall** 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 del sitio web de AVG (http://www.avg.com/), sección ***Descargas***. 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

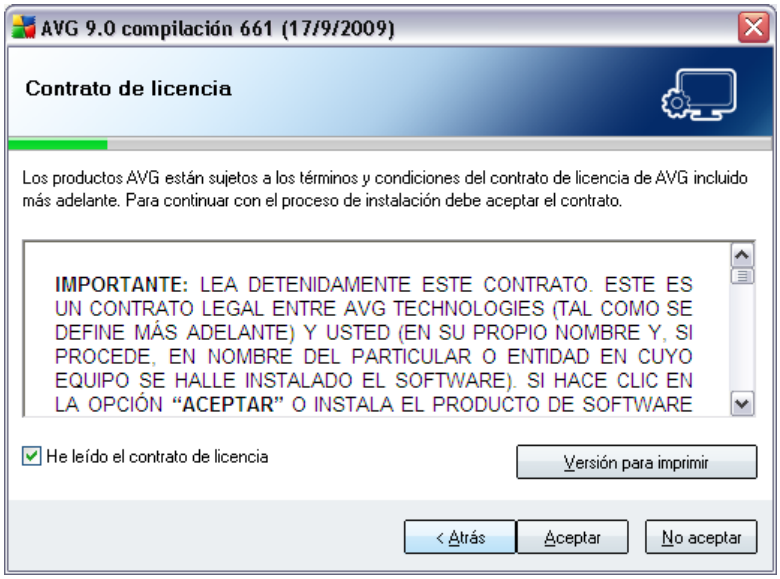


El proceso de instalación inicia con la ventana ***Bienvenido al programa de instalación de AVG*** . Aquí se selecciona el idioma empleado para el proceso de instalación. En la parte inferior de la ventana del diálogo, busque el elemento ***Elegir idioma para la instalación*** y seleccione el idioma 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



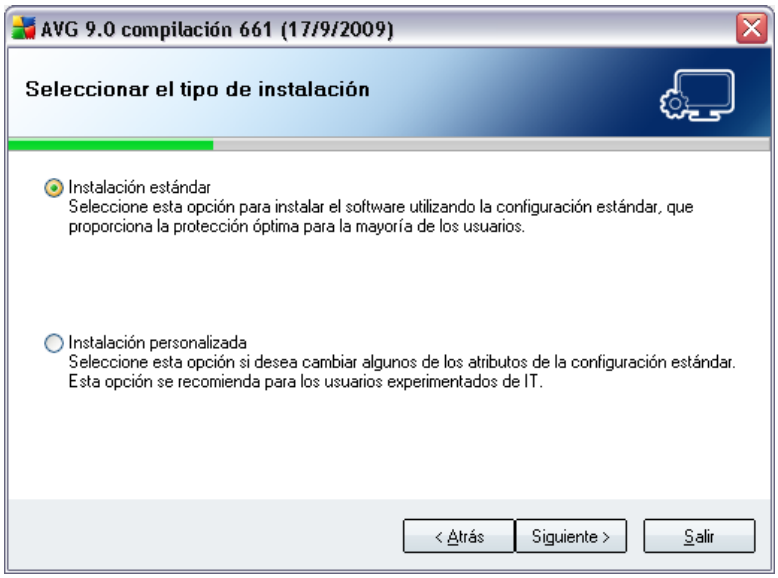
El diálogo ***Contrato de licencia*** muestra íntegramente el contrato de licencia de AVG. Lea detenidamente el contrato de licencia, y confirme que lo ha leído y entendido. A continuación, acéptelo seleccionando la casilla de verificación ***He leído el contrato de licencia*** y presionando el botón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

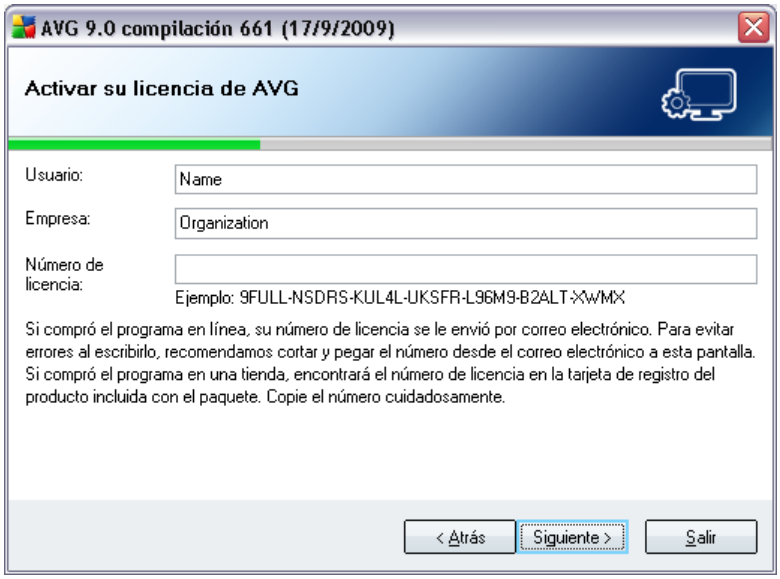
La instalación personalizada sólo deben utilizarla los usuarios con experiencia que tienen un motivo válido para instalar AVG con una configuración distinta de la estándar. Por ejemplo, para adaptarse a unos requisitos específicos del sistema.

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/número de venta en el campo de texto ***Número de licencia***. El número de venta se puede encontrar en el empaquetado 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

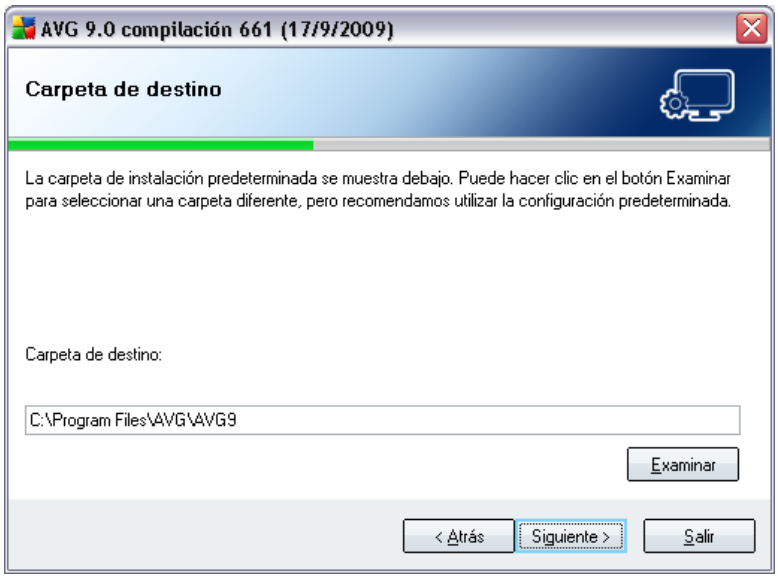
en línea de **Anti-Virus AVG 9 más Firewall**. Debe escribir el número exactamente como se muestra. Si está disponible el formulario digital del número de licencia (*en el correo electrónico*), se recomienda utilizar el método de copiar y pegar para insertarlo.



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 diálogo ***Carpeta de destino*** .

5.6. Instalación personalizada: carpeta de destino

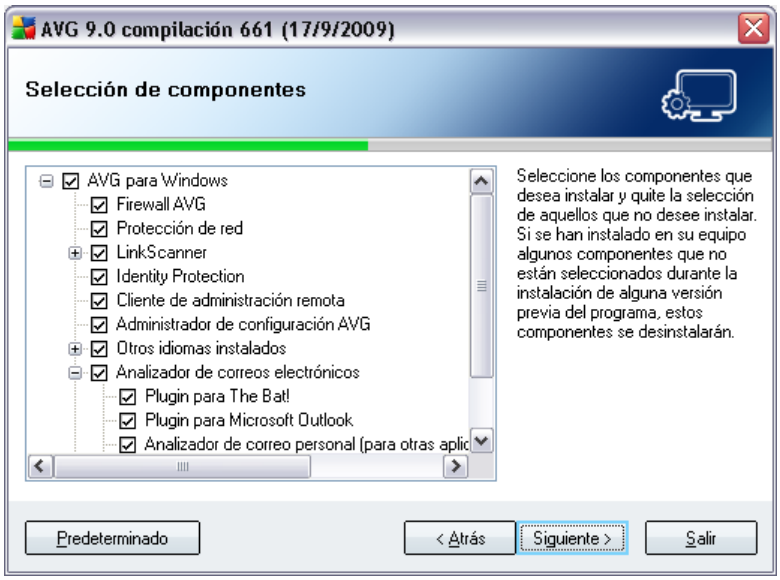


El diálogo ***Carpeta de destino*** permite especificar la ubicación donde se debe instalar **Anti-Virus AVG 9 más Firewall** De modo predeterminado, AVG se instalará en la carpeta de archivos de programa de la unidad C:. Si la carpeta no existe, un nuevo cuadro de diálogo le pedirá que confirme que 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 unidades y seleccione la carpeta correspondiente.

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

5.7. Instalación personalizada: selección del componente



El diálogo ***Selección de componentes*** muestra una descripción general de todos los componentes de **Anti-Virus AVG 9 más Firewall** que se pueden instalar. 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 (s) en que se instalará AVG. Seleccione el elemento ***Otros idiomas instalados*** y, a continuación, seleccione 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 personal*** para asegurar de forma automática la comunicación por correo electrónico, sin

importar el programa de correo electrónico que utilice.

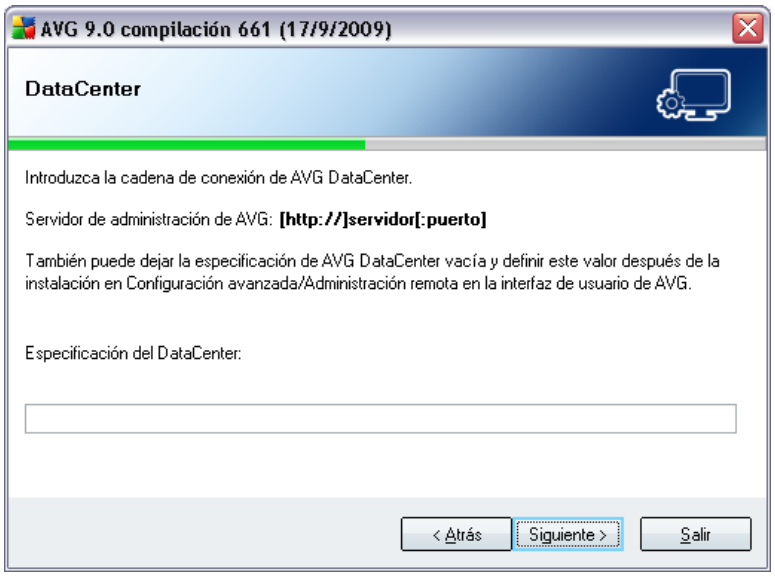
- ***Administración remota***

  Si planea conectar el equipo a AVG Remote Administration más adelante, seleccione también el elemento correspondiente que se va a instalar.

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

5.8. AVG DataCenter

Si en un cuadro de diálogo anterior de ***Instalación personalizada o Selección de componentes*** ha seleccionado que se instale el elemento ***Administración remota*** , es necesario especificar los parámetros de ***AVG DataCenter***:



En el campo de texto ***especificación de AVG DataCenter*** , proporcione la cadena de conexión a ***AVG DataCenter*** con el formato *servidor:puerto*. Si esta información no está disponible por el momento, deje el campo en blanco; más tarde, puede proporcionar la configuración en el cuadro de diálogo ***Configuración avanzada/ Administración remota***.

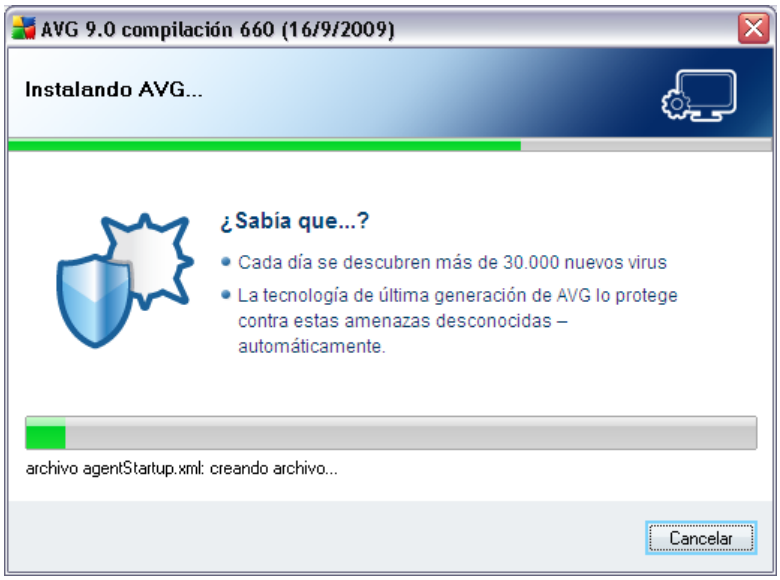
Nota: *para obtener información más detallada sobre AVG Remote Administration, consulte el manual del usuario de AVG Network Edition, que puede descargar del sitio web de AVG (http://www.avg.com/).*

5.9. Barra de herramientas AVG Security

En el cuadro de diálogo de la ***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 instala automáticamente en el navegador de Internet para proporcionarle una protección exhaustiva en línea mientras navega por la red.

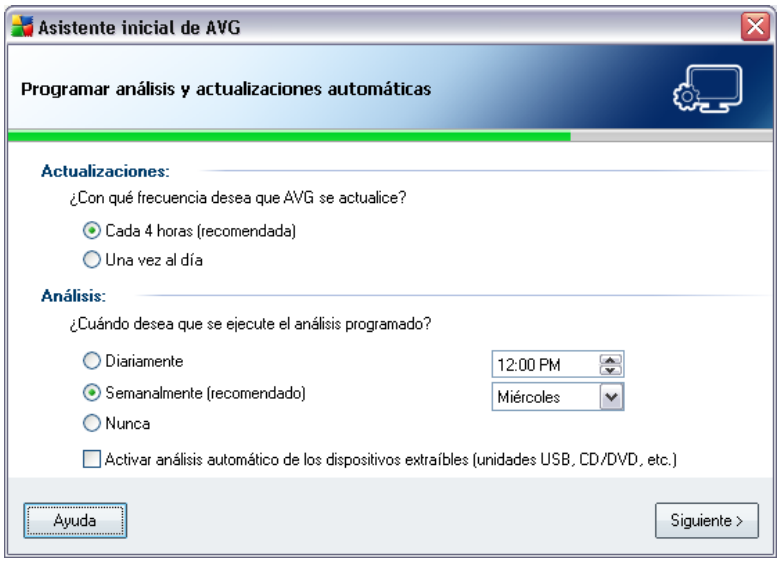
5.10. Instalación de AVG

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



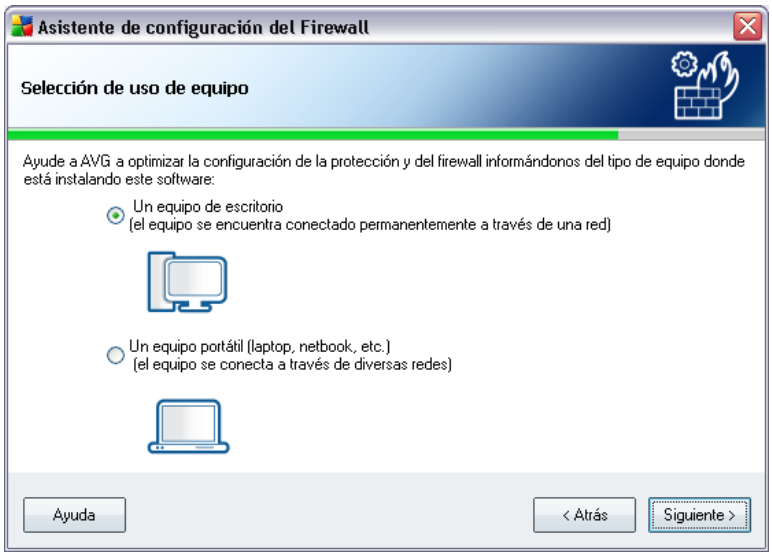
Después de finalizar el proceso de instalación, pasará al siguiente cuadro de diálogo automáticamente.

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



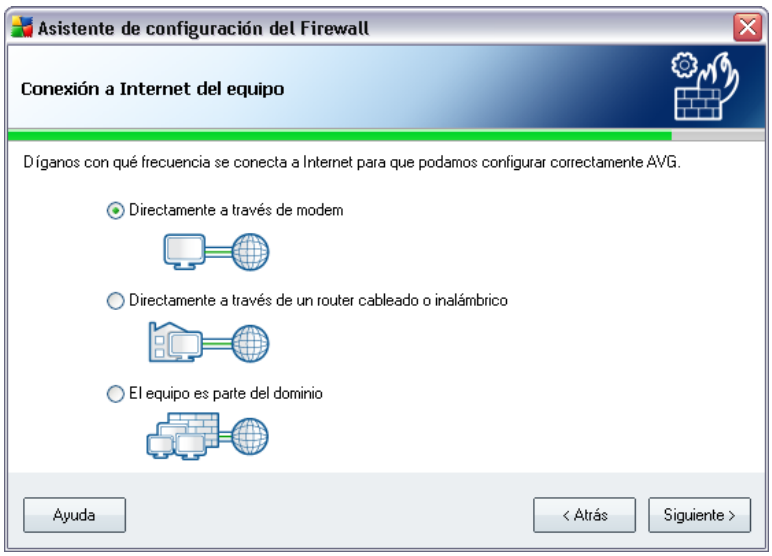
En este cuadro de diálogo, el ***Asistente de configuración del Firewall*** pregunta qué tipo de equipo utiliza. Por ejemplo, un equipo portátil, que se conecta a Internet desde varios lugares diferentes (*aeropuertos, habitaciones de hotel, etc.*) necesita reglas de seguridad más estrictas que las que 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 diálogo.

5.13. Diseño de conexión en red de su equipo



En este 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:

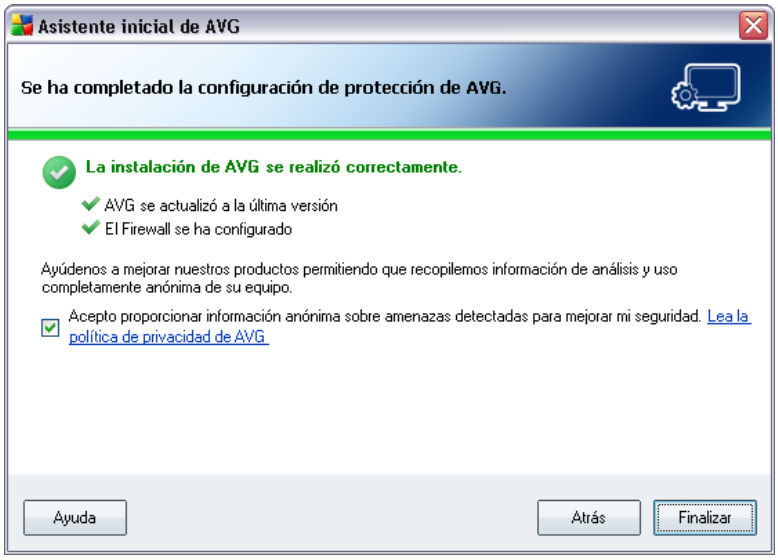
- ***Directamente a Internet***

- ***Red doméstica pequeña***
- ***El equipo está en un 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 diálogo.

5.14. La configuración de la protección AVG ha finalizado



Ahora se ha configurado **Anti-Virus AVG 9 más Firewall**.

En este cuadro de diálogo decide si desea activar la opción de generación de informes 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. 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 de Registro*** (*siguiendo las instrucciones proporcionadas 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.

6.2. 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***

6.3. Análisis de todo el equipo

Existe el riesgo potencial de que un virus informático se haya transmitido a su equipo antes de que usted instalase **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***.

6.4. 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, ***Web Shield*** reaccionará con una advertencia. Esta notificación de ***Web Shield*** demuestra que el programa AVG se ha instalado correctamente en su equipo.

Si AVG no identifica el archivo de análisis EICAR como un virus, deberá verificar otra vez la configuración del programa.

6.5. 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** viene 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 abra 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 **Anti-Virus AVG 9 más Firewall** ventana principal. 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 de 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-Spyware***: abre la página predeterminada del componente ***Anti-Spyware***.
- ***Firewall***: abre la página predeterminada del componente ***Firewall***.

- ***Link Scanner***: abre la página predeterminada del componente ***Link Scanner***.
- ***Analizador de correos electrónicos***: abre la página predeterminada del componente ***Analizador de correos electrónicos***.
- ***Licencia***: abre la página predeterminada del componente ***Licencia***.
- ***Web Shield***: abre la página predeterminada del componente ***Web 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 la protección residente*** : abre un diálogo con una descripción general de las amenazas detectadas por la ***Protección residente***
- ***Detección del analizador de correo electrónico*** : abre un diálogo con una descripción general de los archivos adjuntos de los mensajes detectados como peligrosos por el componente ***Analizador de correos electrónicos***
- ***Hallazgos de Web Shield***: abre un diálogo con una descripción general de las amenazas detectadas por ***Web 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 AVG y ejecuta un análisis del equipo completo

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

- ***Analizar archivo***: permite ejecutar un análisis a pedido 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 diálogo ***Configuración avanzada de AVG*** en el cual es posible editar la **Anti-Virus AVG 9 más Firewall** configuración. 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 diálogo ***Activar AVG*** con la información introducida en el

diálogo ***Personalizar AVG*** del proceso de instalación. Dentro de este diálogo puede introducir el número de licencia para reemplazar el número de venta (*el número con el que instaló AVG*), o reemplazar el número de licencia antiguo (*como al actualizar a un nuevo producto AVG*).

- ***Inscribirse 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 que registren su producto AVG podrán recibir soporte técnico gratuito.

- ***Acerca de AVG***: abre el diálogo ***Información*** con cinco fichas que proporcionan información acerca del nombre del programa, versión del programa y la base de datos de virus, información del sistema, 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. Dentro de esta sección encontrará siempre 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 de contexto 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 brevedad.

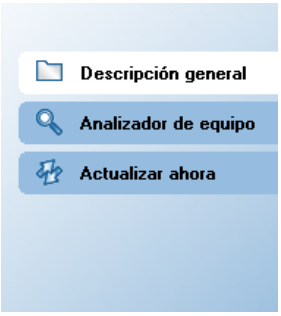
El icono rojo indica que AVG se encuentra en estado crítico Uno o más componentes no funcionan correctamente y AVG no puede proteger su equipo. Preste atención de inmediato para corregir el problema notificado. Si no puede corregir el error sin ayuda, póngase en contacto con el equipo de soporte técnico 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 del 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 (*consulte la Imagen 2*).

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 ***Vista general de componentes*** contiene información sobre los componentes siguientes:

- ***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 explorador de Internet. Detalles >>
- ***Analizador de correos electrónicos*** verifica todo el correo entrante y saliente para ver si contiene virus. Detalles >>
- ***Licencia*** muestra el texto completo del contrato de licencia de AVG. Detalles >>
- ***Web Shield*** analiza todos los datos que descarga un explorador 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 está 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 color gris del 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 8.0.xx, donde 8.0 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

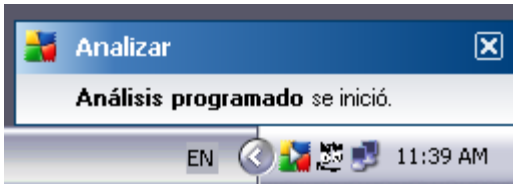
El icono de la bandeja del sistema (*en la barra de tareas de Windows*) indica el estado actual de **Anti-Virus AVG 9 más Firewall**. Está visible en todo momento en la bandeja del sistema, tanto si la ventana principal de AVG está abierta como si está cerrada.

Si aparece de color completo , 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 ***Ignorara el estado del componente***.

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

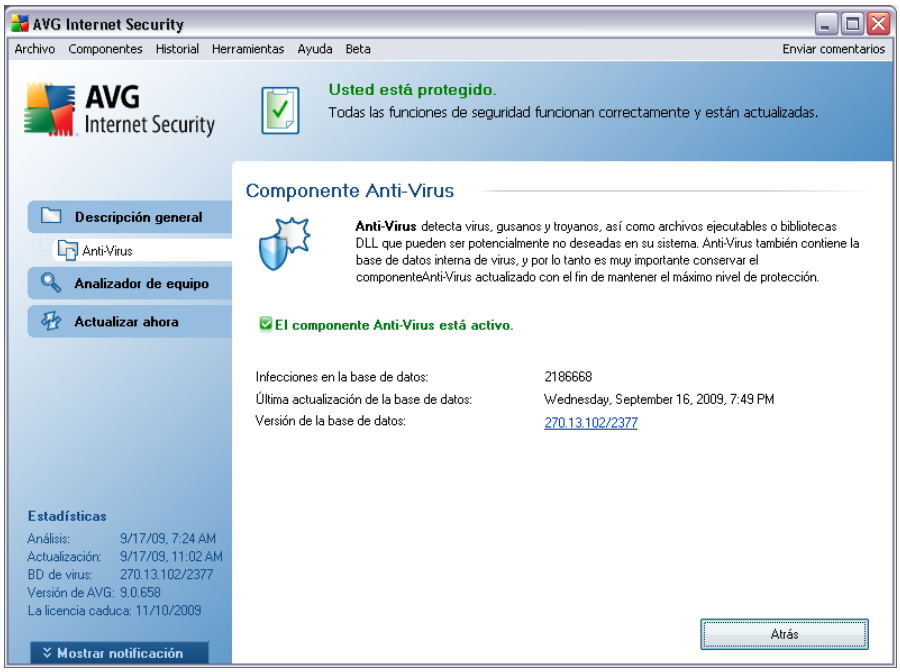
La función esencial de la protección antivirus es que ningún virus conocido pueda ejecutarse en el equipo.

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 diálogo Configuración avanzada de AVG abierto recientemente.*

8.2. Anti-Spyware

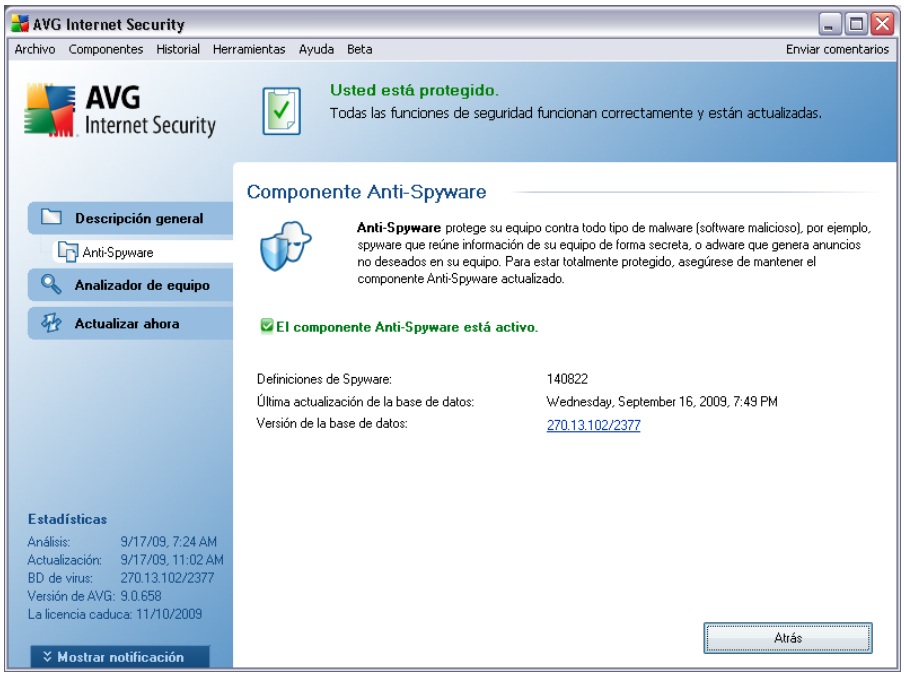
8.2.1. Anti-Spyware Principios de

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 predeterminada del usuario de AVG (descripción general de los componentes).

Observe que: el *proveedor del software ha configurado todos los componentes de AVG para que proporcionen el 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.*

8.3. 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; esto elimina el riesgo de posibles conflictos y cualquier problema relacionado con esto.*

8.3.1. 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.
- Mantener un archivo de todos los perfiles y configuración
- Cambiar el perfil de forma automática al conectarse a diferentes redes, o utilizar diferentes adaptadores de red

8.3.2. 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***:

  - ***Equipo portátil*** : 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.

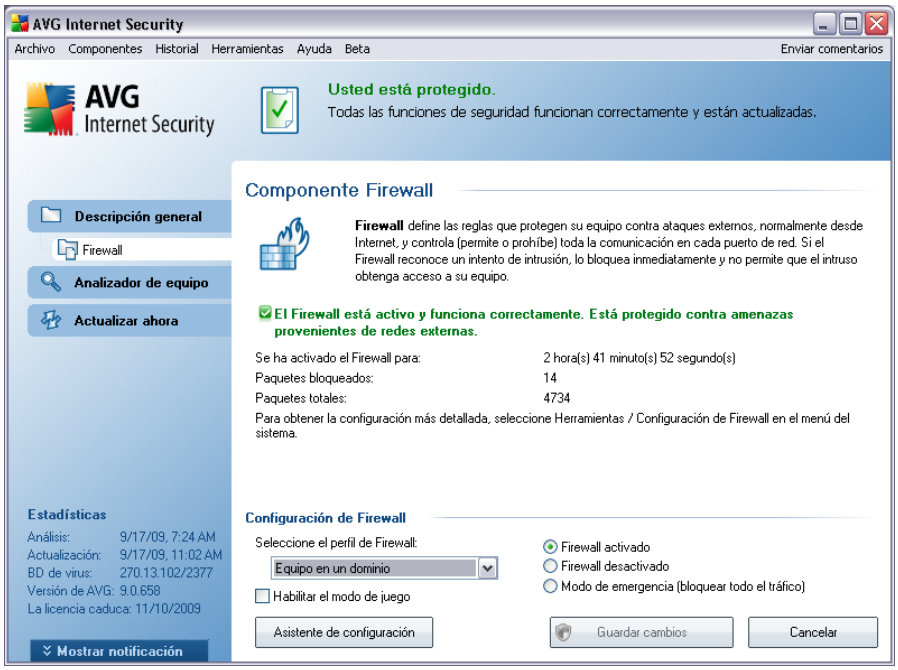
Cambio de perfiles

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 diálogo ***Perfiles de adaptadores y áreas*** , donde también puede deshabilitar 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.

8.3.3. 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 diálogos 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 a 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*** estará en ejecución pero se detendrá 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* ***Archivo/ Configuración del Firewall*** *y edite la configuración del Firewall en el 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*)

8.4. 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 navegan 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.

8.4.1. 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*).

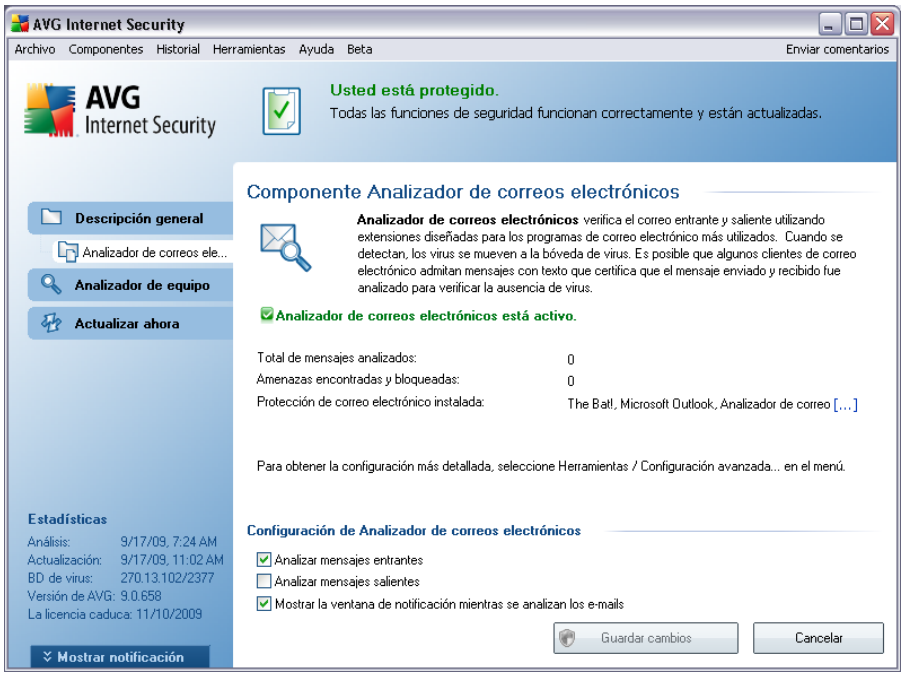
El Analizador de correos electrónicos funciona como una interfaz entre el cliente de correo electrónico y los servidores de correo electrónico en Internet.

- ***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.*

8.4.2. 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* : durante el análisis el componente ***Analizador de correos electrónicos*** muestra un diálogo de notificación que informa de la tarea que está realizando el componente (*conectando al servidor, descargando el mensaje, analizando el mensaje, ...*). Esta opción está activada y no se puede editar.

Se puede acceder a la configuración avanzada del componente ***Analizador de correos electrónicos*** mediante el elemento ***Archivo/Configuración avanzada*** del menú del sistema; no obstante, la configuración avanzada solo 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.*

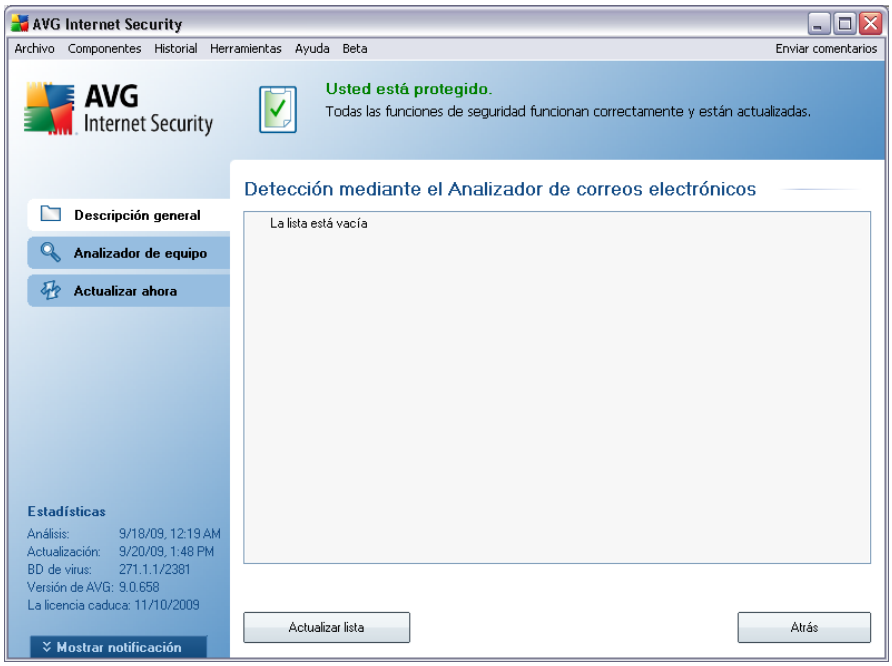
Botones de control

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).

8.4.3. Detección del analizador de correos electrónicos



En el diálogo de ***detección del Analizador de correos electrónicos*** (*accesible mediante la opción de menú del sistema Historial/detección del 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 (probablemente aún 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

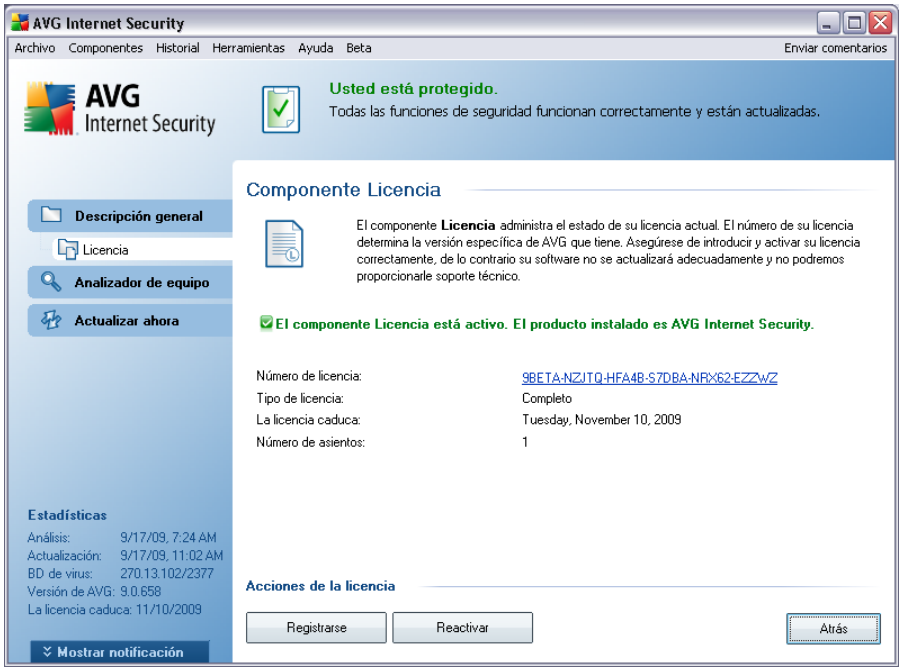
En la parte inferior del diálogo, debajo de la lista, encontrará información sobre el número total de los objetos detectados listados anteriormente. Adicionalmente puede exportar toda la lista de objetos detectados en un archivo (***Exportar lista a archivo***) y eliminar todas las entradas en los objetos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

Botones de control

Los botones de control disponibles en la interfaz de ***Detección mediante el analizador de correos electrónicos*** son:

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

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

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

8.6. Link Scanner

8.6.1. 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 para búsquedas AVG*** y ***Protección de navegación activa AVG***:

- ***Protección para búsquedas AVG*** contiene una lista de sitios web (*direcciones URL*) que se sabe que son peligrosos. Al realizar búsquedas con Google, Yahoo!, MSN o Baidu, todos los resultados se comprueban según esta lista y aparece un icono de veredicto (para los resultados de búsqueda *de 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.

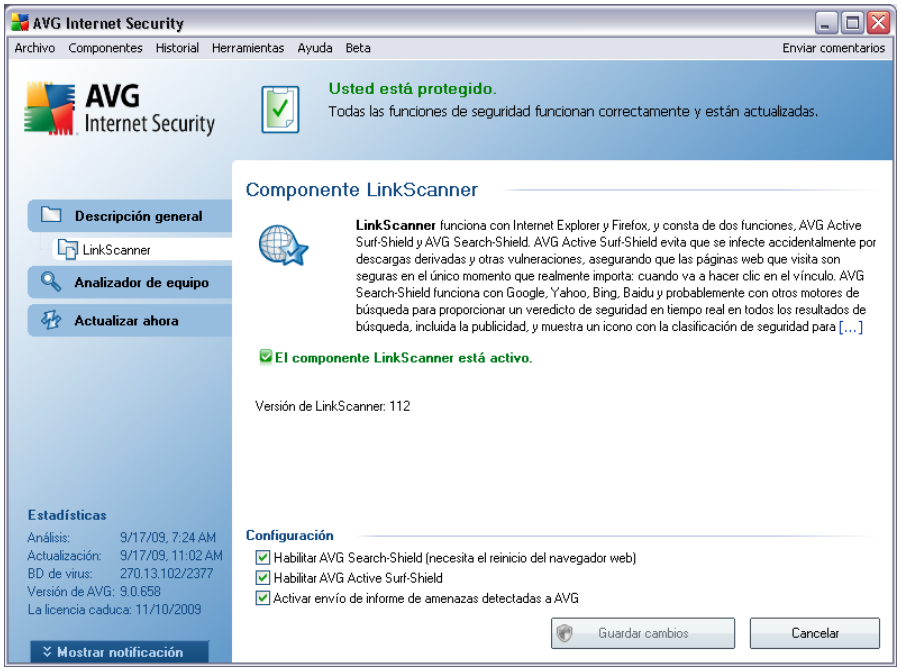
- ***La Protección de navegación activa AVG*** analiza el contenido de los sitios web que visita, independientemente de la dirección del sitio web. Aunque la ***Protección para búsquedas AVG*** no detecte alguno de estos sitios web (*por ejemplo, un sitio web malicioso que se haya creado recientemente 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.*

8.6.2. Interfaz de Link Scanner

El componente ***LinkScanner*** consta de dos partes que se pueden activar/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***: (*activado de manera predeterminada*): iconos asesores de notificación sobre las búsquedas realizadas en Google, Yahoo o MSN que han comprobado por anticipado el contenido de los sitios devueltos por el motor de búsqueda.

- ***Activar la Protección de navegación activa AVG***: *(activado de manera predeterminada*): protección (*en tiempo real*) activa contra sitios de explotación cuando se tiene acceso a ellos. Las conexiones de 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 utiliza HTTP*).

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

8.6.3. Protección de búsqueda AVG

Al realizar búsquedas en Internet con la ***Protección de búsqueda AVG*** activada, todos los resultados de búsqueda que devuelven los motores de búsqueda más populares como Yahoo!, Google, MSN, etc. se evalúan para buscar vínculos peligrosos o sospechosos. Al comprobar estos vínculos y marcar los vínculos malos, la ***barra de herramientas AVG Security*** muestra una advertencia antes de hacer clic en los vínculos peligrosos o sospechosos, así puede estar seguro de que sólo visite 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*).

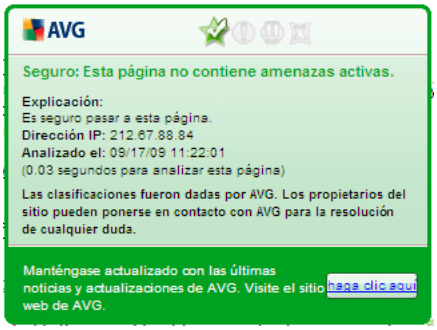
La página vinculada no contiene amenazas pero es algo sospechosa (*origen o motivos cuestionables, por lo tanto no recomendable para realizar compras por Internet, etc.*).

La página vinculada puede ser segura por sí misma pero contener 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.

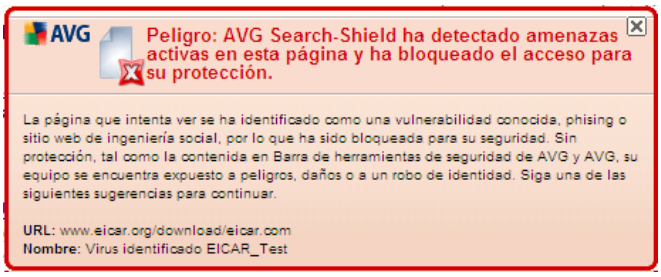
Al desplazarse sobre un icono de calificación se mostrarán detalles acerca del vínculo en cuestión. La información incluye detalles adicionales acerca de la amenaza (si hubiere), la dirección IP del vínculo y la fecha en que la página fue analizada con AVG:



8.6.4. 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 función 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, la ***barra de herramientas AVG Security*** no permitirá que su navegador la muestre.

Si encuentra un sitio web malicioso, la ***barra de herramientas AVG Security*** del navegador web le advertirá con una pantalla similar a:



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

8.7. Web Shield

8.7.1. Principios de Web Shield

Web 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.

Web Shield detecta que la página que se va a visitar contiene 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 Web Shield no está diseñado para plataformas de servidor.*

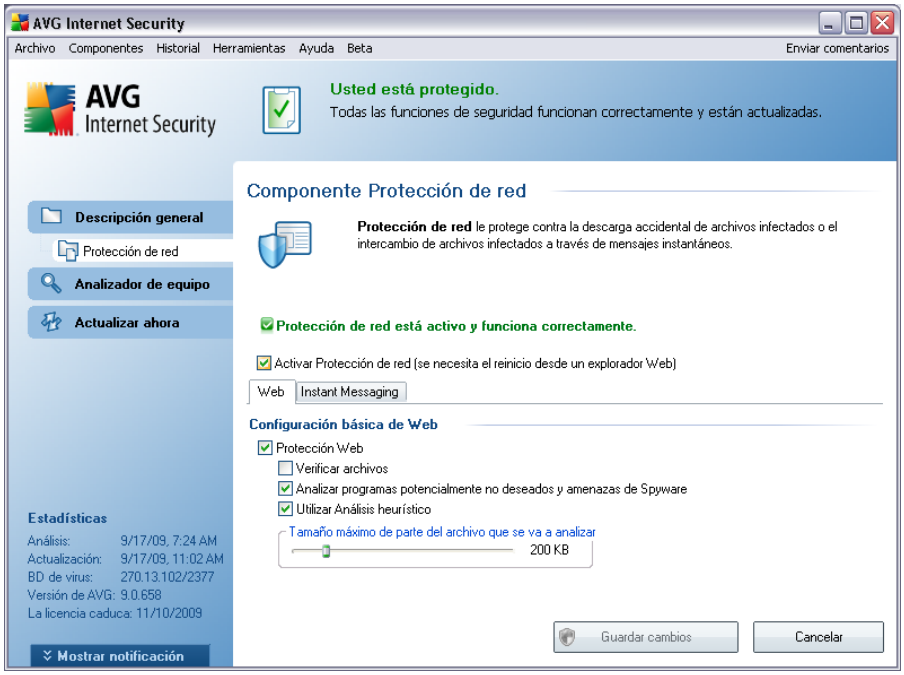
8.7.2. Interfaz de Web Shield

La interfaz del componente ***Web Shield*** describe el comportamiento de este tipo de protección. Adicionalmente puede encontrar información acerca del estado actual del componente (*Web Shield está activa 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 ***Web Shield*** haciendo clic en el elemento ***Activar Web Shield*** . Esta opción está activada de manera predeterminada, y el componente ***Web 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 la ***Web 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:

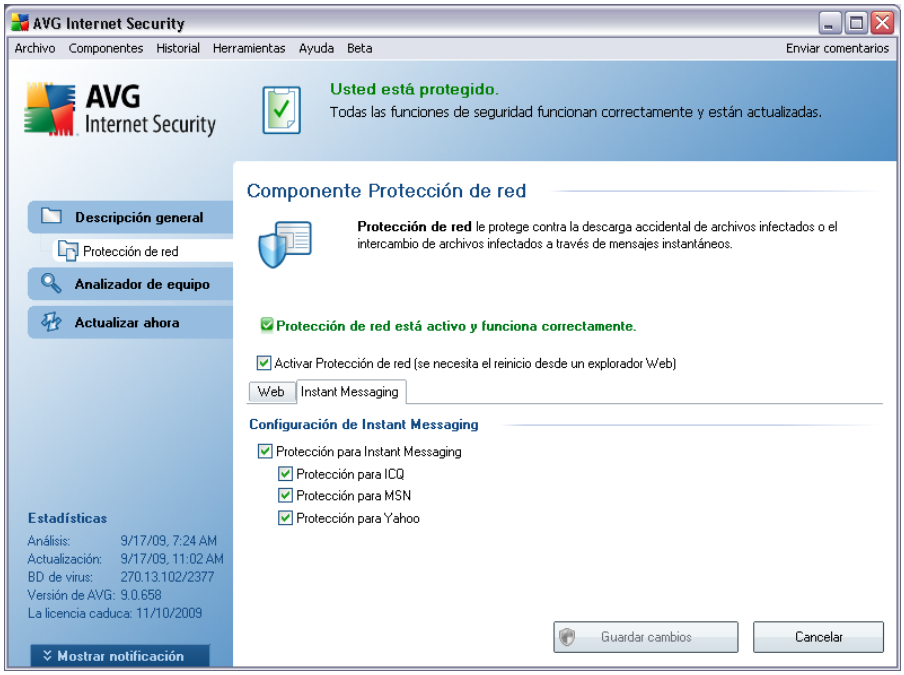


o ***Web Shield***: esta opción confirma que ***Web Shield*** debe analizar el contenido de las páginas www. Mientras esta opción esté seleccionada (*valor predeterminado*), podrá activar o desactivar estos elementos:

- ***Examinar archivos***: analiza el contenido de los archivos que probablemente contenga la página web que se visualizará.
- ***Analizar programas potencialmente no deseados***: analiza los programas potencialmente no deseados (*programas ejecutables que pueden actuar como spyware o adware*) incluidos en la página web que se visualizará.
- ***Utilizar análisis heurístico*** : analiza el contenido de la página que se visualizará utilizando el método del análisis heurístico *(emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual; consulte el capítulo Principios 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 un archivo

que se analizará con ***Web Shield***. Aunque el tamaño del archivo descargado sea superior al valor especificado, y por consiguiente no se analice con ***Web 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 ...*).



o Protección de la mensajería instantánea: seleccione este elemento si desea que la Web Shield compruebe que la comunicación en línea no tenga 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 diálogo Configuración avanzada de AVG abierto recientemente.*

Botones de control

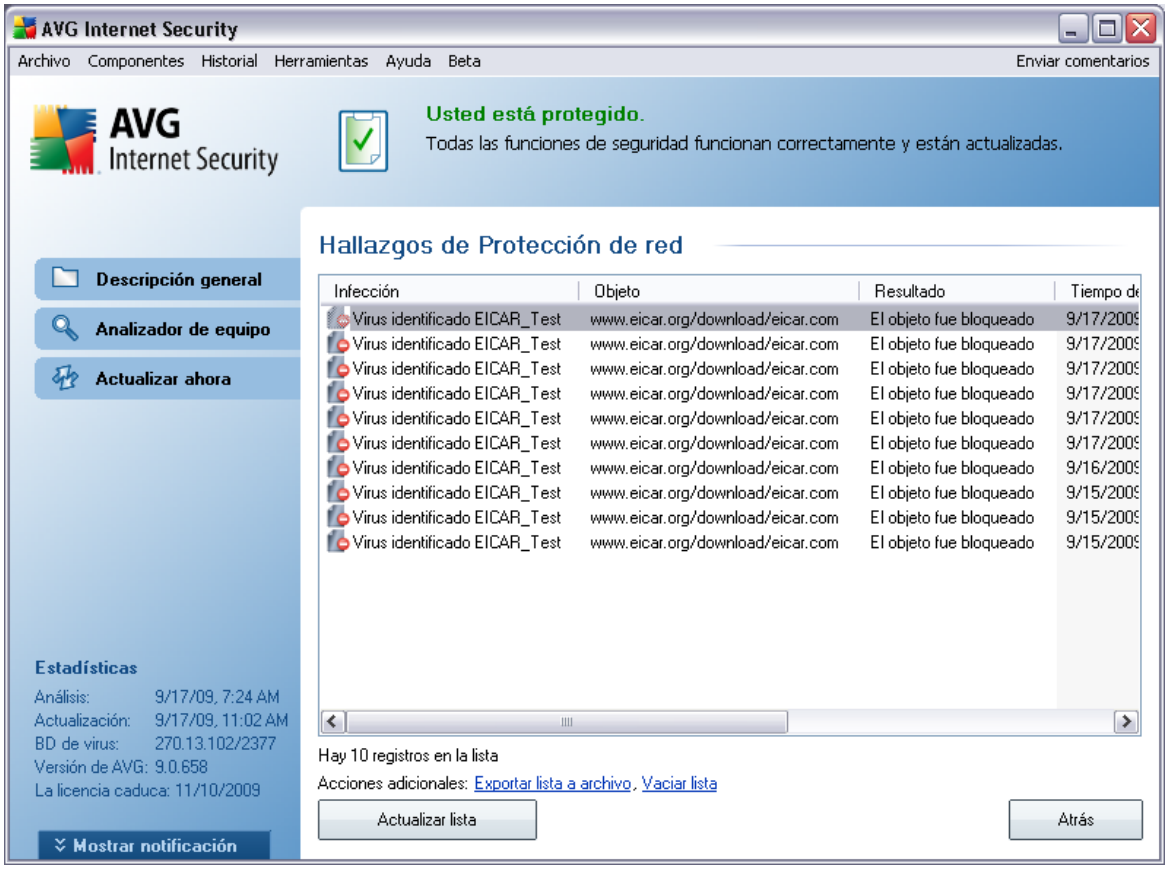
Los botones de control disponibles en la interfaz del ***Web Shield*** son:

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

8.7.3. Detección de Web Shield

Web 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 Web Shield***; esta descripción general de las amenazas detectadas es accesible mediante el menú de sistema ***Historial / Hallazgos de Web 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 ***Web Shield***. El botón ***Atrás*** lo regresará a la ***Interfaz del usuario de AVG*** predeterminada (descripción general de los componentes).

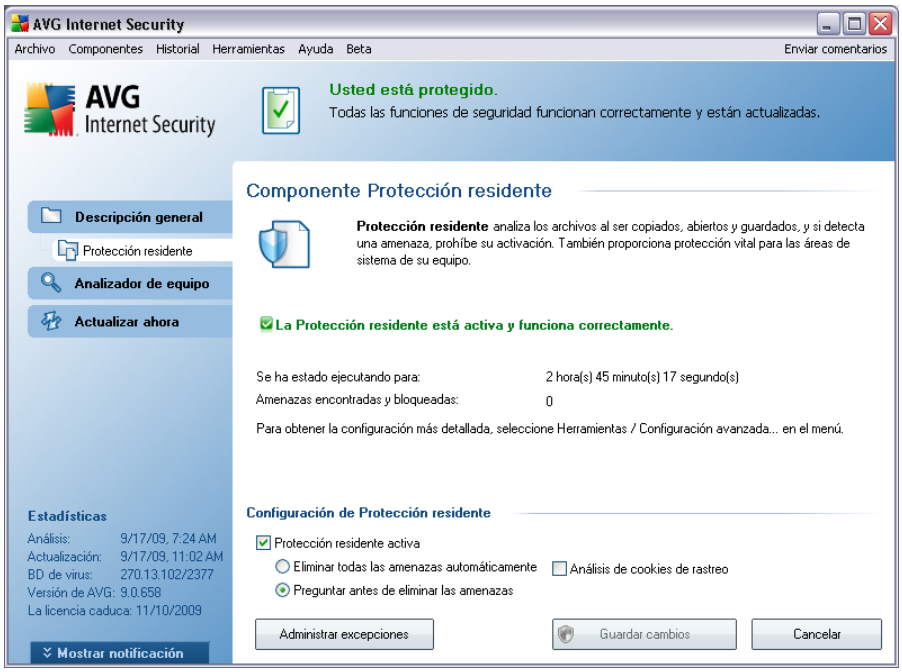
8.8. Protección residente

8.8.1. 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.

8.8.2. 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 de las que se evitó que se ejecutaran/abrieran (*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 del Archivo/Elemento de 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, aún puede seleccionar si desea ***Eliminar las cookies automáticamente.*** 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 diálogo*[*Configuración avanzada de AVG*](#) *abierto recientemente.*

Botones de control

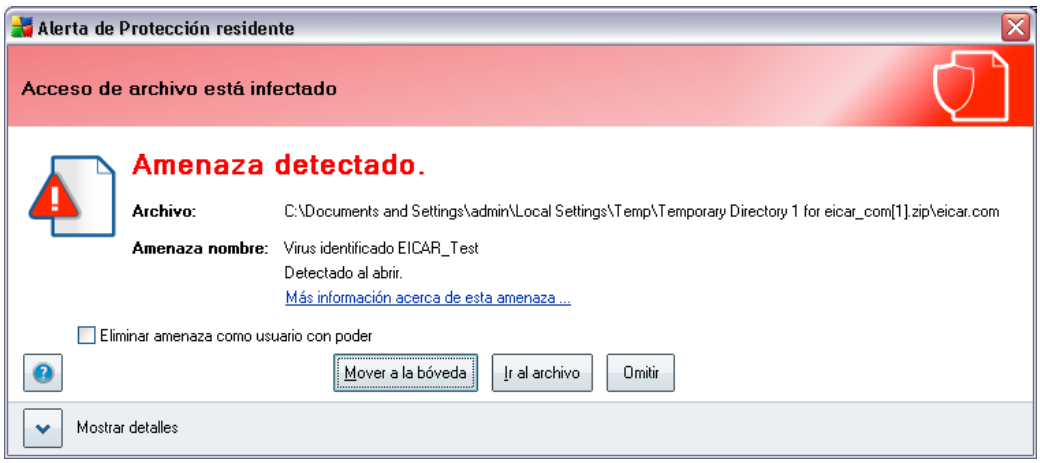
Los botones de control disponibles dentro de la interfaz de la ***Protección residente*** son:

- ***Administrar excepciones*** : abre el diálogo ***Protección residente: Exclusiones de directorio***, donde puede definir carpetas que deberían 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).

8.8.3. Detección de protección residente

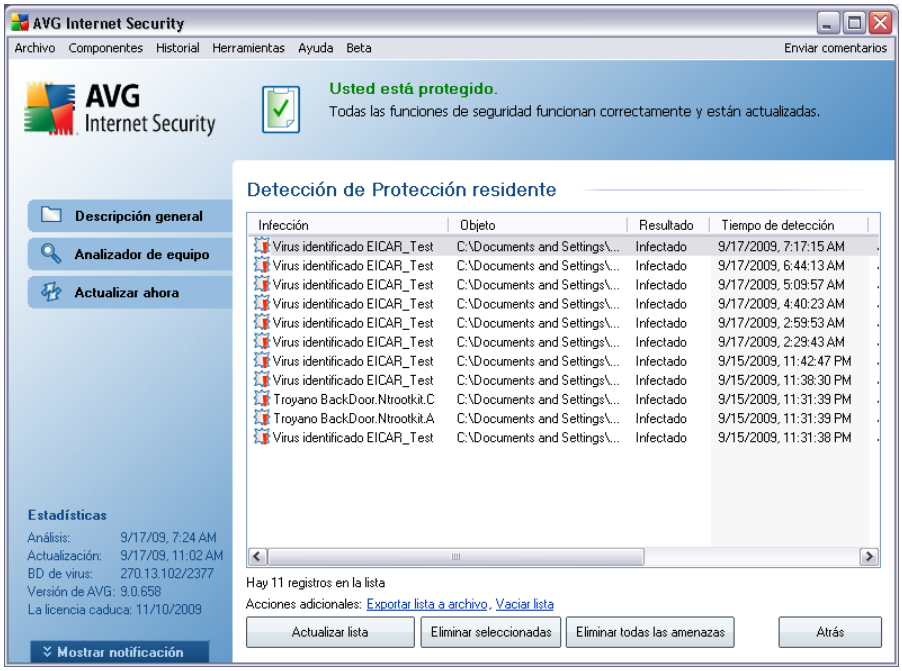
La Protección residente analiza los archivos mientras éstos se copian, se abren o se guardan. Cuando se detecta una amenaza de virus o de cualquier tipo, se le advertirá inmediatamente mediante este diálogo:



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 ampliamente 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 (probablemente aún 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).

8.9. 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.*

El administrador de descargas de AVG es una herramienta sencilla que permite administrar fácilmente descargas de productos de AVG. En función de las selecciones realizadas, el administrador de descargas se configurará con el producto, tipo de licencia e idioma específicos. La gran ventaja de esta utilidad es ayudarle a administrar la descarga de productos de AVG en sus términos. Además, siempre se descarga el archivo de instalación más reciente, de modo que el programa de AVG esté completamente actualizado tras la instalación.

Administrador de descargas de AVG

- Siempre descarga el archivo de instalación más reciente;
- Reduce el tamaño del archivo descargado;
- Es posible continuar con la descarga si ésta se interrumpe por algún motivo;
- Funciona con todas las ediciones del programa AVG para uso doméstico

Nota: *Tenga en cuenta que el Administrador de descargas de AVG no es adecuado para las ediciones de descarga de red y SBS, y que sólo es compatible con los siguientes sistemas operativos: Windows 2000 (SP4 + SRP roll-up), Windows XP (SP2*

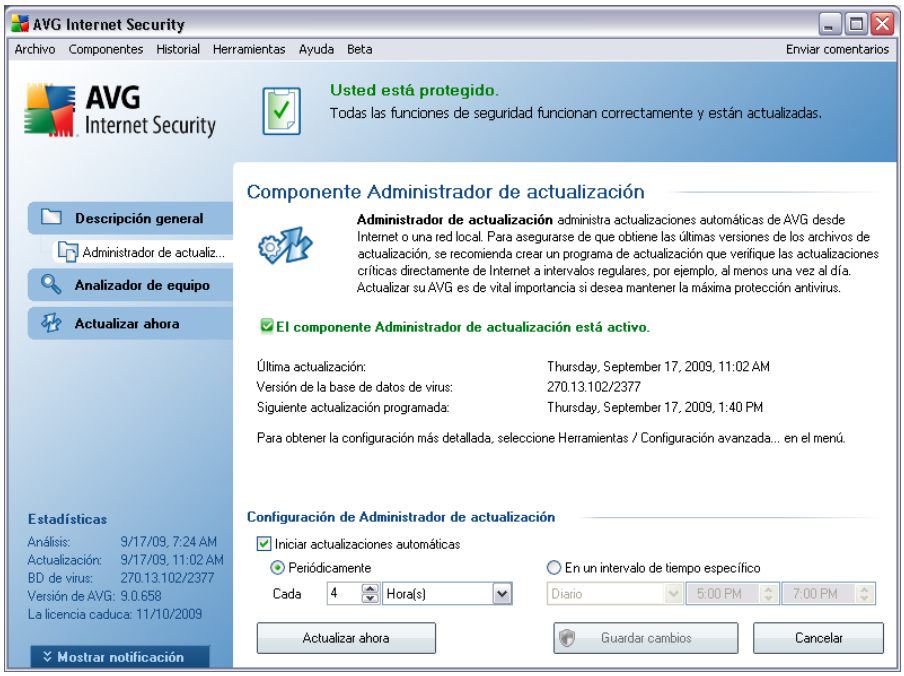
y más recientes), Windows Vista (todas las ediciones).

8.9.1. Principios de administrador de actualización

El administrador de descargas de AVGfunciona en los siguientes pasos:

- Primero, es necesario descargar la aplicación del ***Administrador de descargas de AVG*** . Al iniciarse, el ***Administrador de descargas de AVG*** le pide que seleccione el idioma para el proceso de instalación.
- A continuación, el ***Administrador de descargas de AVG*** intentará establecer una conexión a Internet para realizar la prueba de conectividad. Si la prueba de conectividad se realiza correctamente, podrá seleccionar qué versión del programa AVG desea instalar (*versión completa, de prueba o edición gratuita*).
- Una vez seleccionada la versión del programa AVG, se le pedirá que elija el producto que desea instalar.
- Finalmente, se descargarán todos los archivos de instalación requeridos. El ***Administrador de descargas de AVG*** se cierra y empieza la instalación de AVG.

8.9.2. 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 diálogo Configuración 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).

8.10. Barra de herramientas AVG Security

La Barra de herramientas AVG Security es una nueva herramienta que funciona con el componente ***Link Scanner*** y que comprueba los resultados de búsqueda de los motores de búsqueda de Internet compatibles (*Yahoo!, Google, MSN, Baidu*).

Si elige instalar la barra de herramientas durante la instalación de **Anti-Virus AVG 9**

más Firewall, se agregará automáticamente en el navegador Web.

La Barra de herramientas AVG Security puede utilizarse para controlar las funciones de ***Link Scanner*** y ajustar su comportamiento, así como para actualizar **Anti-Virus AVG 9 más Firewall**en caso de que existan nuevas actualizaciones disponibles.

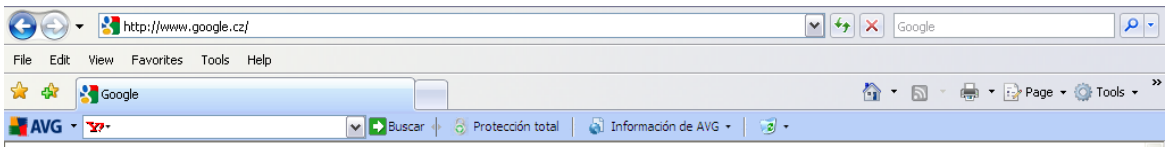
Nota: *Si está utilizando algún navegador de Internet alterno (por ejemplo, Avant Browser) puede producirse un comportamiento inesperado.*

8.10.1. 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 1.5 o posterior*).

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

Una vez que haya decido instalar la ***Barra de herramientas AVG Security*** (*durante el proceso de instalación de AVG, se le pedirá que decida si desea instalar el componente*), el componente se ubicará en el navegador Web, justo debajo de la barra de direcciones:



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

- ***Botón del logo 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***, con información detallada acerca de la protección que le ofrece la barra de herramientas.
    - ***Iniciar·AVG 9.0***: abre lainterfaz del usuario de AVG
    - ***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 de 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, ponerse en contacto con el ***soporte técnico de AVG*** o ver los detalles de la versión actual de la barra de herramientas

- ***Cuadro de búsqueda de Yahoo!***: una forma sencilla y segura de buscar en Internet con la búsqueda de Yahoo!. Introduzca una palabra o una frase en el cuadro de búsqueda y presione***Buscar*** para iniciar la búsqueda en el servidor de Yahoo! directamente, independientemente de la página que se muestra 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.

- ***Botón Protección de navegación activa AVG***: el botón de encendido/ apagado controla el estado de la ***protección de navegación activa AVG***

- ***Botón Protección de búsqueda AVG***: el botón de encendido/apagado controla el estado de la ***protección de búsqueda AVG***

- ***El botón AVG Info***: proporciona vínculos a información de seguridad importante ubicada en el sitio web de AVG (http://www.avg.com/).

8.10.2. Opciones de la Barra de herramientas AVG Security

Toda la configuración de los parámetros de la ***Barra de herramientas de AVG Security*** se encuentra directamente accesible dentro del 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 tres secciones:

- ***General***

En la pestaña, puede especificar el botón que se debe visualizar/ocultar en el panel de la ***Barra de herramientas AVG Security***:

- ***Botón Noticias de AVG***: esta opción muestra el botón ***Noticias de AVG***. Al presionar el botón en el panel de la ***Barra de herramientas AVG Security*** puede abrir un menú desplegable con vínculos a los comunicados de prensa relacionados con la última versión de AVG.

- ***Botón AVG Info*** : el ***botón AVG Info*** abre el menú con las siguientes opciones:

  - *Información de la barra de herramientas*: abre la página del producto ***Barra de herramientas AVG Security*** con información detallada acerca del componente

  - *Acerca de las amenazas*: abre la página web del laboratorio de virus de AVG con información acerca de las amenazas actuales, recomendaciones para la eliminación de virus, lista de preguntas frecuentes, etc.

  - *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

o ***Botón Borrar historial***: este botón le permite *Eliminar historial completo,* o *Eliminar el historial de búsqueda, Eliminar el historial del navegador, Eliminar historial de descargas,* o *Eliminar cookies* directamente desde el panel de la ***Barra de herramientas AVG Security***.

- ***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 de AVG Security*** que desee utilizar:

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

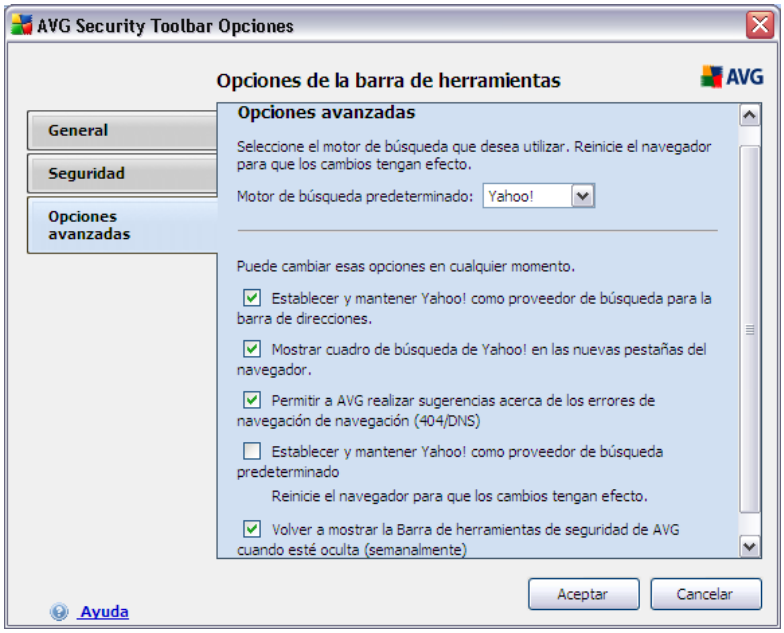
o ***Clasificaciones***: seleccione los símbolos gráficos utilizados para las

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
- la página contiene amenazas activas
- 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.***

- ***Opciones avanzadas***



En la pestaña ***Opciones avanzadas*** , puede activar o desactivar configuraciones específicas adicionales de la***Barra de herramientas AVG Security***:

- ***Establecer y mantener Yahoo! como proveedor de búsqueda para la barra de direcciones*** : (*activada de forma predeterminada*): si se selecciona, esta opción le permite introducir una palabra clave de búsqueda directamente en la barra de direcciones en el navegador de Internet, y el servicio de Yahoo! se utilizará automáticamente para buscar los sitios web de interés.

- ***Mostrar cuadro de búsqueda de Yahoo! en las nuevas pestañas del navegador*** : (*activada de forma predeterminada*): si se selecciona, esta opción muestra el cuadro de búsqueda de Yahoo! en cada nueva pestaña del navegador de Internet que se abre.

- ***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*), la ***Barra de herramientas AVG Security*** automáticamente ofrece una descripción general de 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 dentro de la ***Barra de herramientas AVG Security***, y al activar esta opción se puede convertir también en el motor de búsqueda predeterminado del navegador Web.

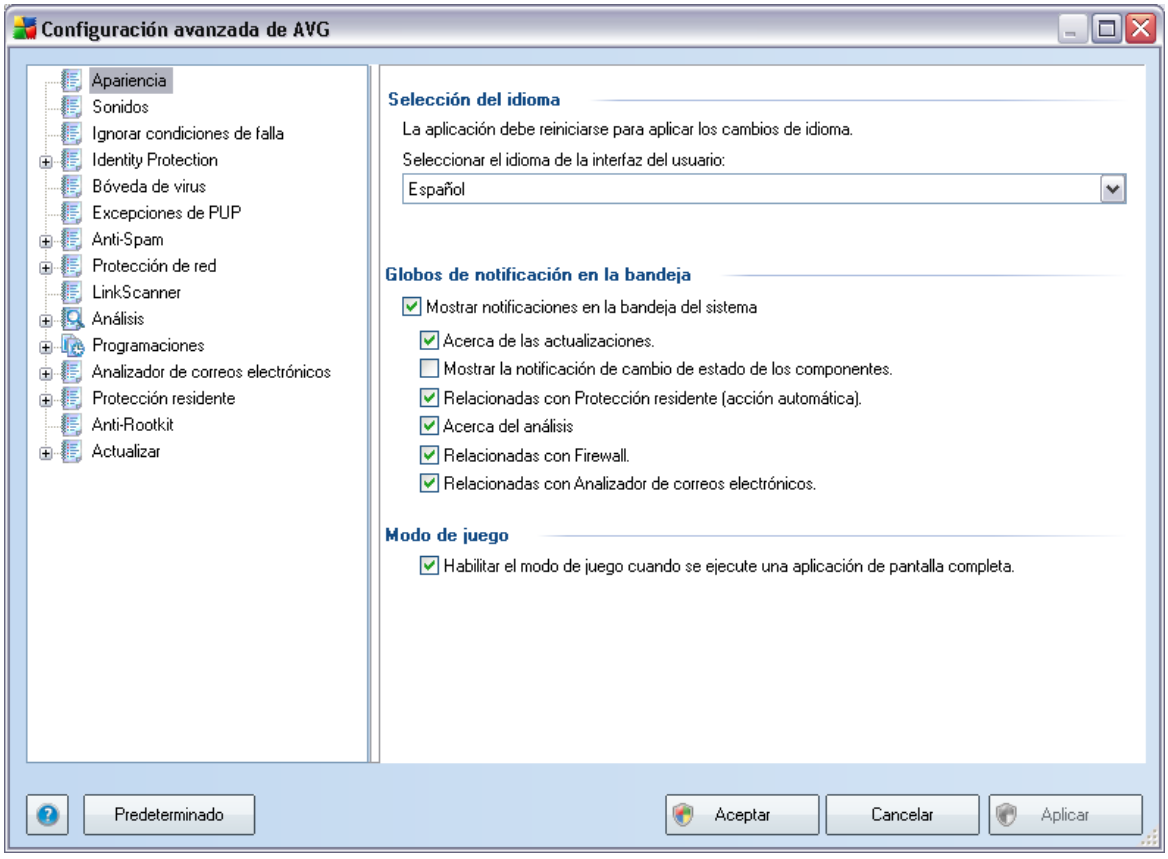
- ***Volver a mostrar la barra de herramientas AVG Security cuando esté oculta (semanalmente)***: (*activada de forma predeterminada*): esta opción está seleccionada de manera predeterminada, así que cuando la ***Barra de herramientas AVG Security*** se oculta accidentalmente, se volverá a mostrar nuevamente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

9. Configuración avanzada de AVG

El diálogo de configuración avanzada de **Anti-Virus AVG 9 más Firewall** se abre en una nueva ventana llamada ***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.

9.1. Apariencia

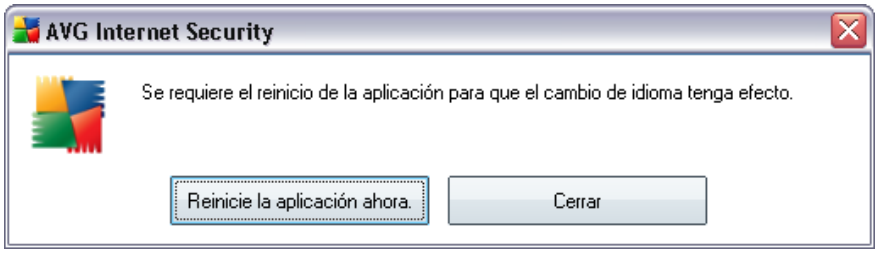
El primer elemento del árbol de navegación, ***Apariencia***, hace referencia a la configuración general de la Interfaz del usuario de AVG y a unas cuantas opciones básicas del comportamiento de la aplicación:



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
- La nueva ventana 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/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 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 archivos;

- ***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.

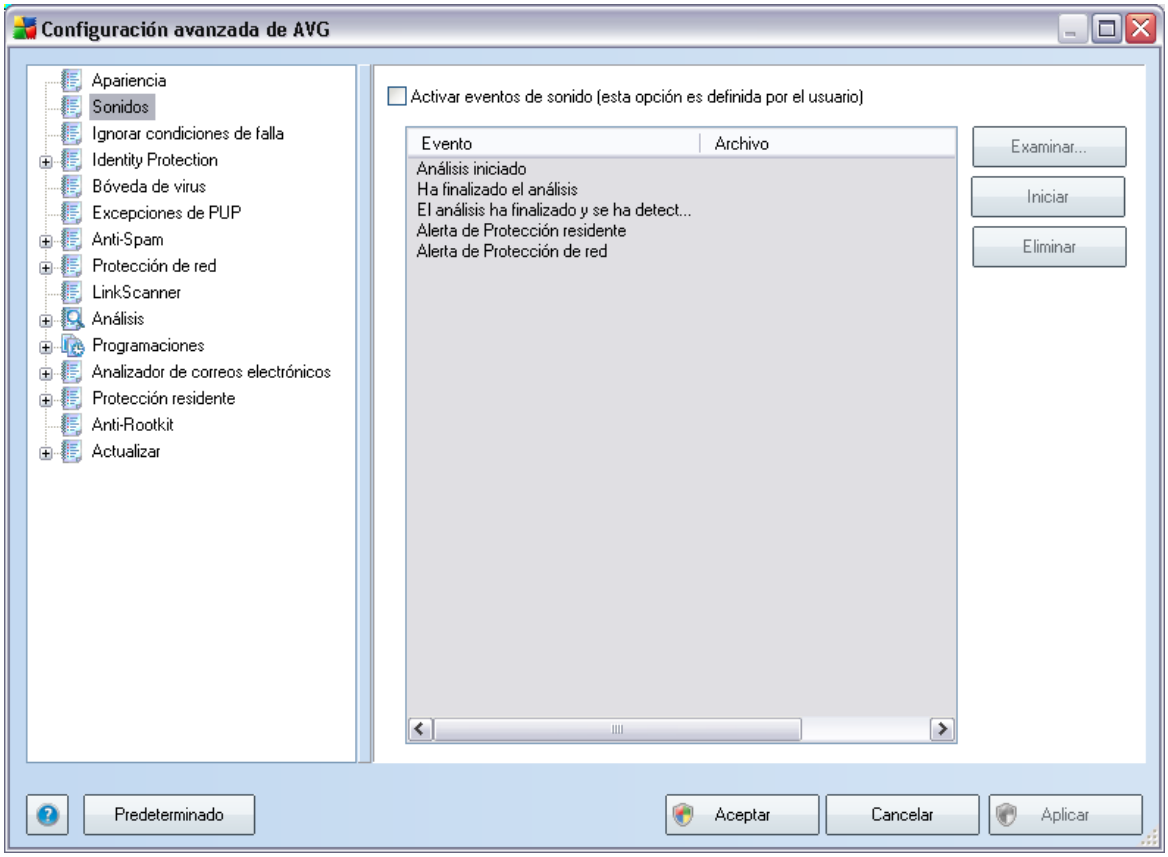
- ***Mostrar las notificaciones de la bandeja relacionadas con el Analizador de correos electrónicos*** : decida si debe visualizarse información sobre análisis de todos los mensajes de correo electrónico entrantes y salientes.

Modo de juego

Esta función de AVG está diseñada para aplicaciones de pantalla completa que necesitan comunicarse mediante Internet y posibles cuadros de diálogos de pregunta de AVG que afectarían la aplicación (*minimizándola o dañando sus 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*).

9.2. 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:

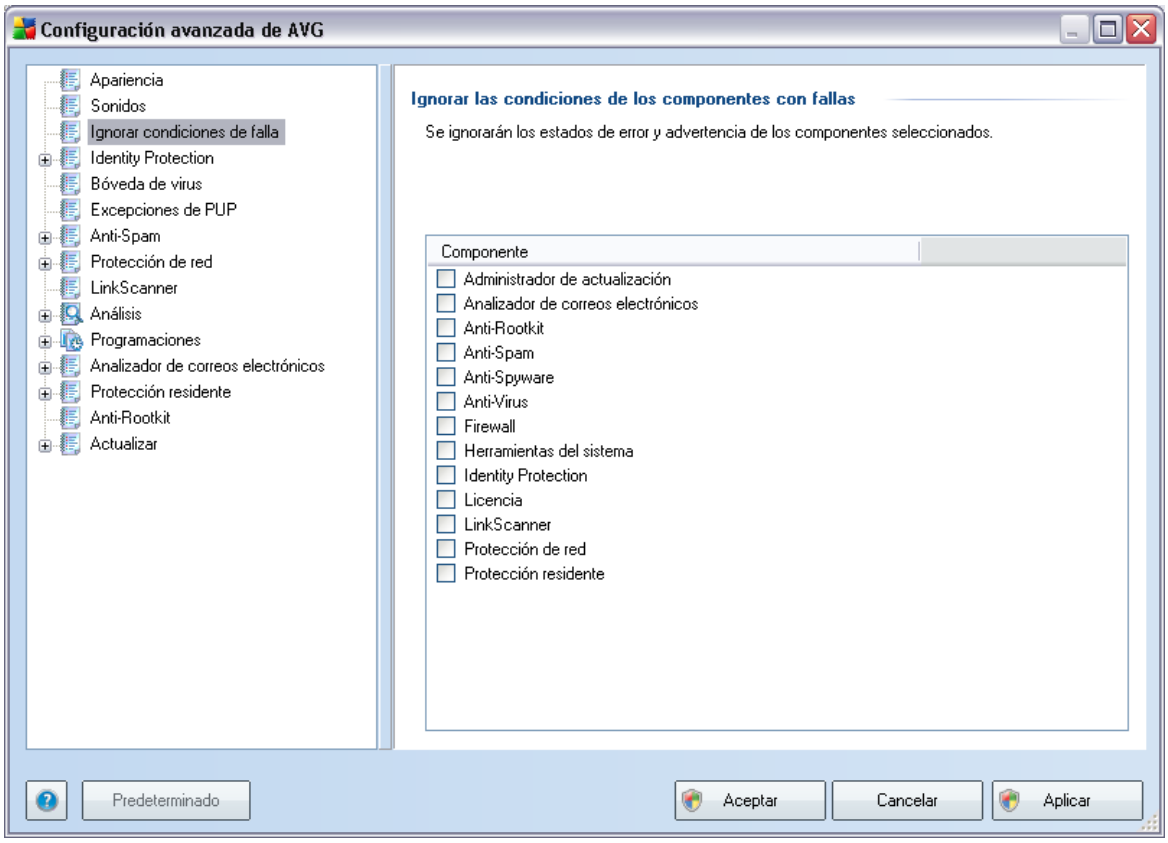


A continuación, seleccione el evento correspondiente de la lista y busque (***Examinar***) en el disco el sonido adecuado que desea asignar a este evento. Para escuchar el sonido seleccionado, resalte el evento en la lista y presione el botón ***Reproducir*** . Utilice el botón ***Eliminar*** para eliminar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

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

9.3. 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:

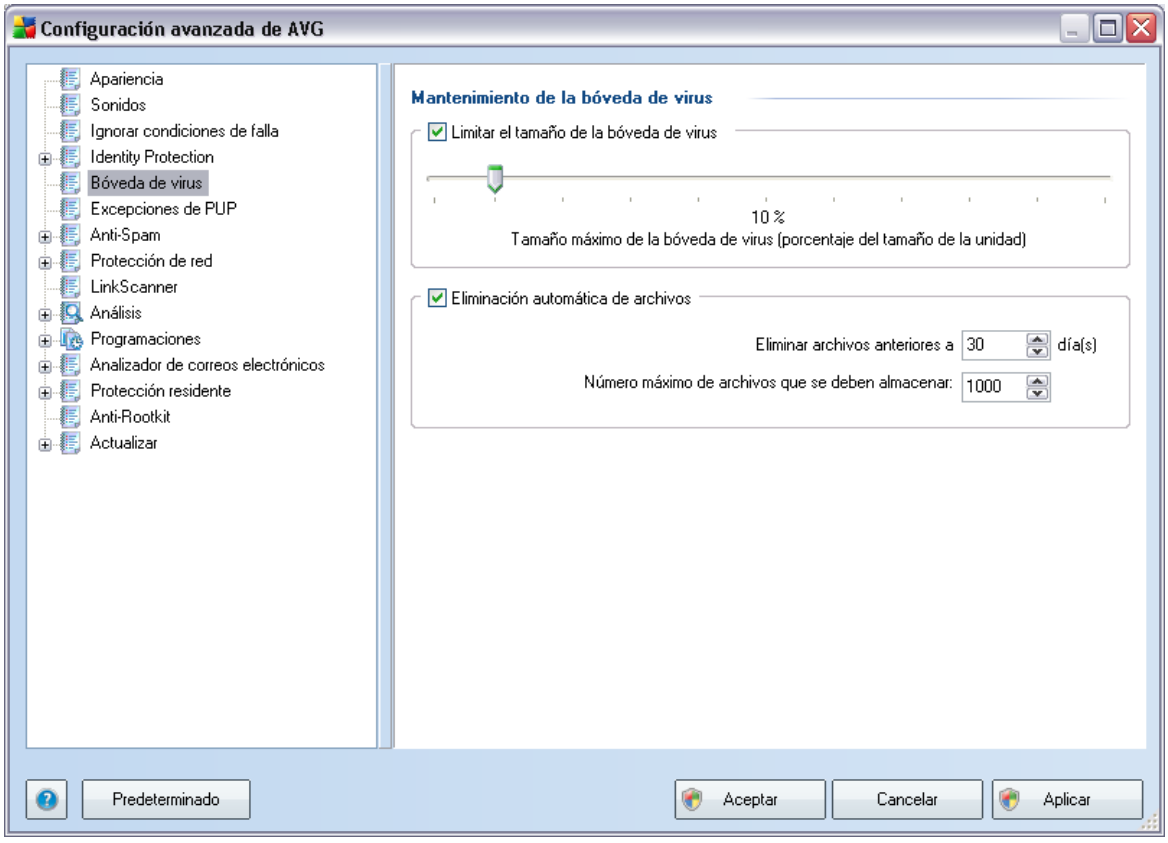
- ***el icono en la bandeja de sistema***: mientras todas las partes de AVG funcionen correctamente, el icono se muestra en cuatro colores; sin embargo, si ocurre un error, el icono aparece con un signo de admiración amarillo
- la descripción de texto del problema existente en la sección ***Información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

9.4. Bóveda de Virus



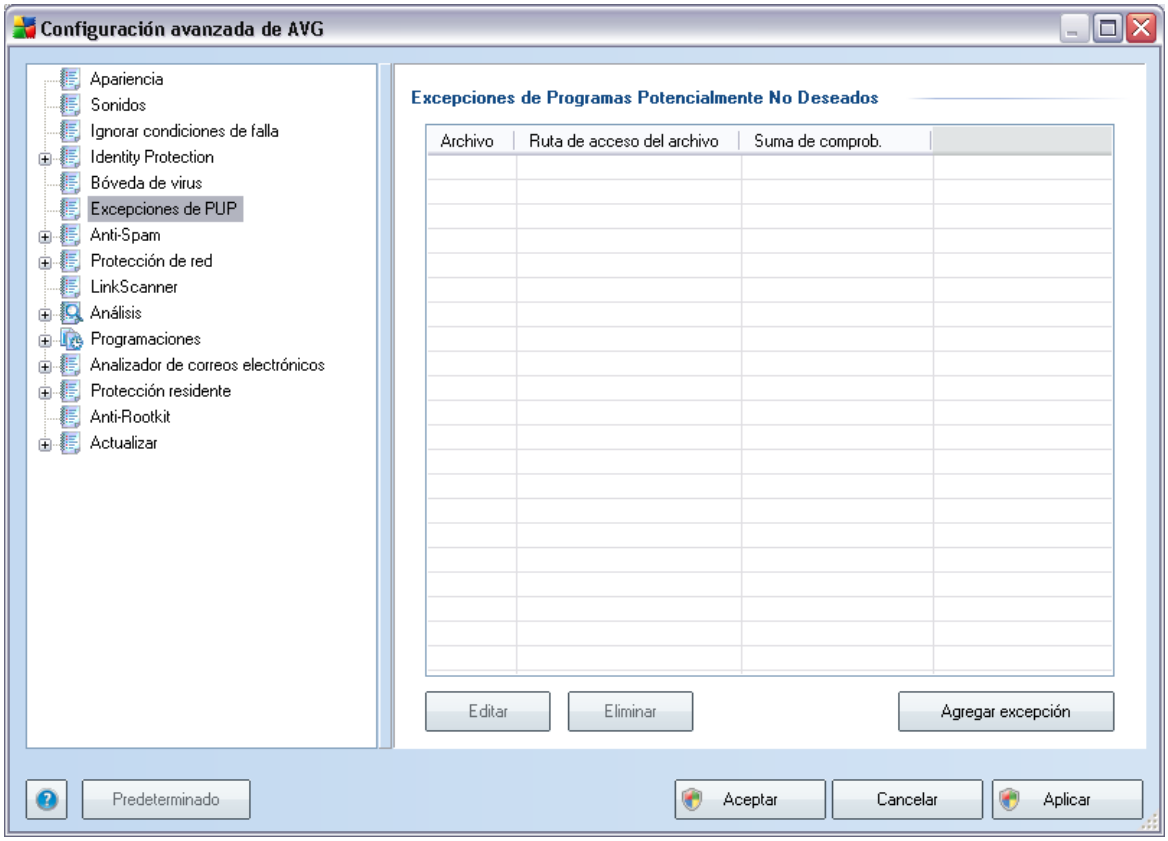
El diálogo ***Mantenimiento de la Bóveda de Virus*** permite definir varios parámetros relacionados con la administración de objetos almacenados en la ***Bóveda de Virus***:

- ***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***).

9.5. Excepciones de PPND

Anti-Virus AVG 9 más Firewall puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas dentro del 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.

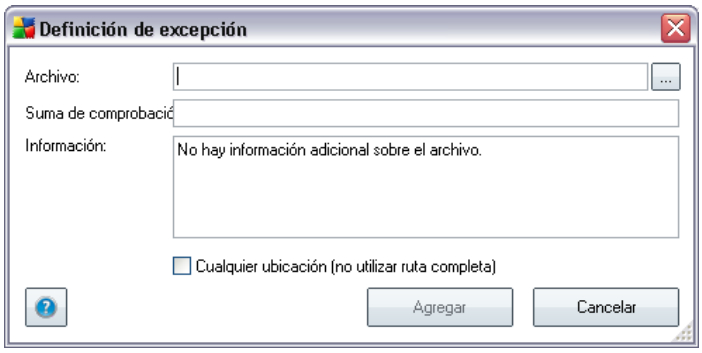
- ***Archivo***: proporciona el nombre de la aplicación en cuestión
- ***Ruta del archivo***: muestra la ruta hacia la ubicación de la aplicación
- ***Suma de comprobación***: muestra la 'firma' única del archivo elegido. Esta suma de verificación es una cadena de caracteres generados automáticamente 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 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 diálogo de edición en el cual es posible definir parámetros para una excepción que se creará:



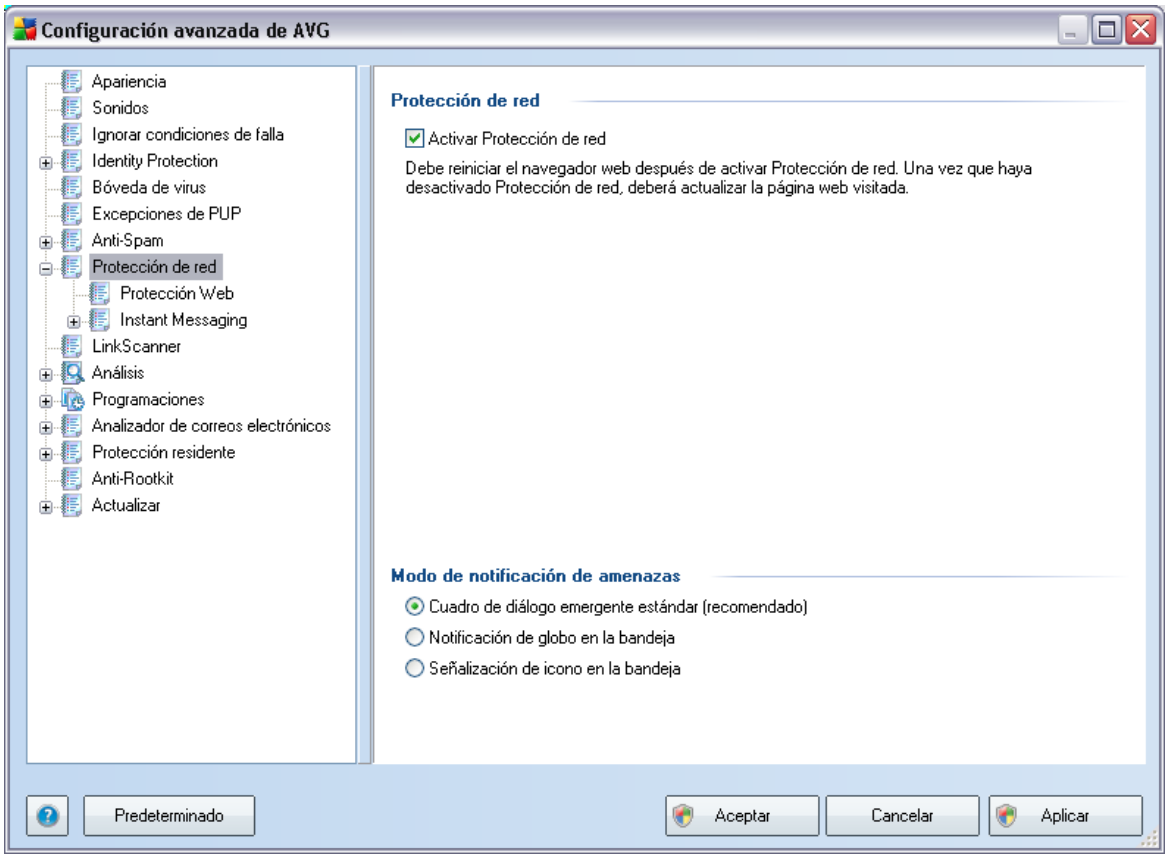
  - ***Archivo***: introduzca la ruta completa del archivo que desea marcar como una excepción

  - ***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

9.6. Web Shield



El cuadro de diálogo ***Protección Web*** le permite activar o desactivar el componente ***Web Shield*** mediante la opción ***Activar Web 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:

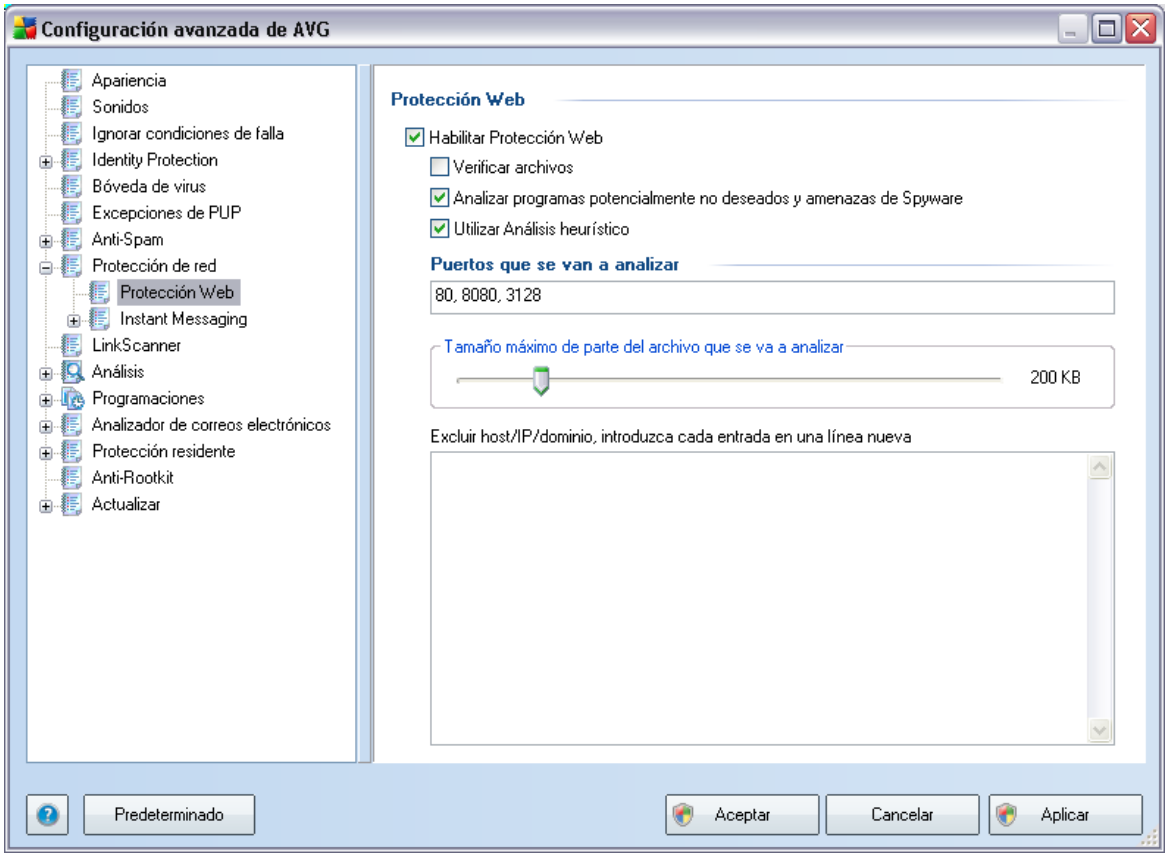
- ***Protección Web***
- ***Mensajería instantánea***

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.

9.6.1. 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 ***Web Shield*** debe analizar el contenido de las páginas www. Mientras esta opción esté seleccionada (*valor predeterminado*), podrá activar o desactivar estos elementos:
    - ***Examinar archivos***: analiza el contenido de los archivos que contenga la página web que se visualizará. .

- ***Analizar programas potencialmente no deseados y amenazas de Spyware***: analiza los programas potencialmente no deseados (*programas ejecutables que pueden actuar como spyware o adware*) incluidos en la página web que se visualizará, junto con las infecciones de spyware.

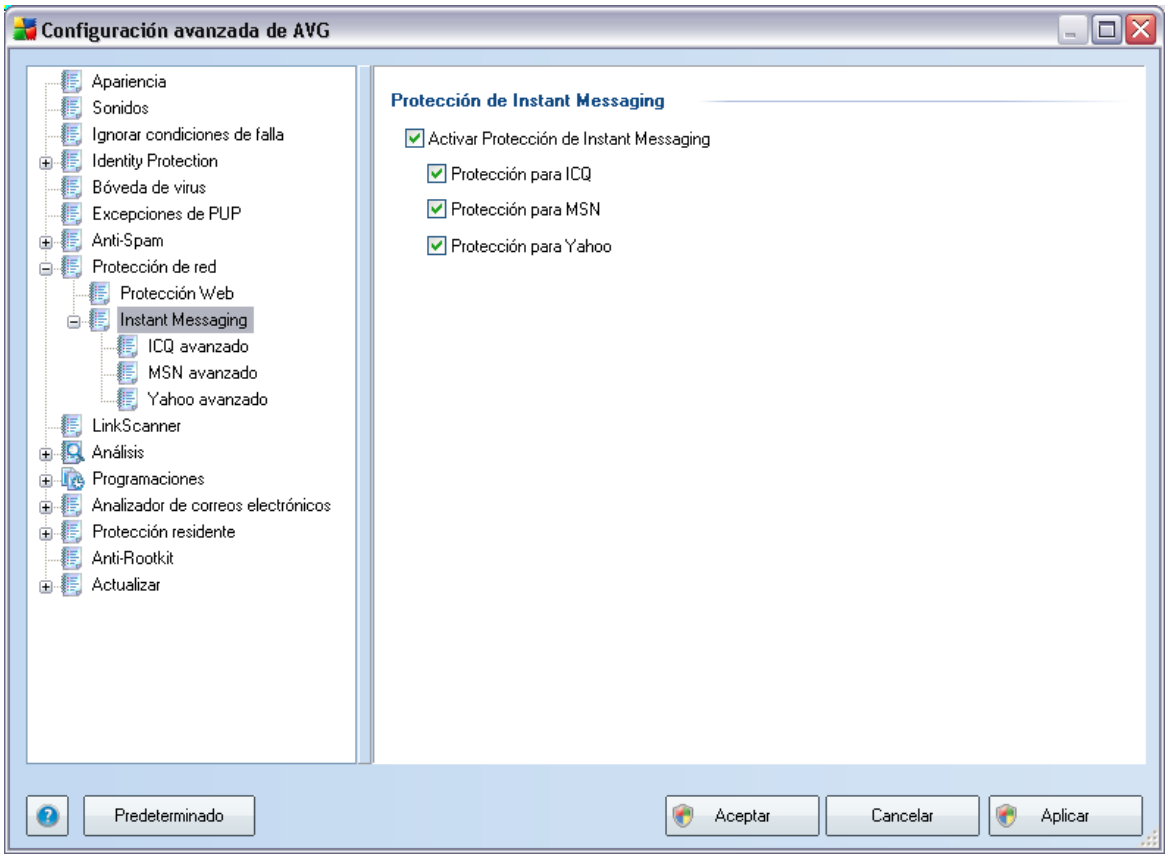
- ***Utilizar análisis heurístico***: analiza el contenido de la página que se visualizará utilizando el método del análisis heurístico (*emulación dinámica de las instrucciones del objeto analizado en un entorno informático virtual*).

- ***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 un archivo que se analizará con ***Web Shield***. Aunque el tamaño del archivo descargado sea superior al valor especificado, y por consiguiente no se analice con Web 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 de un dominio que ***Web 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.

9.6.2. Mensajería instantánea

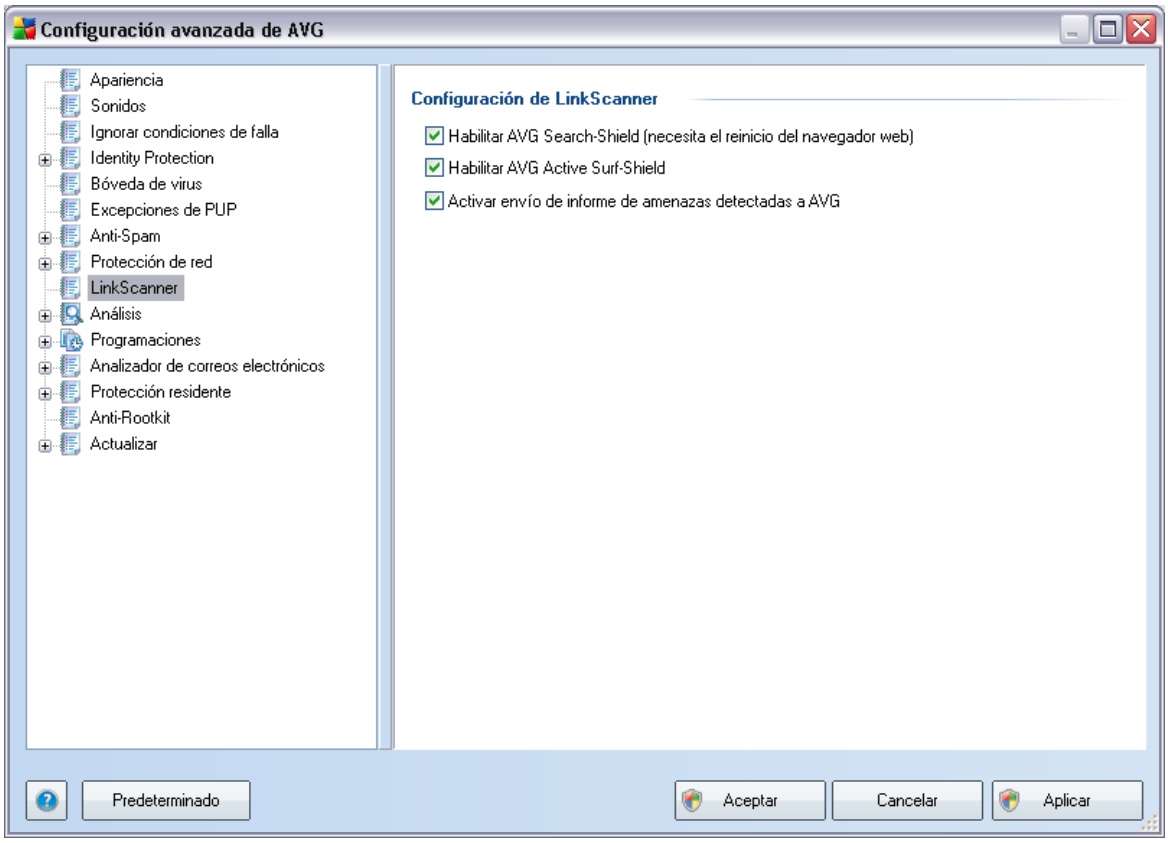


En el diálogo ***Protección de mensajería instantánea*** puede editar la configuración del componente ***Web Shield*** relativa al análisis de la mensajería instantánea. Actualmente sólo se admiten tres programas de mensajería instantánea: ***ICQ*** , ***MSN*** y ***Yahoo***: marque el elemento correspondiente a cada uno de ellos si desea que ***Web Shield*** verifique la comunicación en línea sin 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, 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 negra*** (*usuarios que se bloquearán*).

9.7. Link Scanner

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



- ***Activar la Protección para búsquedas AVG***: (*activada de manera predeterminada*): iconos asesores de notificación sobre las búsquedas realizadas en Google, Yahoo. MSN o Baidu que comprueban por adelantado el contenido de los sitios devueltos por el motor de búsqueda.

- ***Activar la Protección de navegación activa AVG***: *(activado 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 utiliza HTTP*).

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

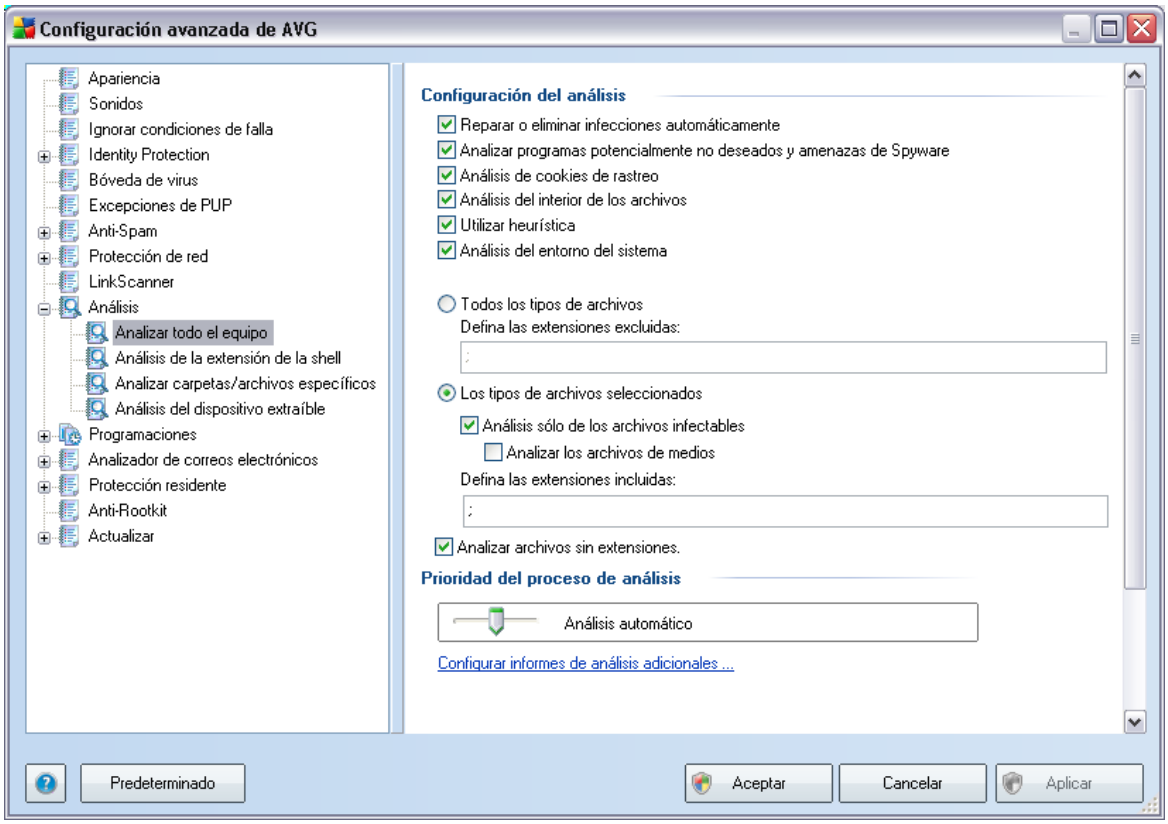
9.8. Análisis

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

9.8.1. 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 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***: este parámetro controla la función ***antivirus*** que hace posible la detección de programas potencialmente no deseados (*archivos ejecutables que se pueden ejecutar como spyware o adware*) y su bloqueo o eliminación.

- ***Analizar cookies de rastreo***: este parámetro del componente Anti-Spyware define qué 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 separadas por comas que no deben ser analizadas; o

- ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos infectables (*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 de medios (*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.

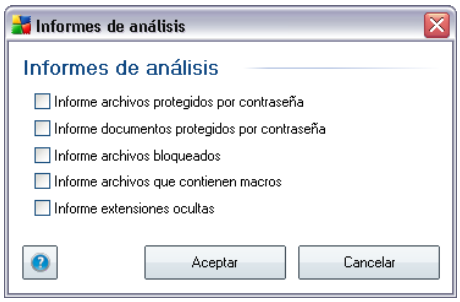
- En forma opcional, puede decidir si desea ***Analizar archivos sin extensión***: esta opción se encuentra activada de manera predeterminada, y se recomienda mantenerla activada a menos que tenga una razón válida para desactivarla. Los archivos sin extensión son muy sospechosos y siempre se deben analizar.

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.

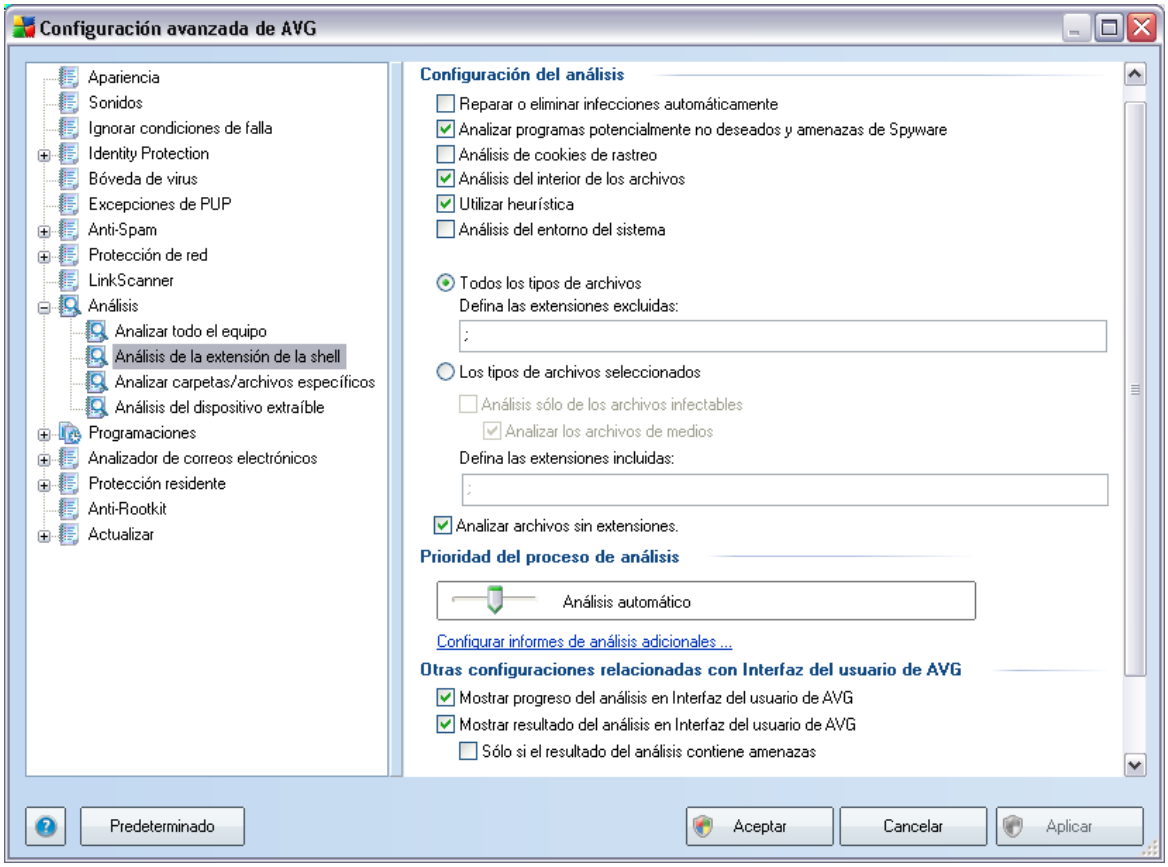
Configurar informes de análisis adicionales ...

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:



9.8.2. 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***:

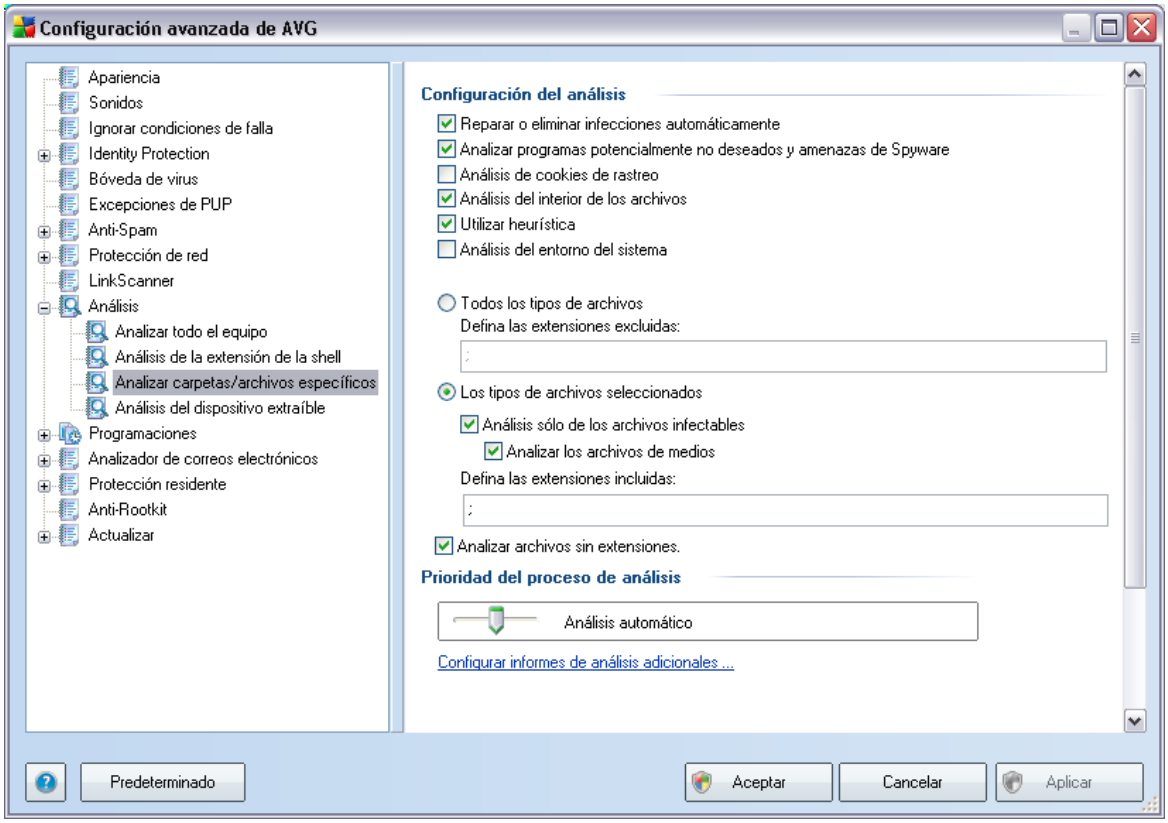


La lista de parámetros muestra parámetros idénticos a los que están disponibles en ***Análisis de todo el equipo***. Sin embargo, la configuración predeterminada varía: con ***Análisis de todo el equipo*** la mayoría de los parámetros están seleccionados, mientras que con ***Análisis de extensión de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

9.8.3. 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***:

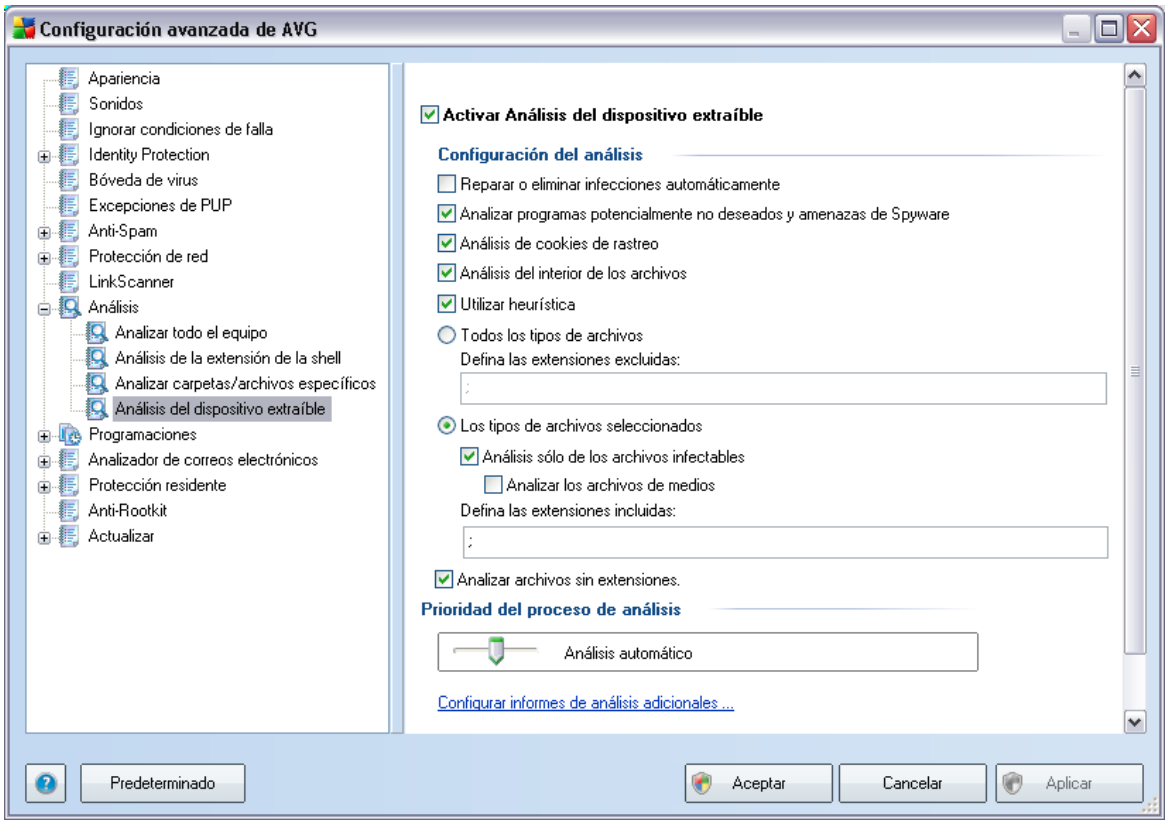


Todos los parámetros definidos en este diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con ***Análisis de archivos o carpetas específicos***. Si marca la opción ***Analizar en busca de rootkits*** de este diálogo de configuración, sólo se llevará a cabo un análisis rápido de rootkits, por ejemplo, el análisis únicamente de rootkits de áreas seleccionadas.

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

9.8.4. 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***

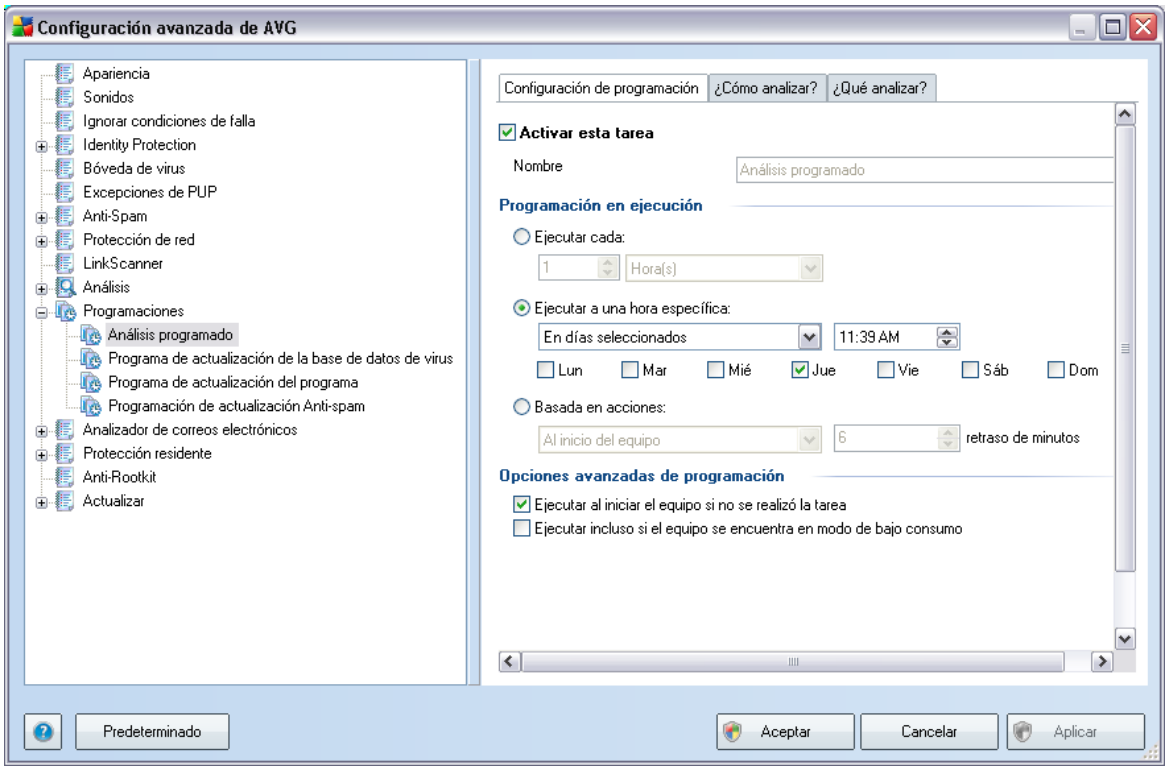
9.9. Programaciones

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

9.9.1. 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 todos 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 ratón 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:

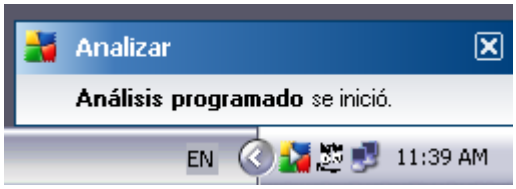
Programación en ejecución

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 de análisis (***Acción basada en el inicio del equipo***).

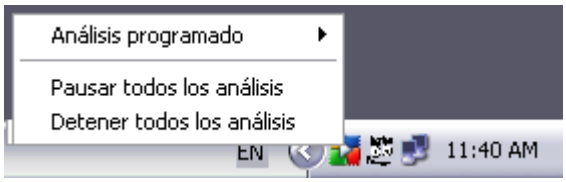
Opciones avanzadas de programación

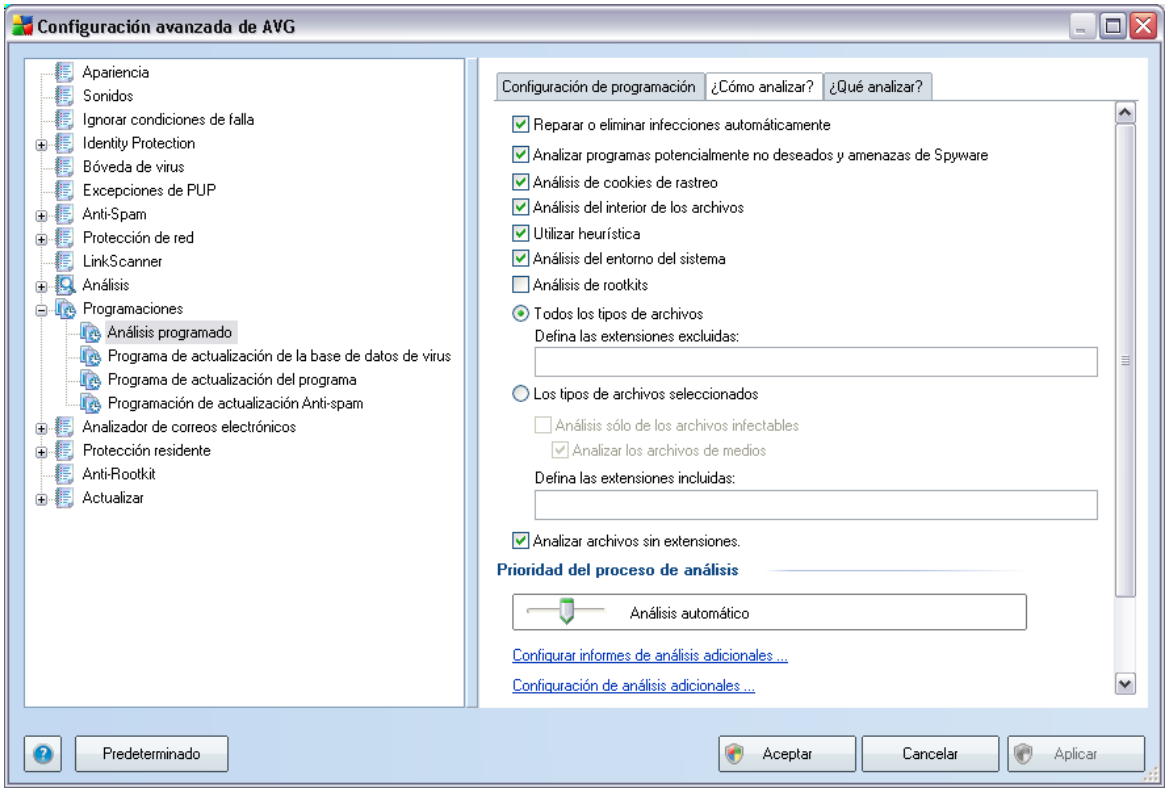
Esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

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***: *activado, de manera predeterminada*: si se identifica un virus durante el análisis, éste se puede reparar automáticamente si está disponible una vacuna 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*** (*activado de forma predeterminada*): este parámetro controla la función antivirus que permite la detección de programas potencialmente no deseados (*archivos ejecutables que se pueden ejecutar como spyware o adware*) para su posterior bloqueo o eliminación;

- ***Analizar cookies de rastreo*** (*activado de manera predeterminada*): este parámetro del componente Anti-Spyware define qué cookies deben detectarse 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 analizado en 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 separadas por comas que no deben ser analizadas; o

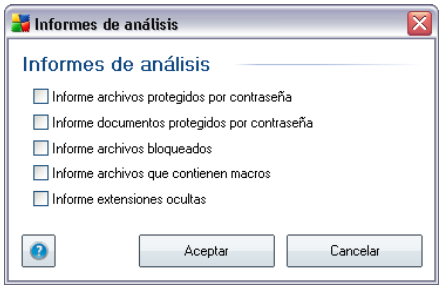
- ***Los tipos de archivos seleccionados***: puede especificar que sólo desea analizar los archivos que posiblemente se puedan infectar (*los archivos que no se pueden infectar no se analizarán, por ejemplo algunos archivos de texto sin formato, o algunos otros archivos no ejecutables*), incluidos los archivos multimedia (*archivos de video, audio; si deja estas casillas sin seleccionar, se reducirá el tiempo de análisis aún más, debido a que, con frecuencia, estos archivos son muy grandes y es poco probable que se infecten con un virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.

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

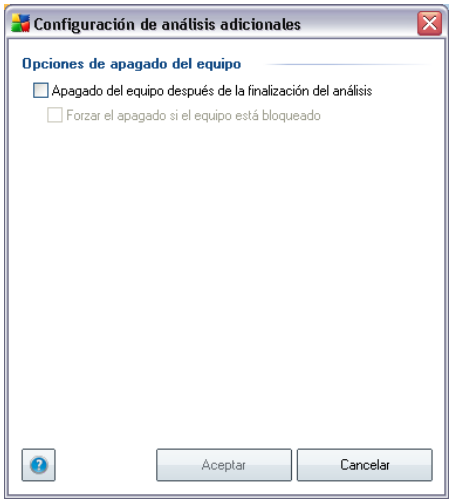
Prioridad del proceso de análisis

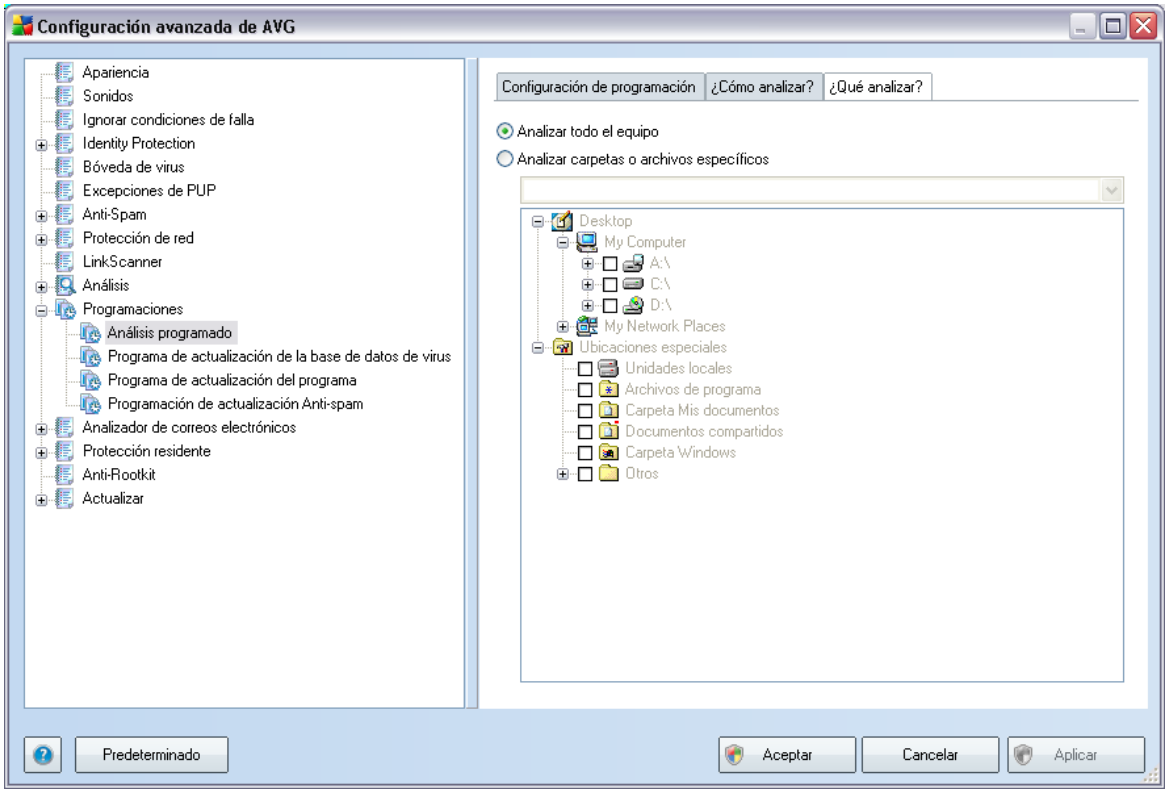
Dentro de la sección ***Prioridad del proceso de análisis*** se puede especificar de manera adicional la velocidad de análisis deseada dependiendo del empleo de recursos del sistema. De manera predeterminada, esta opción está establecida en el nivel medio de empleo automático de recursos. Si desea que 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 PC 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:



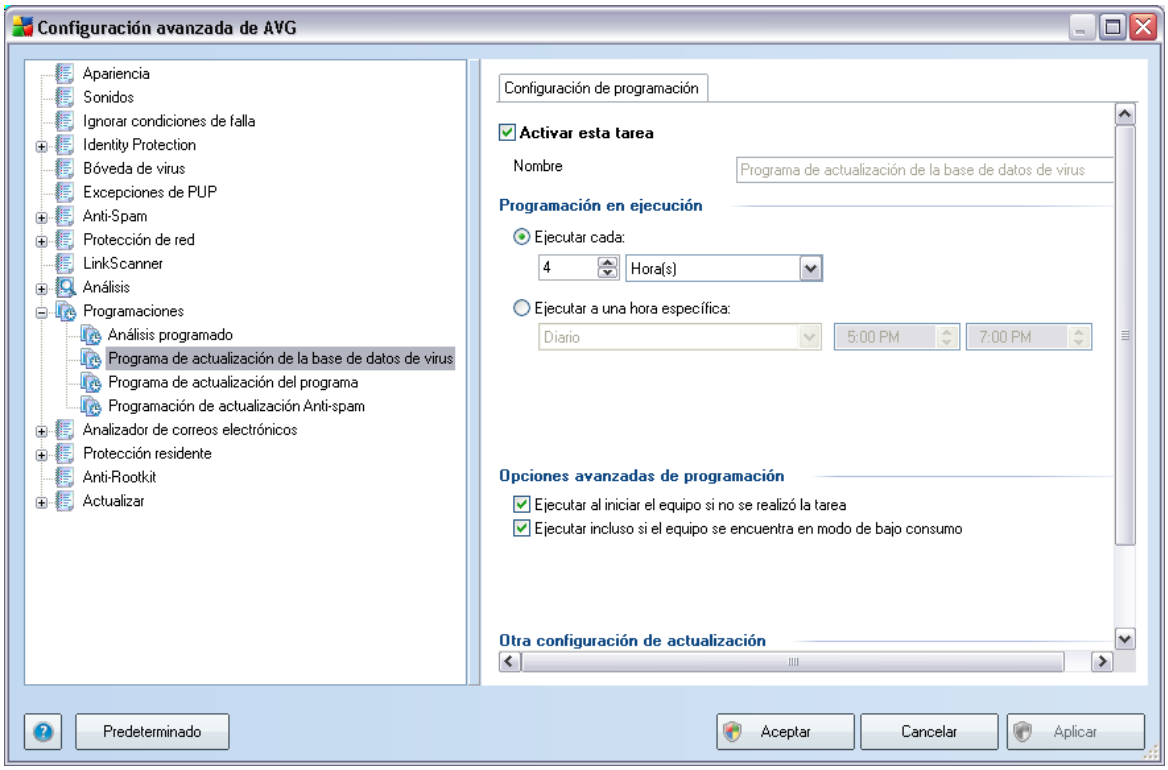
Haga clic en ***Configuración de análisis adicional***para abrir un nuevo diálogo de ***Opciones de apagado del equipo***, donde puede decidir si el equipo se debería apagar automáticamente en cuanto haya finalizado el proceso de análisis en ejecución. Después de haber confirmado esta opción (***Apagado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

9.9.2. 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*), se encuentra el nombre asignado a cada programación por el proveedor del programa. Para programaciones agregadas recientemente (*puede agregar una nueva programación haciendo clic con el botón secundario del ratón en el elemento* ***Programa de actualización de la base de datos de virus*** *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 siempre nombres breves, descriptivos y adecuados para las programaciones con el fin

de facilitar su reconocimiento más adelante.

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 exacta (***Ejecutar en una fecha y hora específica ...***), o posiblemente definiendo un evento con el que se debe asociar la ejecución de la actualización (***Acción basada en el arranque del equipo***).

Opciones avanzadas de programación

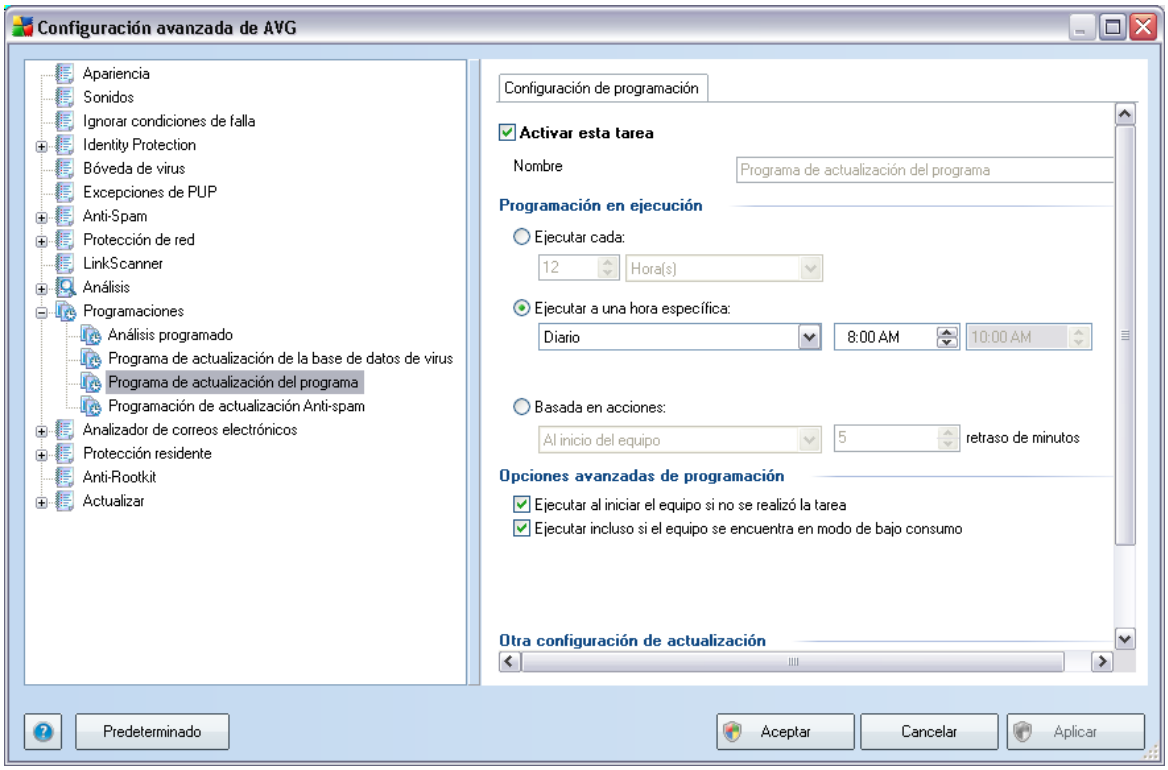
Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización de la base de datos de virus si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

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***).

9.9.3. Programación de actualización del programa



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*), se encuentra el nombre asignado a cada programación por el proveedor del programa. Para las programaciones agregadas recientemente (*es posible agregar una programación nueva haciendo clic con el botón secundario del ratón en el elemento* ***Programa de actualización del programa*** *en el árbol de navegación izquierdo*), puede especificar un nombre y, en este caso, el campo de texto estará abierto para su edición. Intente utilizar siempre nombres breves, descriptivos y adecuados para las programaciones con el fin de facilitar su reconocimiento más adelante.

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 ...***) o 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

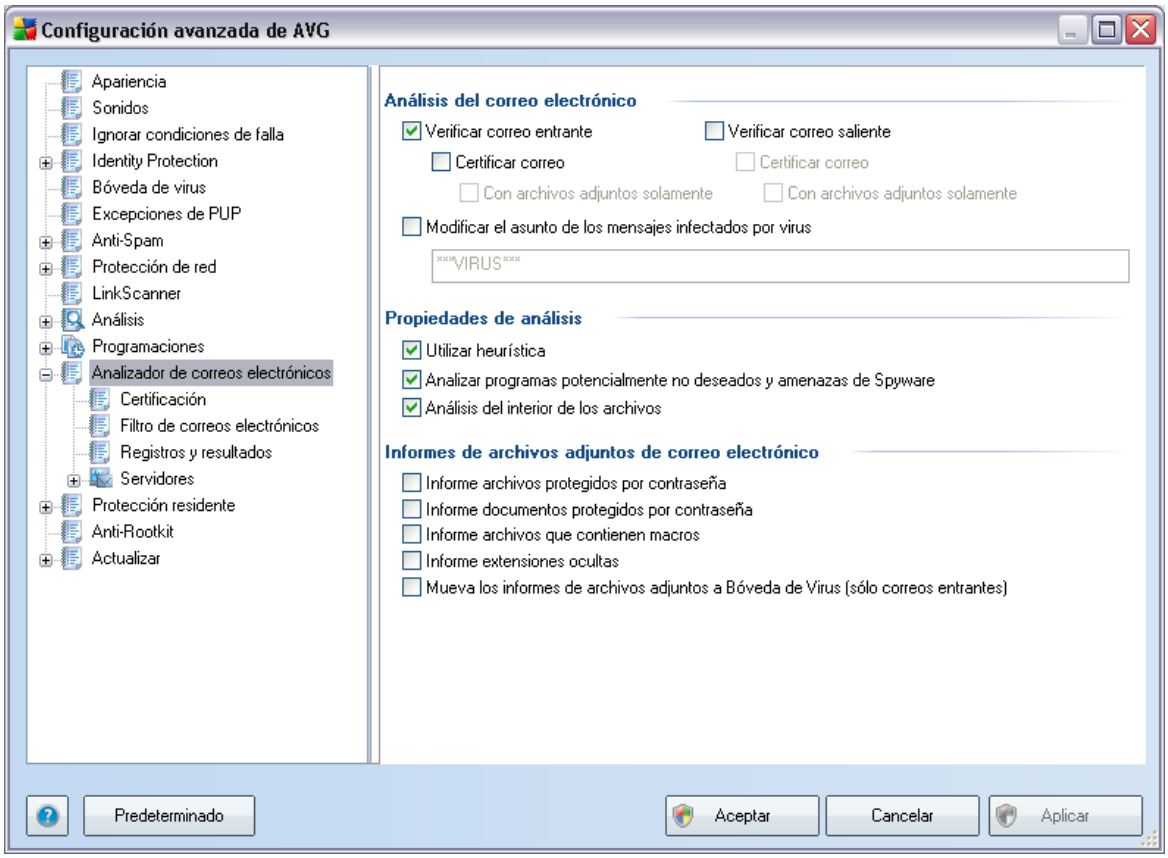
Esta sección le permite definir en qué condiciones debe o no ejecutarse la actualización del programa si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

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***).

9.10. Analizador de correos electrónicos



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

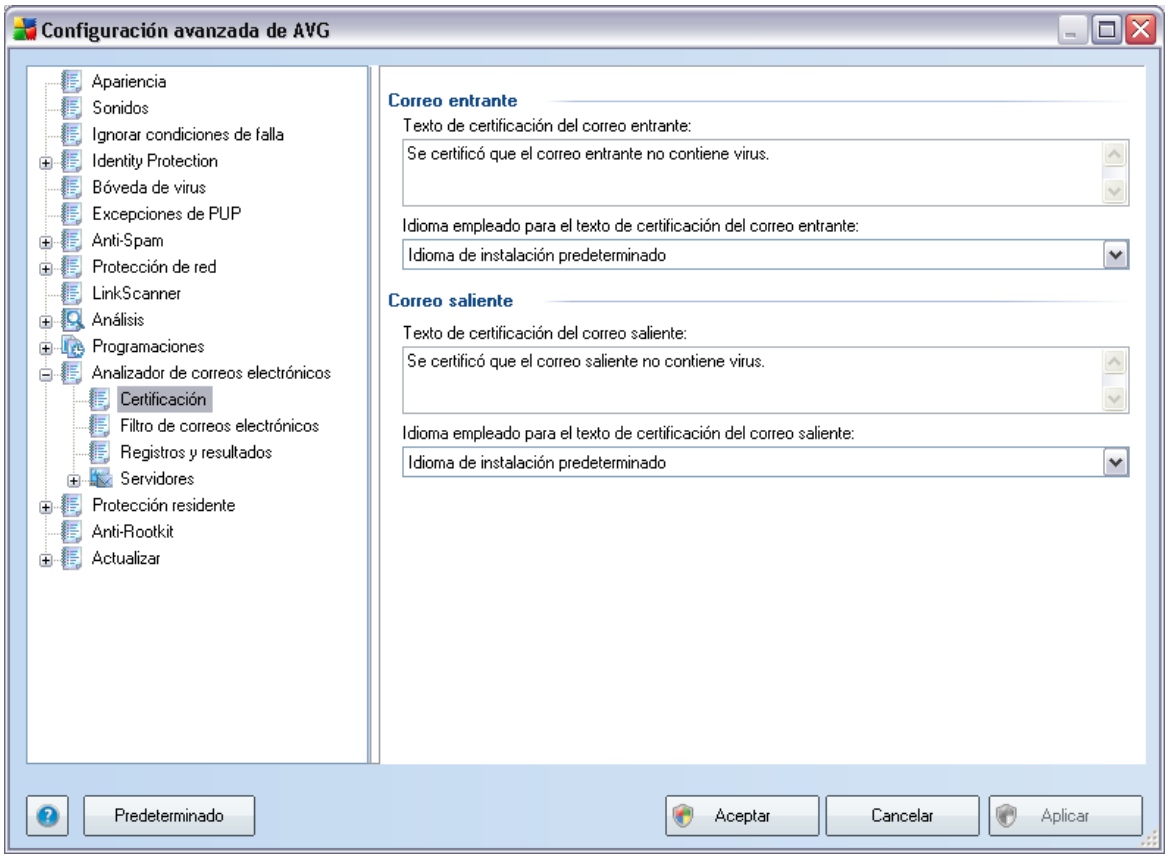
- ***Análisis de correos electrónicos***:en esta sección seleccione si desea analizar los mensajes de correo electrónico entrantes/salientes y si todos los correos electrónicos se deben certificar o sólo los correos electrónicos con datos adjuntos (la certificación de *correos electrónicos libres de virus no es compatible en el formato HTML/RTF*). Además, puede elegir si desea que AVG modifique el asunto de los mensajes que tengan posibles virus. Marque la casilla de verificación ***Modificar el asunto de los mensajes infectados con virus*** y cambie el texto respectivamente (*el valor predeterminado es ***VIRUS****).

- ***Propiedades de análisis***: especifique si se debe utilizar el método de análisis heurístico durante el análisis (***Utilizar método heurístico***), si desea comprobar la presencia de programas potencialmente no deseados (***Informar***

de programas potencialmente no deseados y amenazas de Spyware), y si también se deben analizar los archivos comprimidos (***Análisis del contenido de los archivos***).

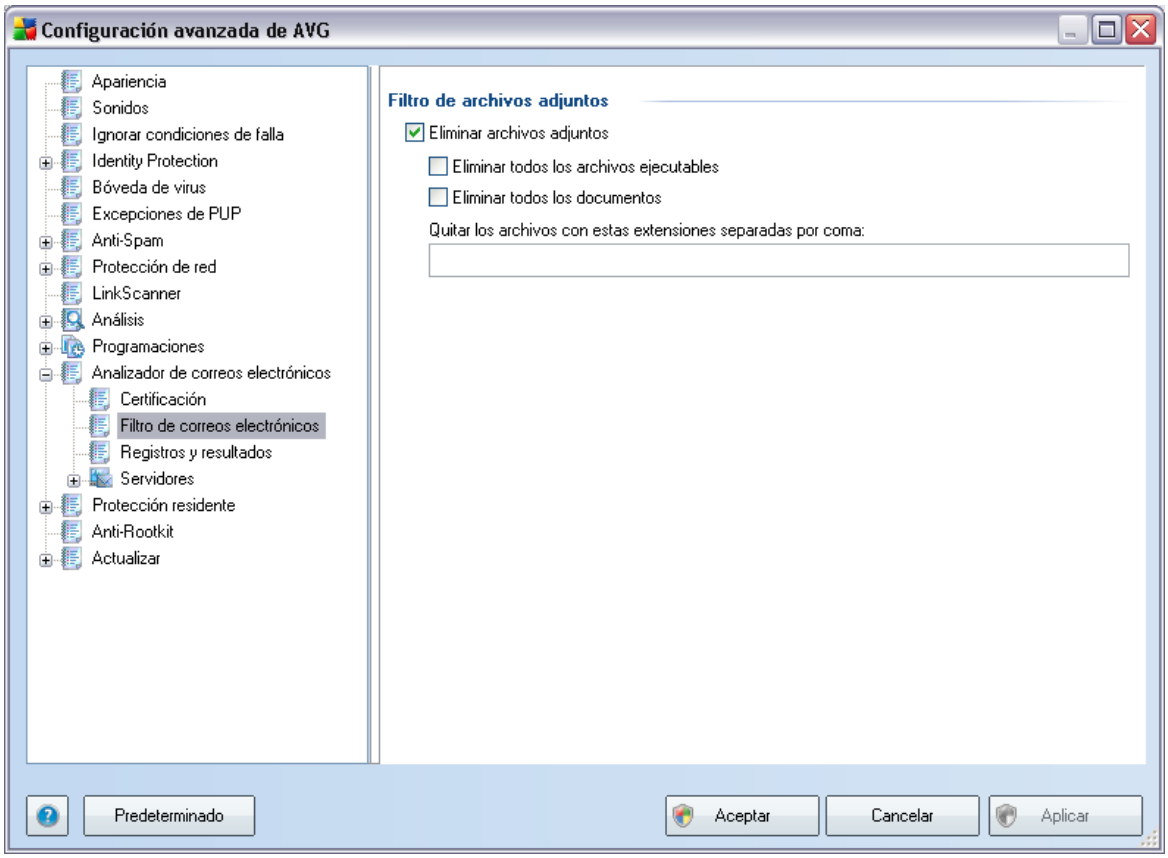
- ***Informes de archivos adjuntos de correo electrónico***: especifique si desea que se le notifique mediante correo electrónico acerca de los archivos protegidos con contraseña, los documentos protegidos con contraseña, los archivos que contienen macros y los archivos con extensión oculta detectados 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***.

9.10.1. 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***.

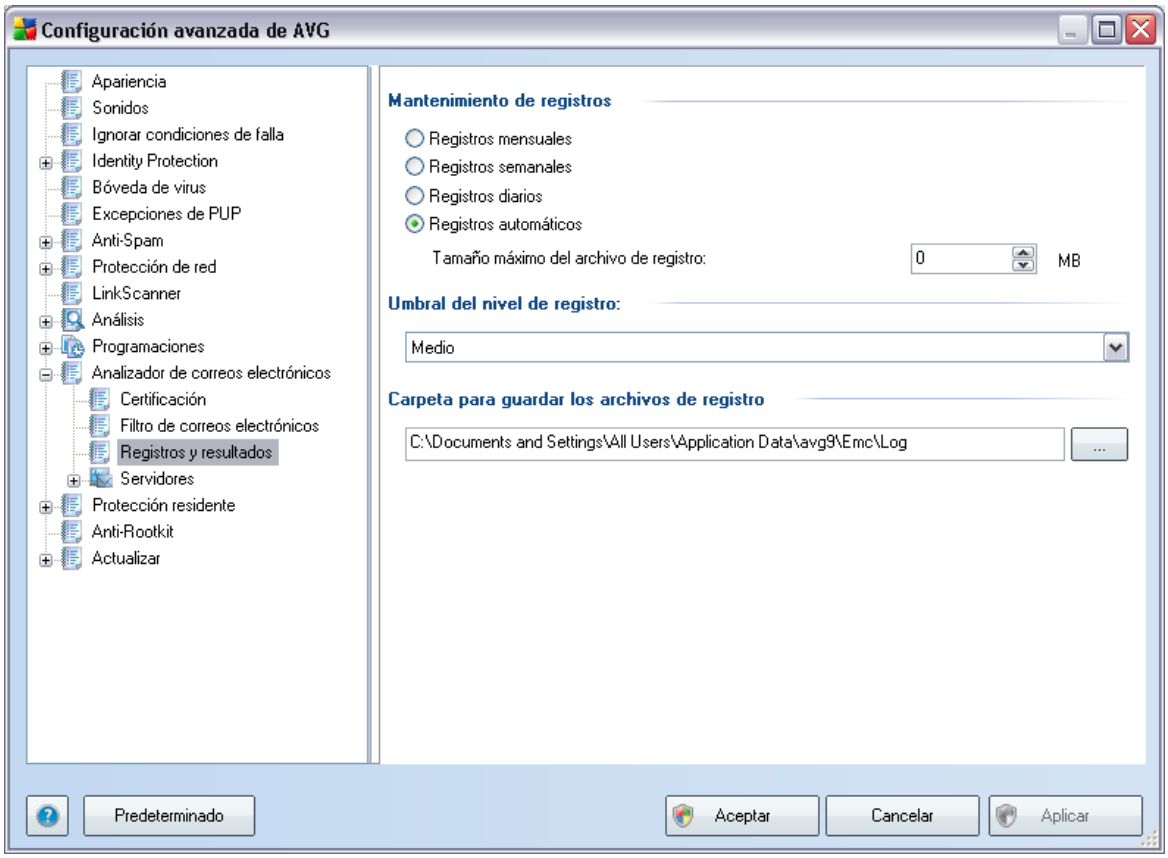
9.10.2. Filtro de correos electrónicos



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
- ***Eliminar los archivos con las siguientes extensiones separadas por coma***: se eliminarán todos los archivos con las extensiones definidas

9.10.3. Registros y resultados

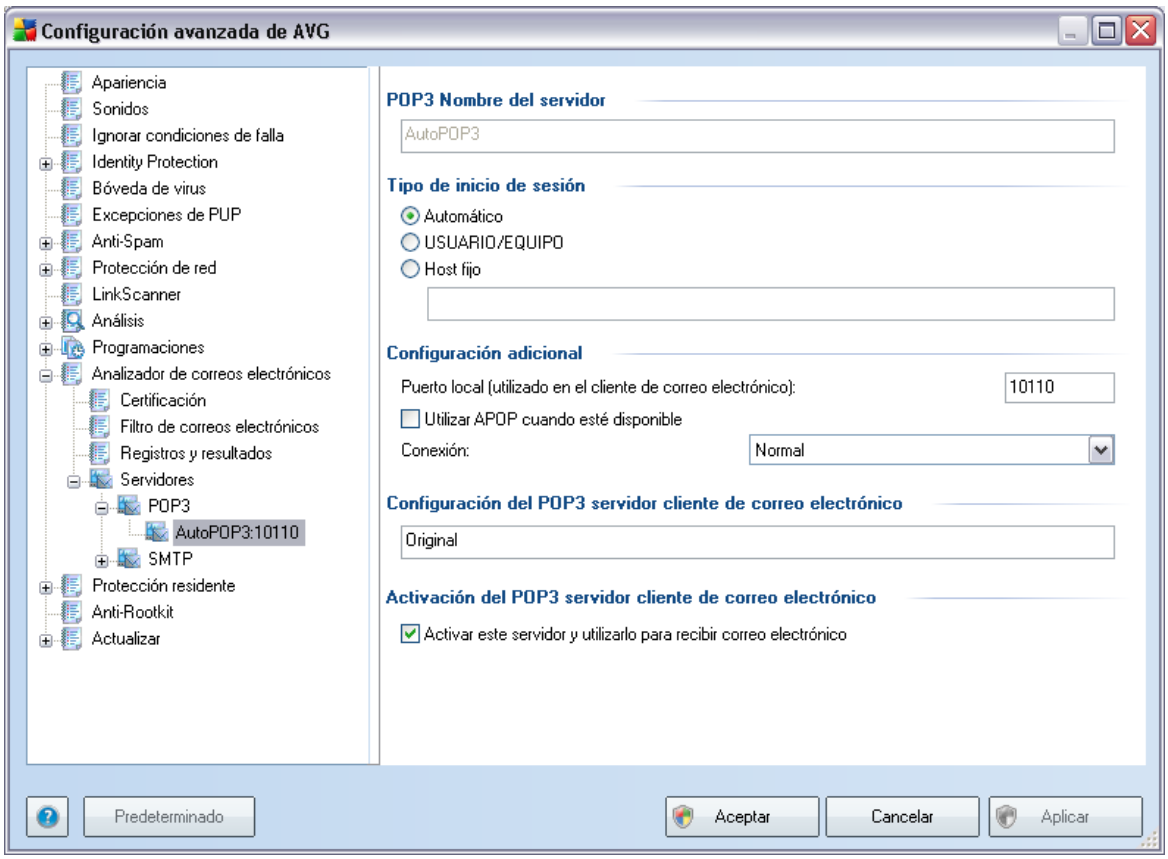


El diálogo abierto mediante el elemento de navegación ***Registros y resultados*** permite especificar los parámetros para el mantenimiento de los resultados del análisis de los correos electrónicos. El diálogo se divide en varias secciones:

- ***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

9.10.4. 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.

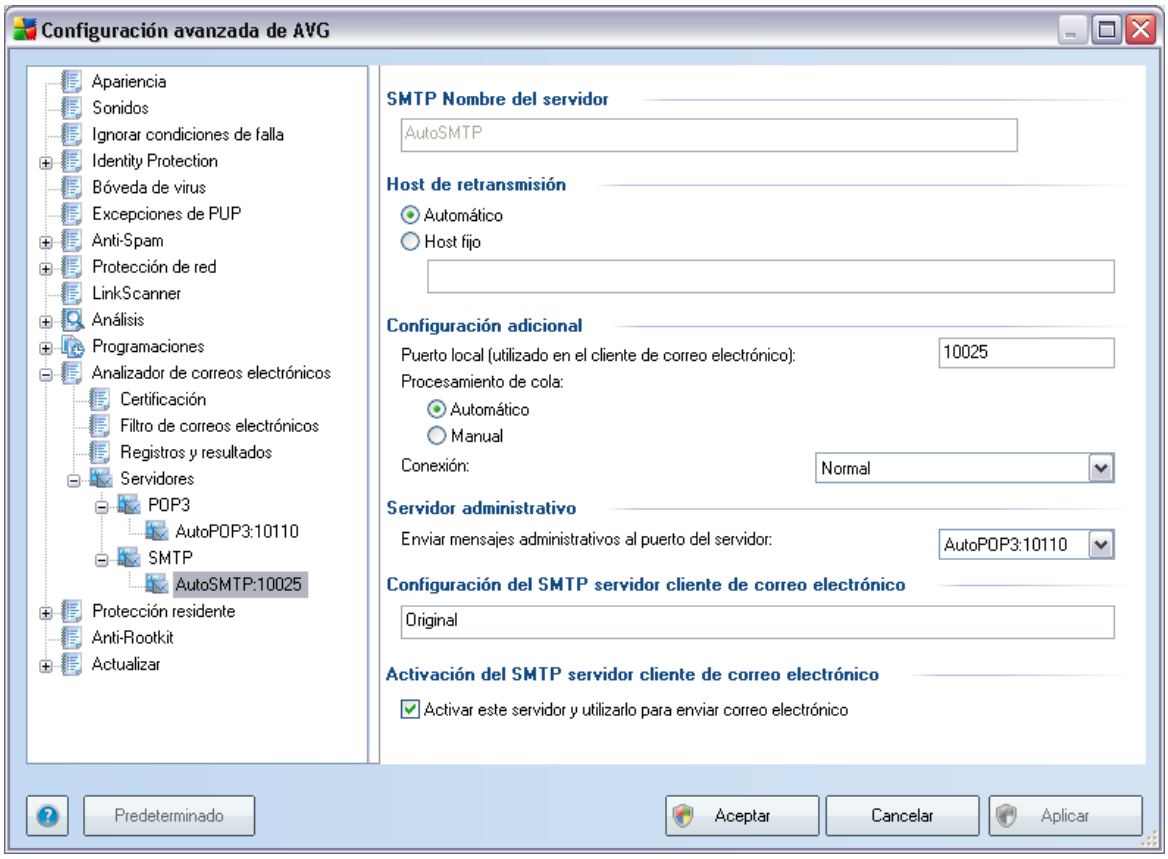
  - ***Utilizar APOP cuando esté disponible***: esta opción proporciona un inicio de sesión más seguro en el servidor de correo. Esto asegura que el ***Analizador de correos electrónicos*** utilice un método alternativo de enviar al servidor la contraseña de inicio de sesión de la cuenta del usuario no 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.

- ***Activación del servidor de cliente POP3 de correo electrónico***:

proporciona información breve sobre los valores necesarios 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 diálogos relacionados.

- ***Activación del servidor de cliente POP3 de correo electrónico***: seleccione/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.

- ***Relay Host*** : 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.

  - ***Servidor 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.

- ***Configuraciones adicionales***: especifica más parámetros detallados:

  - ***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

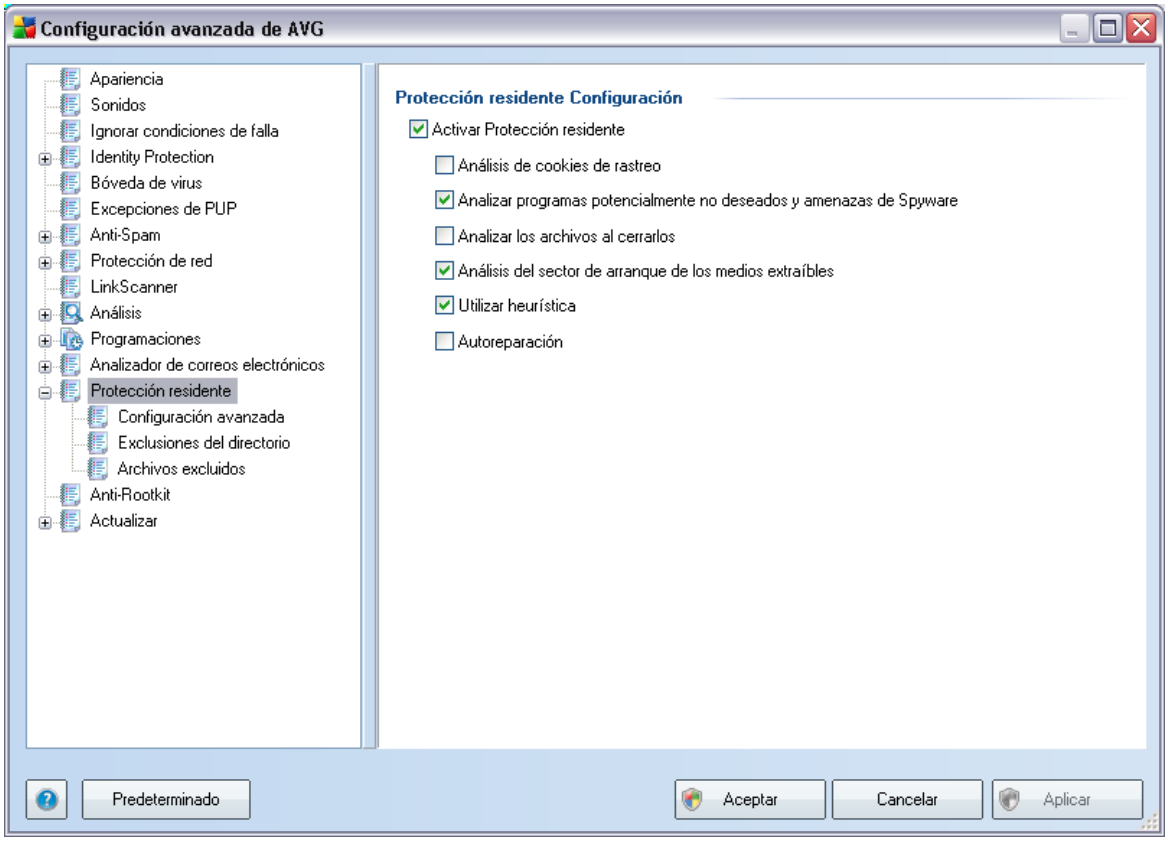
  - ***Conexión***: en este menú desplegable, puede especificar qué tipo de conexión se utilizará (normal/SSL/valor predeterminado de SSL). Si elige una conexión SSL, los datos enviados se encriptan sin el riesgo de ser rastreados o controlados por un tercero. Esta función sólo se encuentra disponible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

9.11. 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*** (*opción activada de modo predeterminado*): analiza los programas potencialmente no deseados (*aplicaciones ejecutables que pueden actuar como diversos tipos de spyware o adware*).

- ***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.

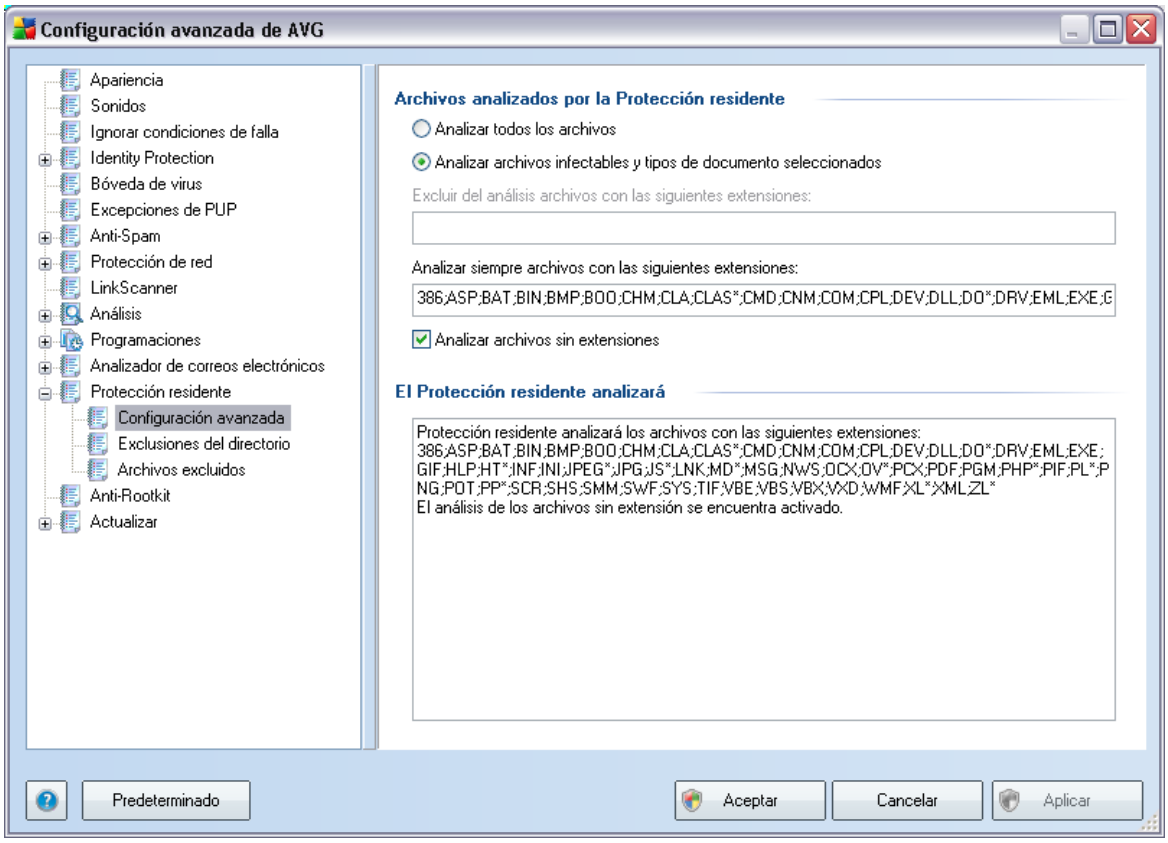
- ***Analizar sector de arranque de medios extraíbles***: (*opción seleccionada de modo predeterminado*).

- ***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*).

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

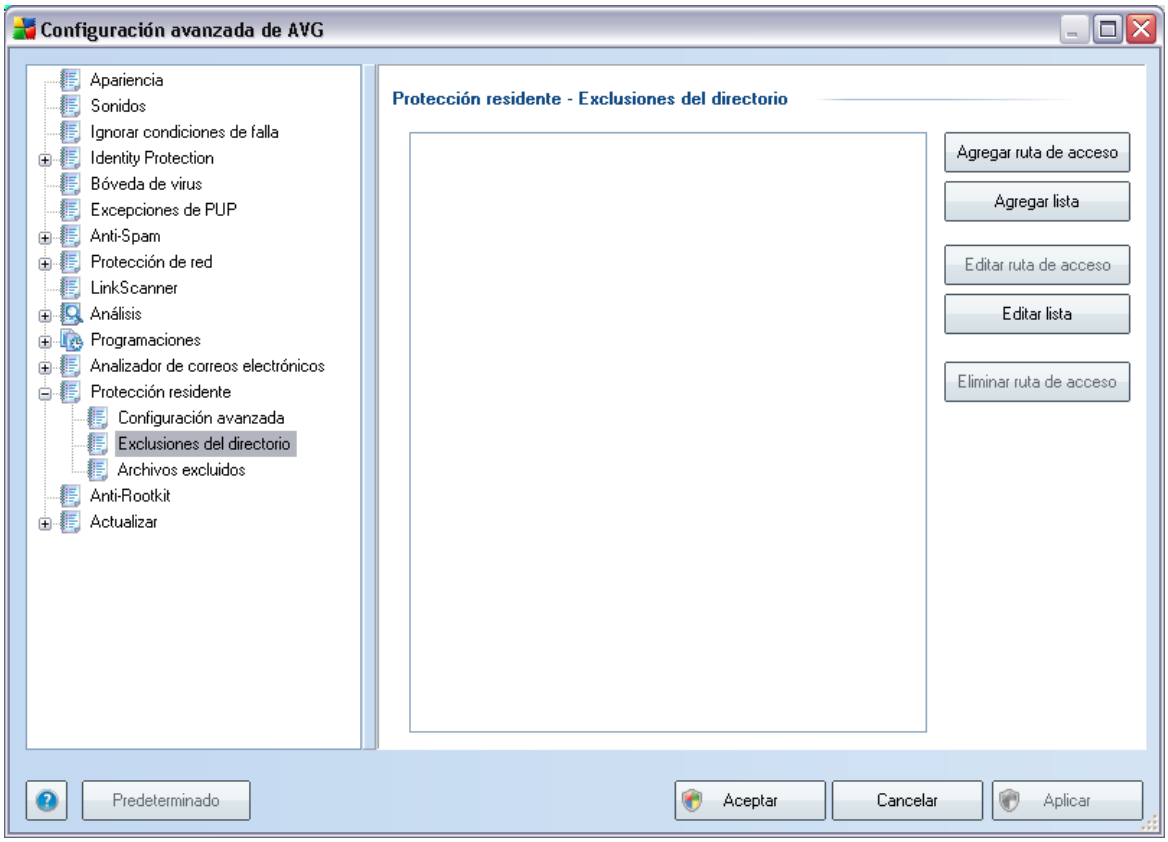
9.11.1. Configuración avanzada

En el 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.

9.11.2. 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.

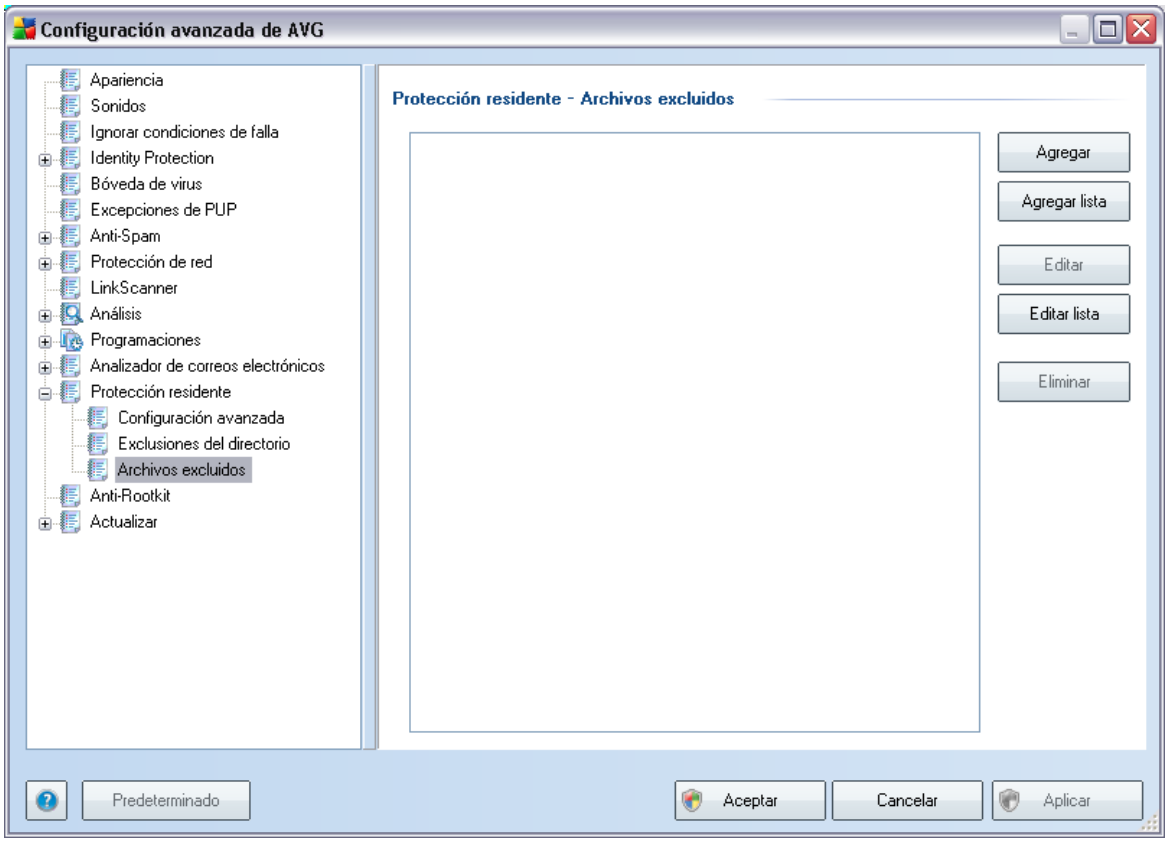
El diálogo proporciona los siguientes botones de control:

- ***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.

9.11.3. Archivos excluidos



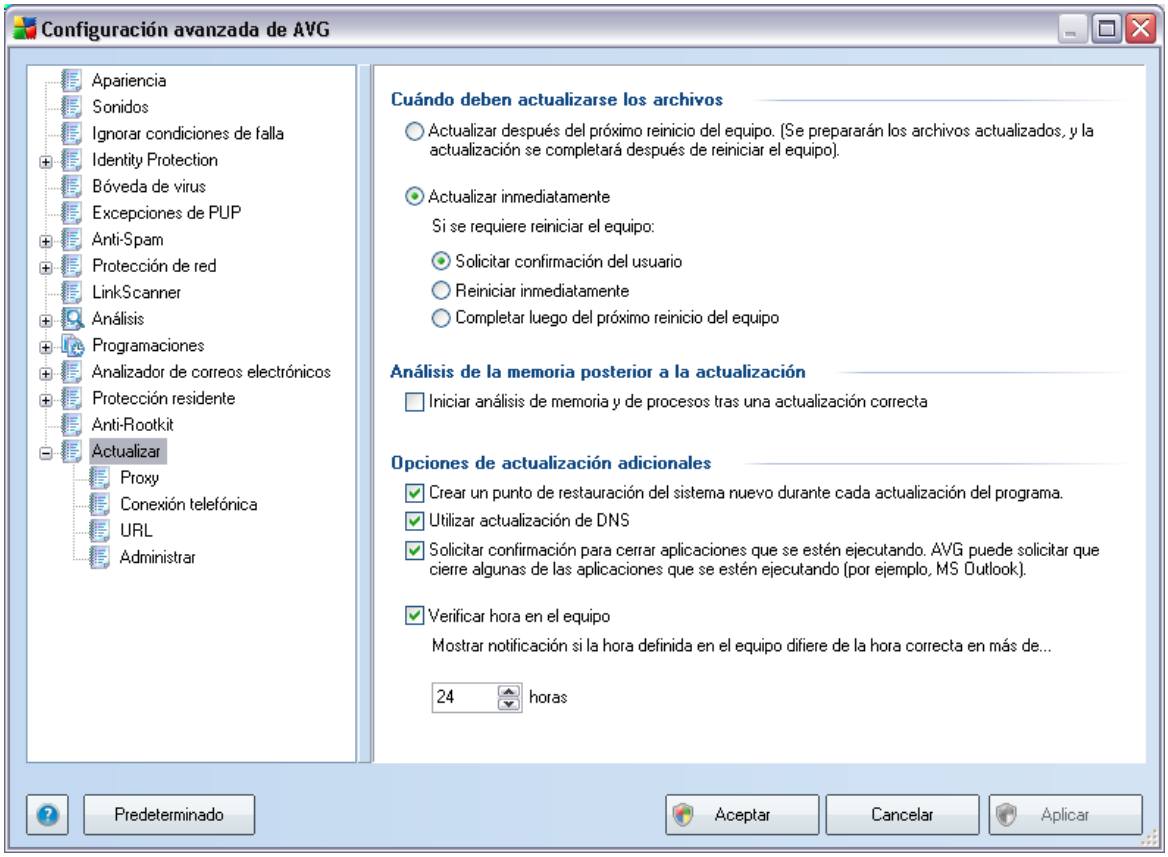
El cuadro de diálogo ***Protección residente - Archivos excluidos*** se comporta como el cuadro de diálogo descrito con anterioridad ***Protección residente - Exclusiones del directorio*** pero en lugar de carpetas ahora puede definir archivos específicos que se deben excluir del análisis de la ***Protección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

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

El diálogo proporciona los siguientes botones de control:

- ***Agregar*** : especifique los directorios 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 directorios que desea excluir del análisis de la ***Protección residente***
- ***Editar*** : le permite editar la ruta de acceso especificada de una carpeta seleccionada
- ***Editar lista*** : le permite editar la lista de carpetas
- ***Eliminar*** : le permite eliminar la ruta de acceso a una carpeta seleccionada de la lista

9.12. 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 el proceso 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

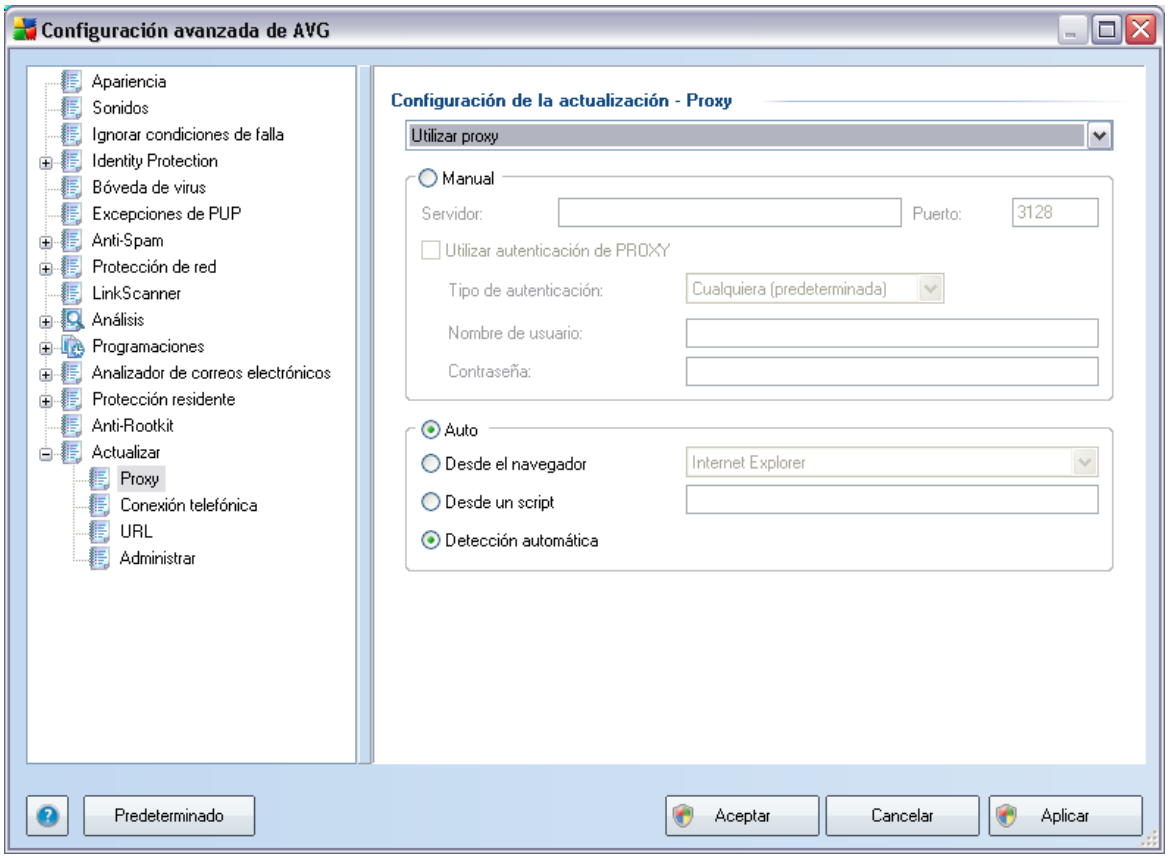
sistema operativo a su configuración original desde este punto. Esta opción es accesible mediante Inicio / Todos los programas / Accesorios / Herramientas del sistema /Restauración del sistema, pero se recomienda que sólo los usuarios experimentados realicen cambios. Mantenga esta casilla seleccionada 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;

- ***Si selecciona el elemento Solicitar confirmación para cerrar aplicaciones que se estén ejecutando*** (*activado de forma predeterminada*), 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.

9.12.1. 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***
- ***Intentar conectar utilizando proxy y, si falla, conectar directamente***: configuración predeterminada

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*).

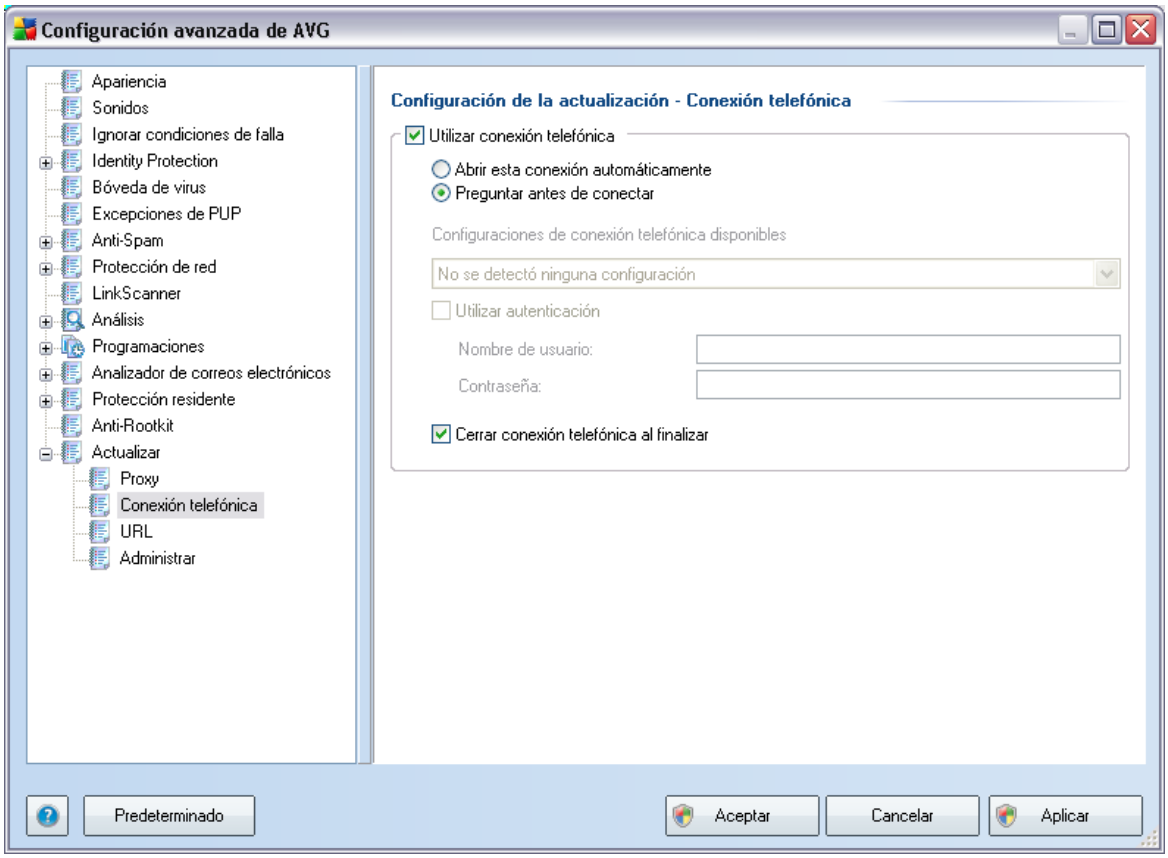
El servidor proxy también puede tener reglas específicas configuradas para cada usuario. Si el servidor proxy está configurado de este modo, seleccione la opción ***Utilizar autenticación de PROXY*** para verificar que el nombre de usuario y la contraseña sean válidos para la conexión a Internet mediante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

Configuración automática

Si selecciona la configuración automática (*marque la opción* ***Auto*** *para activar la sección del 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

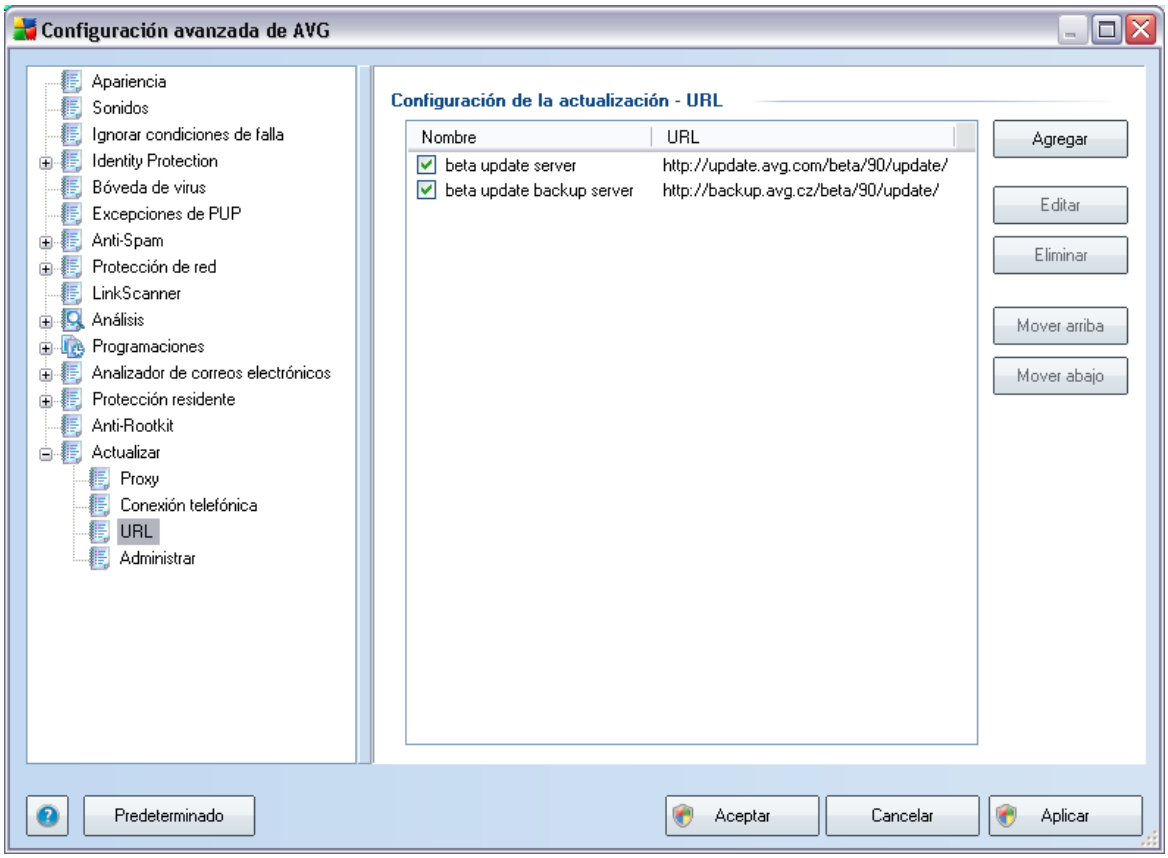
9.12.2. Conexión telefónica



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***).

9.12.3. URL



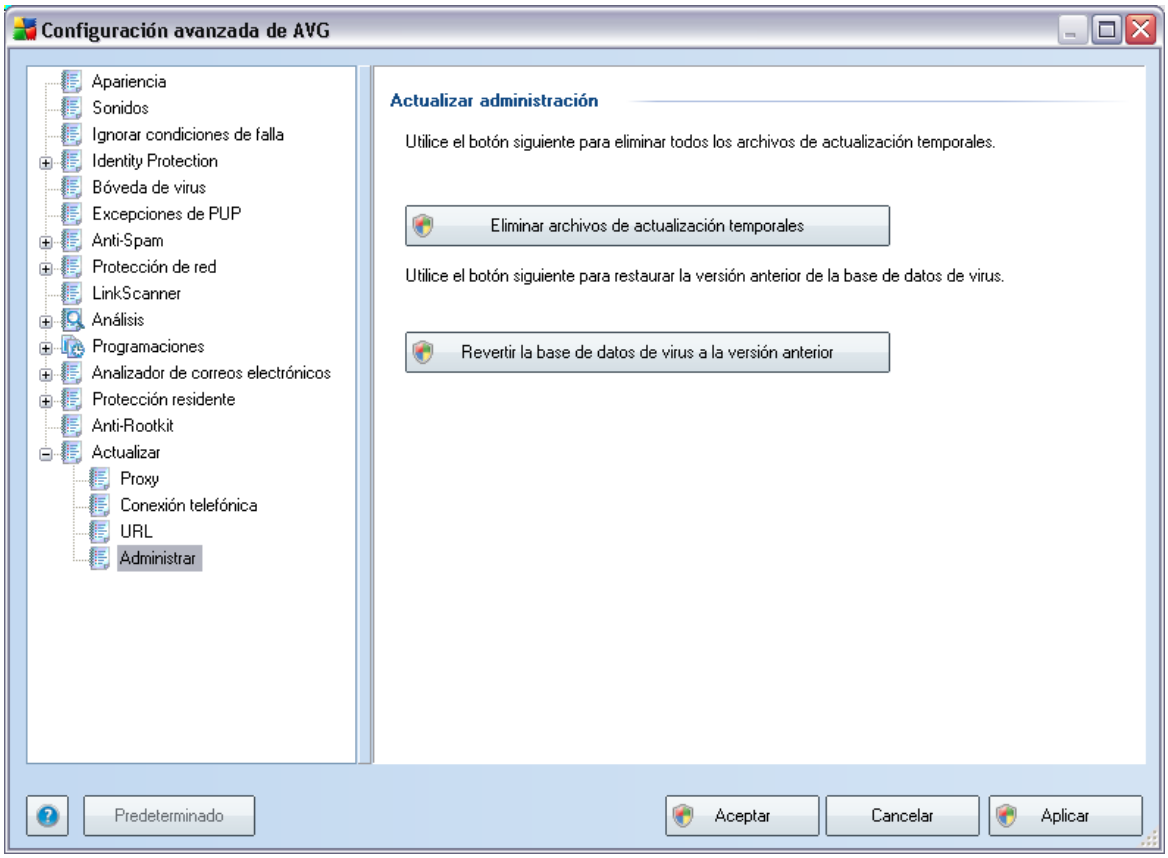
El diálogo ***URL*** ofrece una lista de direcciones de Internet desde las que se pueden descargar los archivos de actualización. La lista y los elementos se pueden modificar por medio de los siguientes botones de control:

- ***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.

9.12.4. Administrar

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



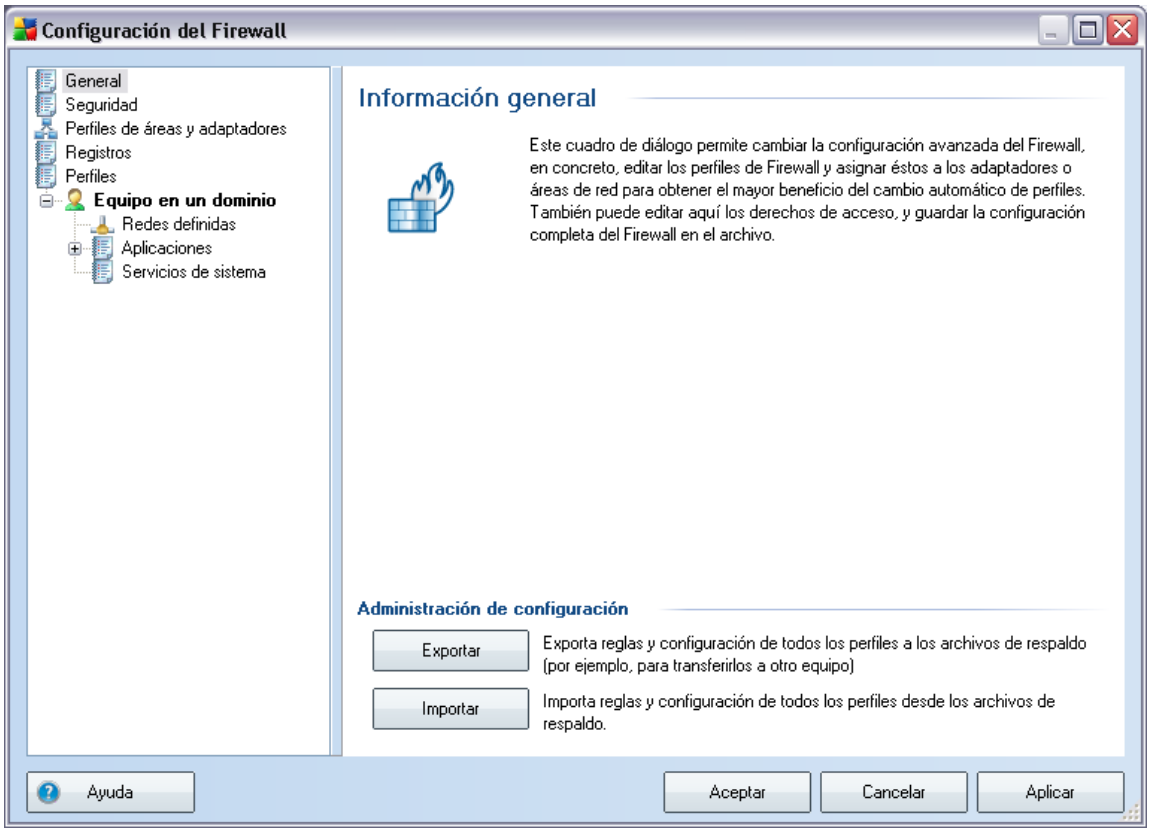
- ***Eliminar archivos de actualización temporales***: presione este botón para eliminar todos los archivos de actualización redundantes del disco duro (*de forma predeterminada estos archivos se guardan durante 30 días*)

- ***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. Configuración del Firewall

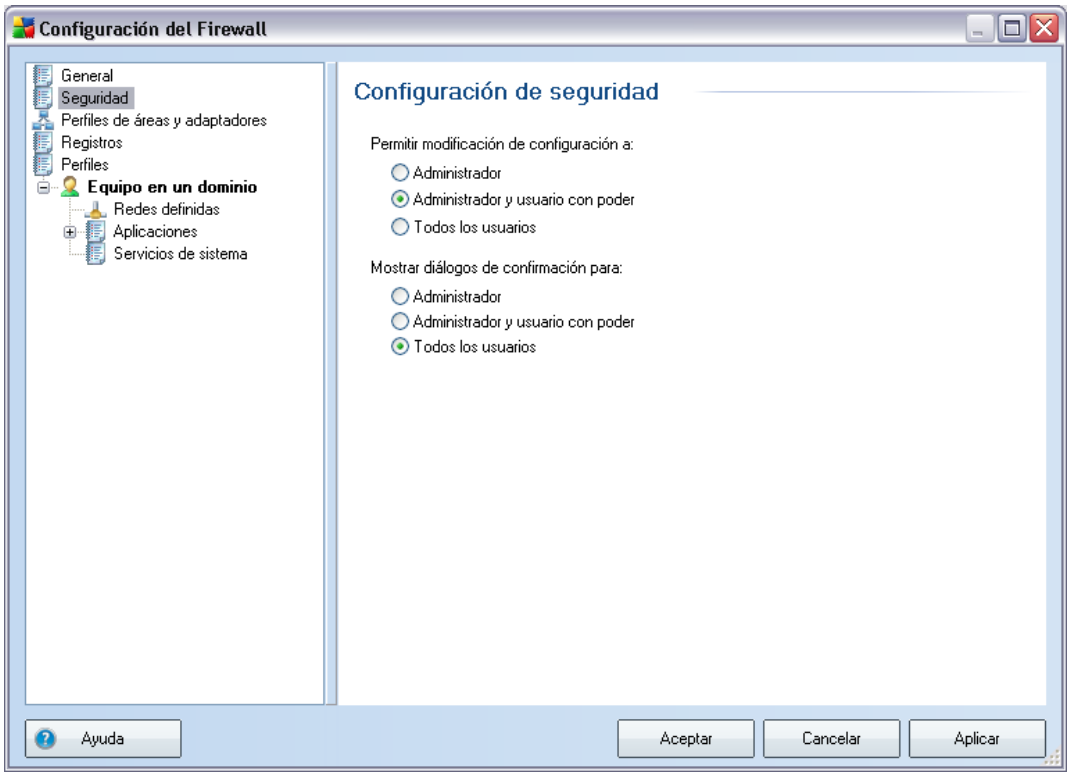
La configuración del ***Firewall*** se abre en una nueva ventana donde se pueden establecer parámetros muy avanzados del componente en varios diálogos. ***Sin embargo, la edición de la configuración avanzada sólo está pensada para expertos y usuarios con experiencia.***

10.1. 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.

10.2. 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***)

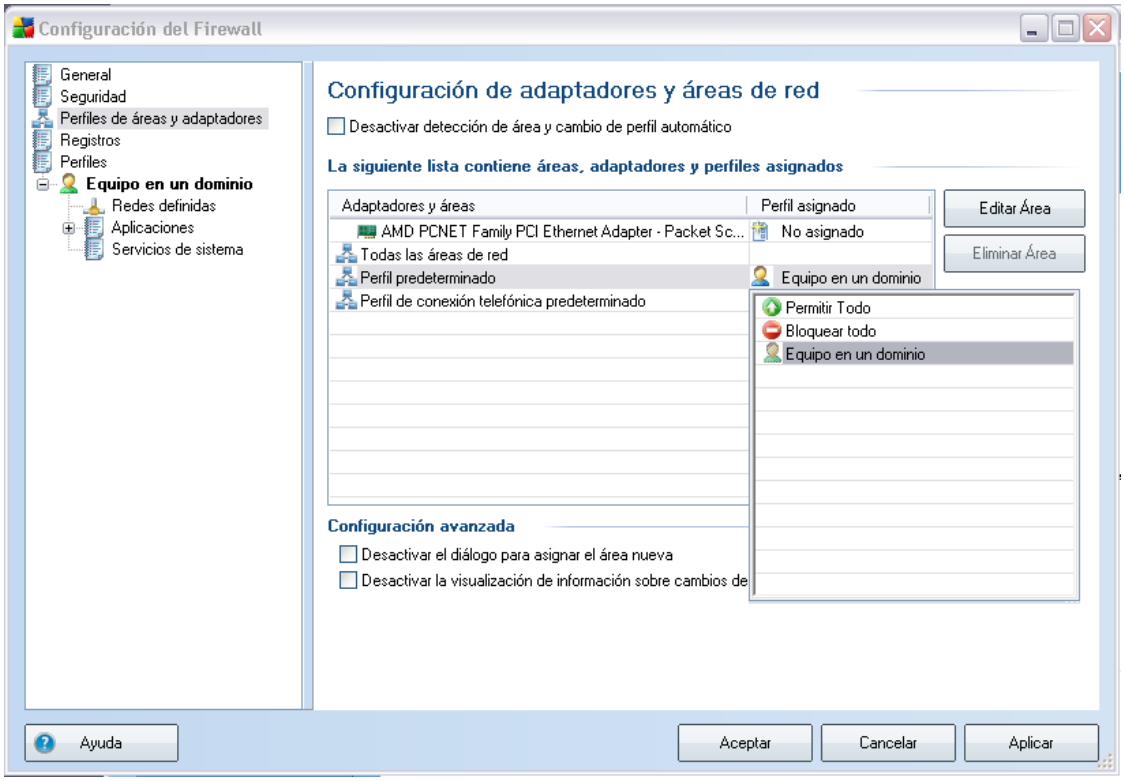
En ambos casos puede asignar el derecho específico a uno de los siguientes grupos de usuarios:

  - ***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

10.3. 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:

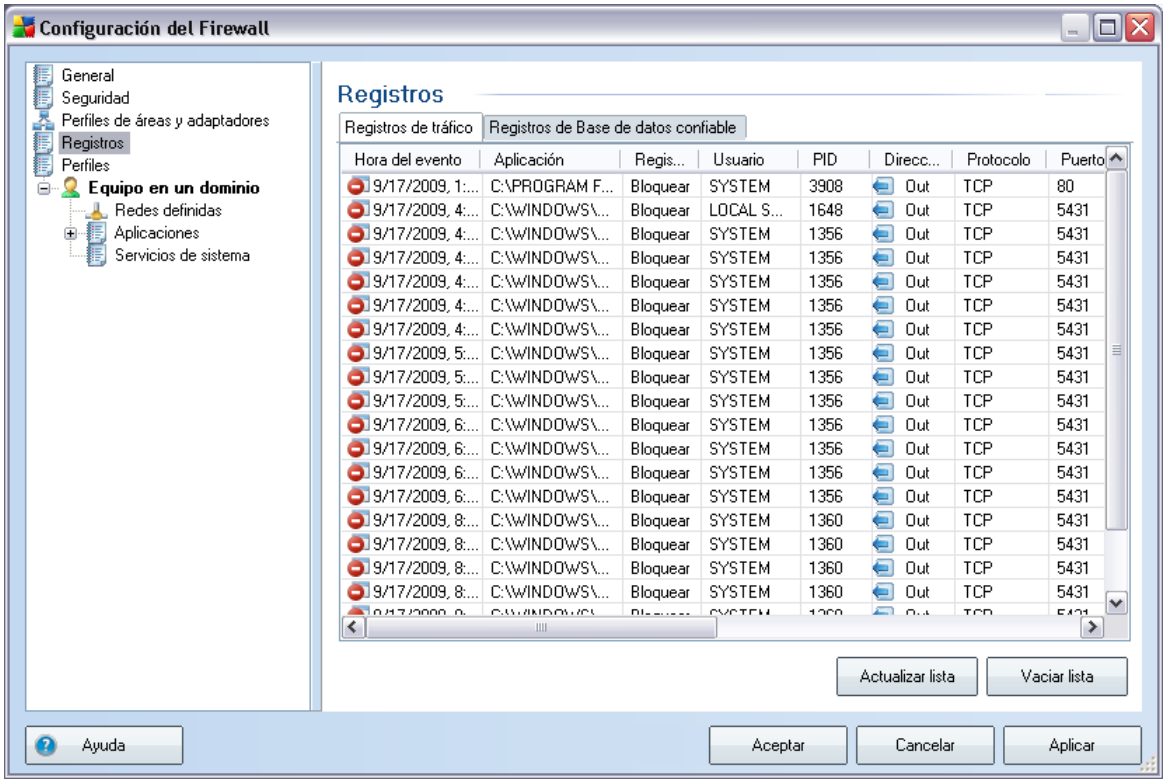
- ***Desactivar la detección de área y el cambio automático de perfil***: uno de los perfiles definidos puede asignarse a cada tipo de interfaz de red, de forma respectiva a cada área. Si desea definir perfiles específicos, se utilizará un perfil común definido según la selección de uso del equipo y 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 ***Desactivar la detección de área y el cambio automático de perfil***.

- ***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..

10.4. Registros



El cuadro de diálogo ***Registros*** le permite revisar la lista de todas las acciones y eventos del ***Firewall*** registrados con una descripción detallada de los parámetros pertinentes (*la hora del evento, el nombre de la aplicación, la acción de registro correspondiente, el nombre de usuario, la 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*** : *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 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

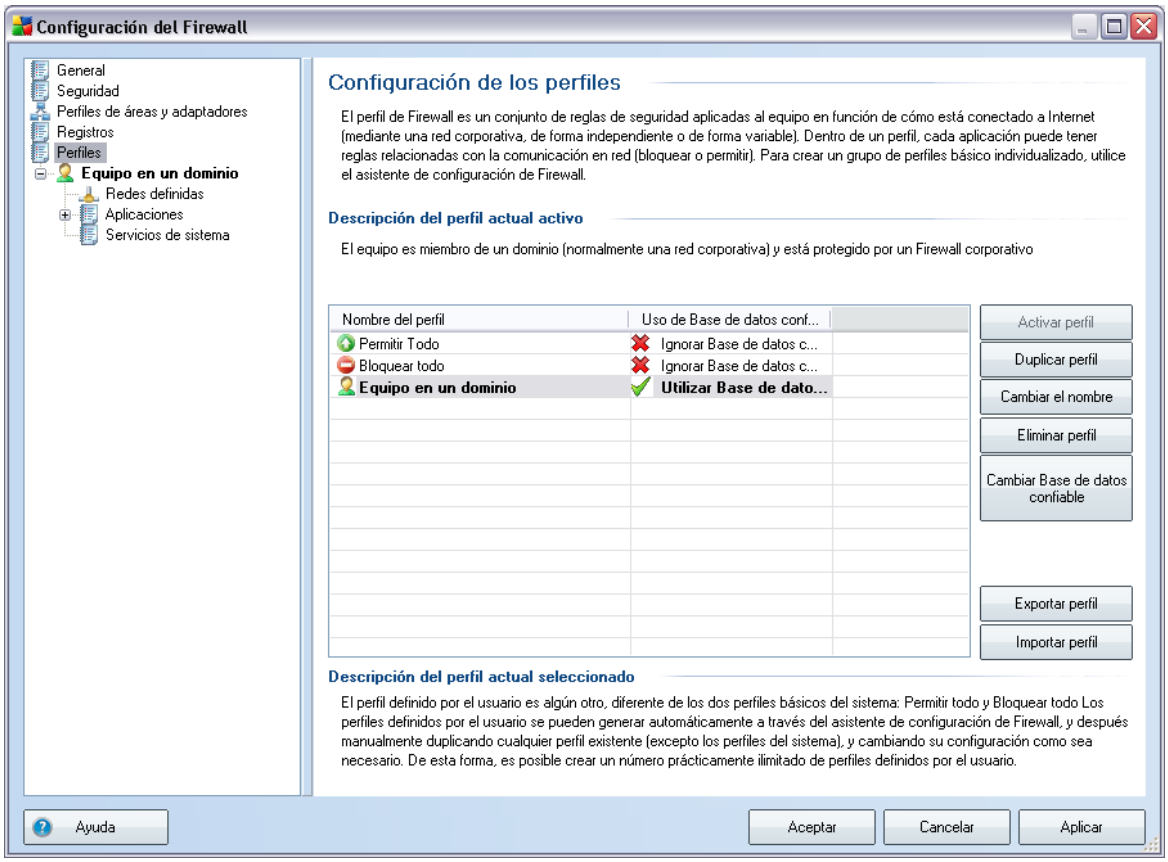
- ***Ayuda***: abre los archivos de ayuda relacionados con el diálogo activo.

- ***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.

10.5. Perfiles

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



Todos los demás perfiles del 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

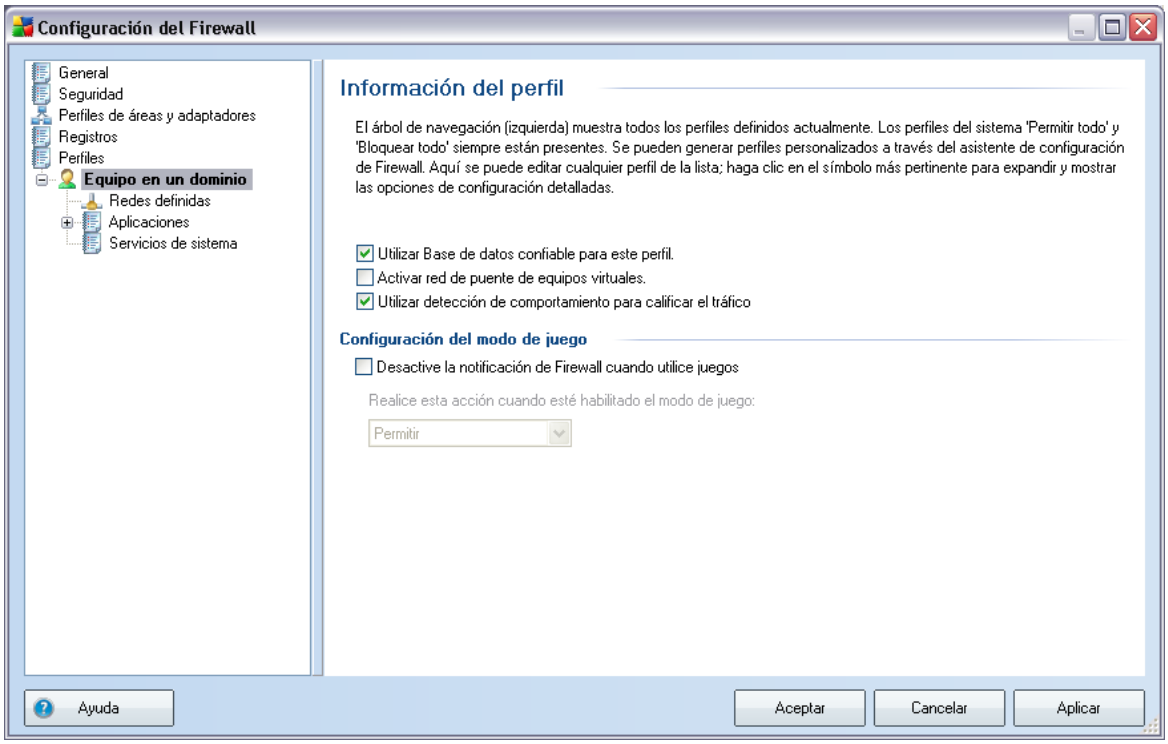
perfil seleccionado

- ***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*):

10.5.1. Información del perfil



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

- ***Utilizar Base de datos confiable para este perfil***: (*activada de forma predeterminada*) 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. Si no está en la lista, se le solicitará que decida si se debe permitir a la aplicación comunicarse a través de la red*) con el perfil correspondiente.

- ***Permitir redes Virtual Machines Bridget***: (*desactivado de manera predeterminada*) seleccione este elemento para permitir que las máquinas virtuales de VMware se conecten directamente a la red.

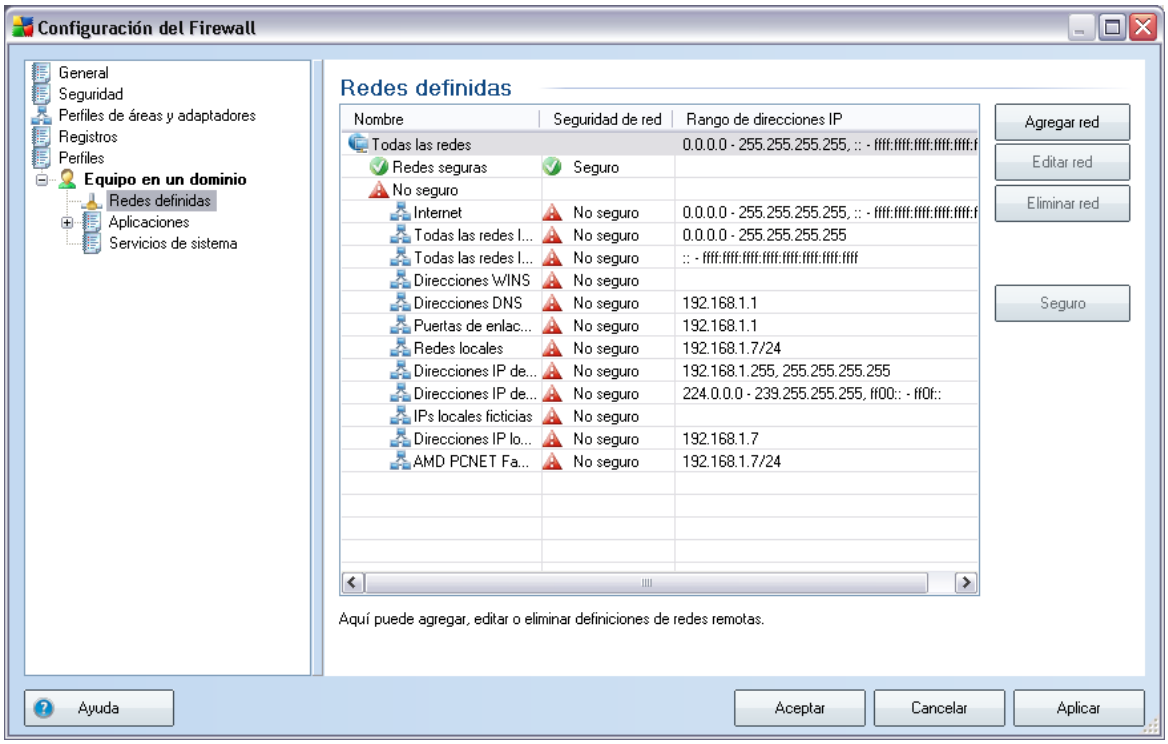
- ***Utilizar detección de comportamiento para calificar el tráfico*** : (*activada de manera predeterminada*) seleccione esta opción para permitir que el ***Firewall*** utilice la funcionalidad de ***LinkScanner*** al evaluar una aplicación; ***LinkScanner*** puede determinar si la aplicación muestra algún comportamiento sospechoso, o si se puede confiar en ella y se le debe permitir la comunicación en línea.

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 diálogo de confirmación*), todas estas aplicaciones pueden permitirse o bloquearse.

10.5.2. Redes definidas

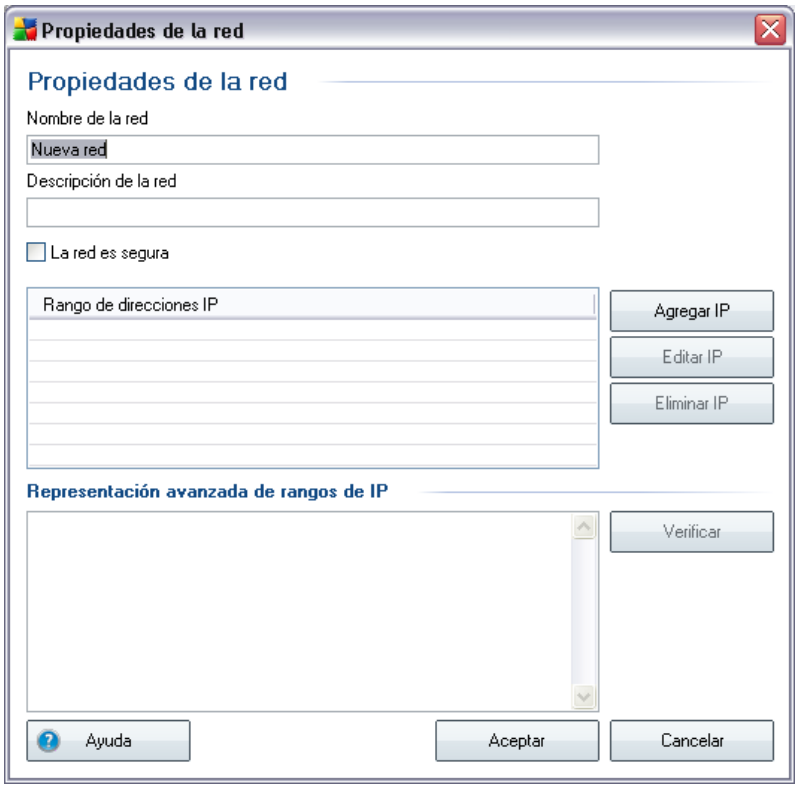


El diálogo ***Redes definidas*** ofrece una lista de todas las redes a las que está conectada su equipo. Se proporciona la siguiente información en cada red detectada:

- ***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 comunican 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 diálogo independiente que se abre mediante el botón ***Agregar IP*** (de forma alternativa, ***Editar IP***/ ***EliminarIP***), dentro de este diálogo puede especificar la red utilizando su rango o máscara IP.

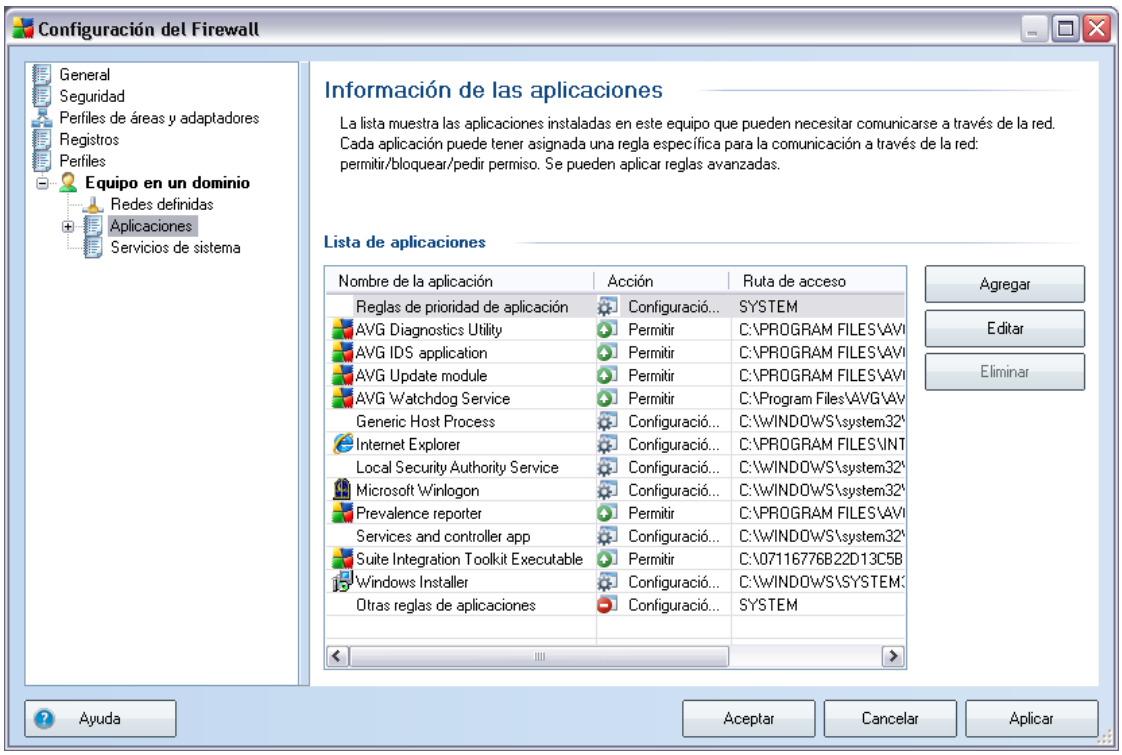
  Para establecer varias redes que deben definirse como parte de una red creada recientemente, puede utilizar la opción de ***Representación avanzada de rango IP***: introduzca la lista de todas las redes en el campo de texto respectivo (*es compatible con cualquier formato estándar* y presione el botón ***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 asignarle el estado de segura a una red si está seguro de que la red es segura
- ***Ayuda***: abre el archivo de ayuda relacionado con el diálogo activo

10.5.3. Aplicaciones

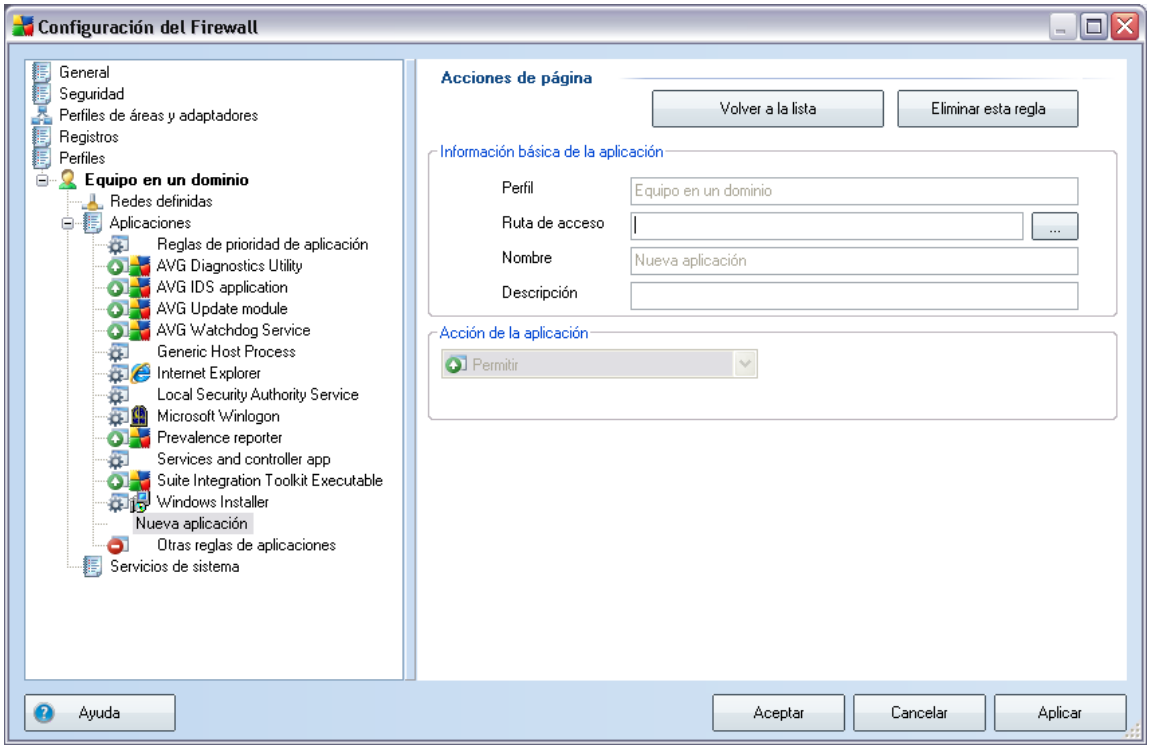


En el cuadro de diálogo ***Información de las aplicaciones*** puede encontrar una descripción general de todas las aplicaciones que se comunican mediante la red. La lista se puede editar utilizando los siguientes botones de control:

- ***Agregar***: abre el diálogo para la definición del nuevo conjunto de reglas de aplicación

- ***Editar*** : abre el diálogo para la edición de un conjunto de reglas de aplicación existente
- ***Eliminar*** : elimina la aplicación seleccionada de la lista
- ***Ayuda***: abre el archivo de ayuda relacionado con el diálogo activo

El diálogo para definir el nuevo conjunto de reglas de aplicación, se abre utilizando el botón ***Agregar*** del diálogo ***Aplicaciones*** dentro de la ***Configuración del Firewall***:



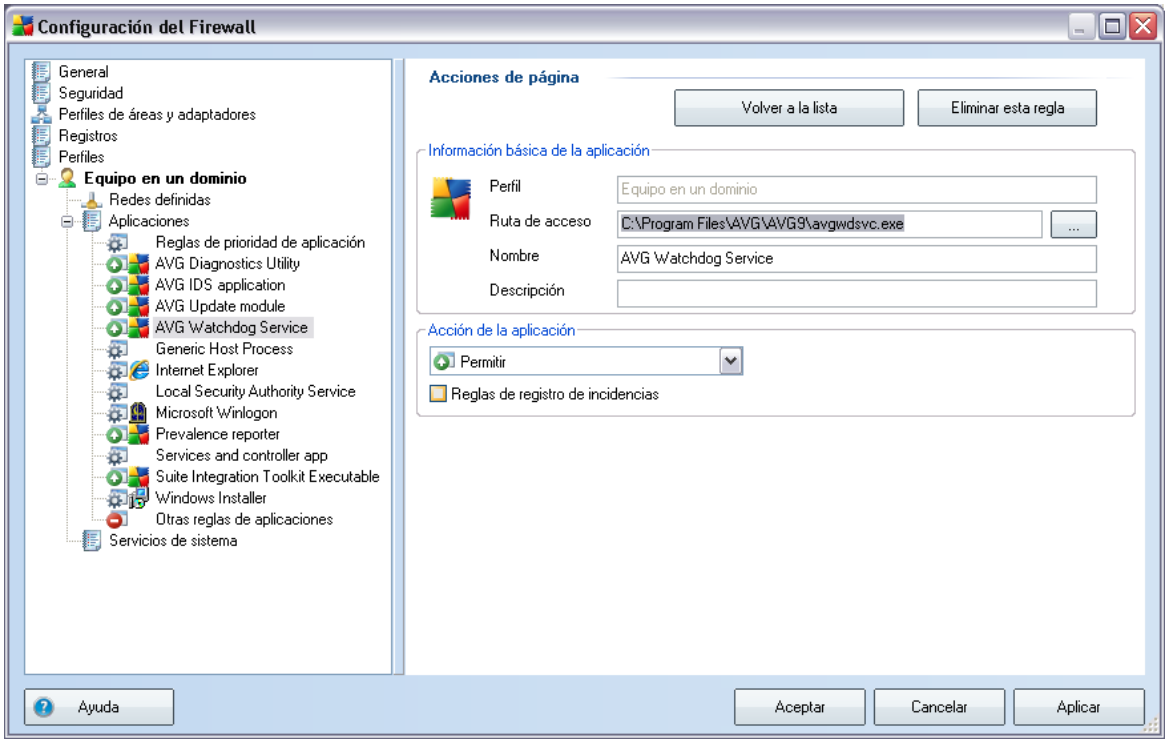
Dentro de este diálogo puede definir:

- ***La información básica de aplicación*** : nombre de la aplicación, una breve descripción y la ruta de acceso a su ubicación en el disco
- ***La acción de la aplicación*** : del menú desplegable seleccione una regla que se debe aplicar al comportamiento de la aplicación:
  - ***Programación avanzada:*** esta opción le permite editar el conjunto de

reglas en detalle en la parte inferior de este diálogo; *para obtener la descripción de esta sección, consulte el capítulo* ***Editar la aplicación***

- ***Permitir todo:*** se permitirá cualquier intento de comunicación de la aplicación
- ***Permitir seguras:*** sólo se permitirá que la aplicación se comunique a través de redes seguras (*por ejemplo, se permitirá la comunicación a la red protegida de la empresa mientras que la comunicación a Internet estará bloqueada*); para obtener una descripción general y la descripción de las redes seguras, consulte el diálogo ***Redes***
- ***Preguntar:*** siempre que la aplicación intente comunicarse a través de la red, se le preguntará si se debe permitir o bloquear esta comunicación
- ***Bloquear:*** se bloquearán todos los intentos de comunicación de la aplicación

El diálogo para editar un conjunto de reglas para una aplicación existente se abre mediante el botón ***Editar*** en el diálogo ***Aplicaciones*** dentro de ***Configuración del Firewall***:



Con este diálogo puede editar todos los parámetros de la aplicación:

- ***Información básica de la aplicación*** : nombre de la aplicación, su descripción corta y la ruta para su ubicación en el disco
- ***Acción de la aplicación*** : del menú desplegable, seleccione una regla que debe aplicarse al comportamiento de la aplicación:
  - ***Configuración avanzada:*** esta opción permite editar la regla establecida en los detalles de la parte inferior de este diálogo
  - ***Permitir todo***: se permitirán todos los intentos de comunicación de la aplicación
  - ***Permitir seguras:*** sólo se permitirá que la aplicación se comunique a través de redes seguras (*por ejemplo, se permitirá la comunicación a la red protegida de la empresa mientras que la comunicación a Internet estará bloqueada*); para obtener una descripción general y la descripción de las redes seguras, consulte el diálogo ***Redes***
  - ***Preguntar:*** siempre que la aplicación intente comunicarse a través de la

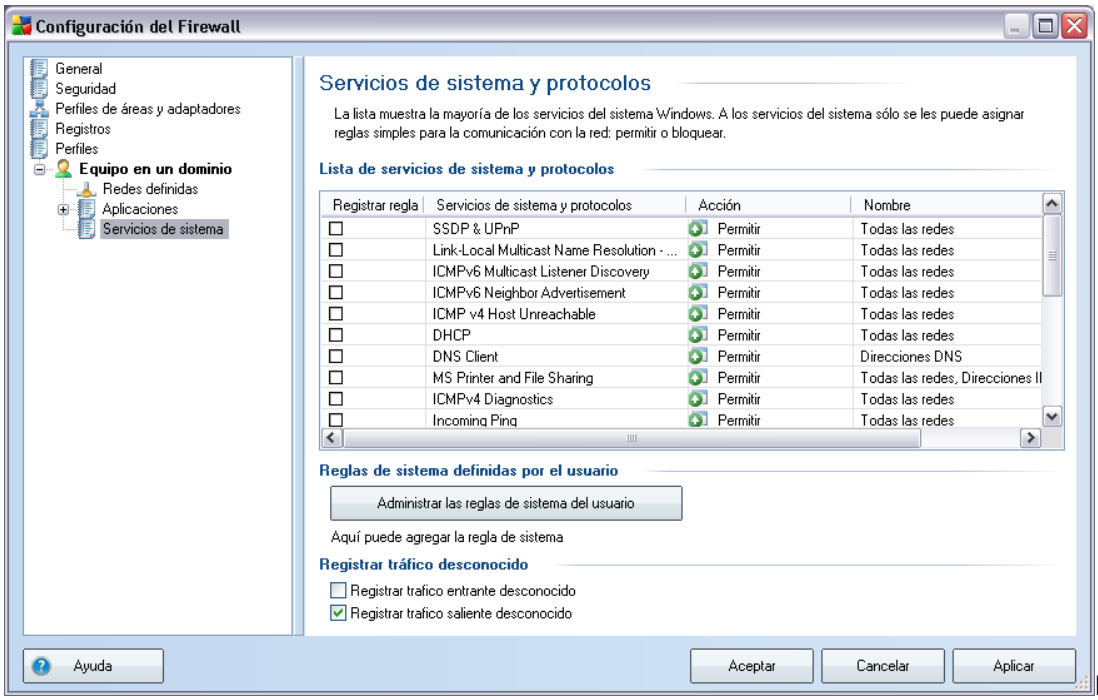
red, se le preguntará si se debe permitir o bloquear esta comunicación

- ***Bloquear:*** se bloquearán todos los intentos de comunicación de la aplicación

- ***Registrar las apariciones de las reglas*** : marque esta opción para confirmar que desea tener registradas todas las acciones del ***Firewall*** relacionadas con la aplicación que ha configurado para el conjunto de reglas. Las entradas de registro respectivas se pueden encontrar a continuación en el diálogo ***Registros***.

10.5.4. Servicios del sistema

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



El diálogo ***Servicios y protocolos de sistema*** abre una descripción general de los servicios de sistema y protocolos que se comunican a través de la red. Debajo de la lista puede encontrar dos opciones: marque o quite la marca para confirmar que desea registrar todo el tráfico desconocido en ambas direcciones (*entrante o saliente*).

Botones de control

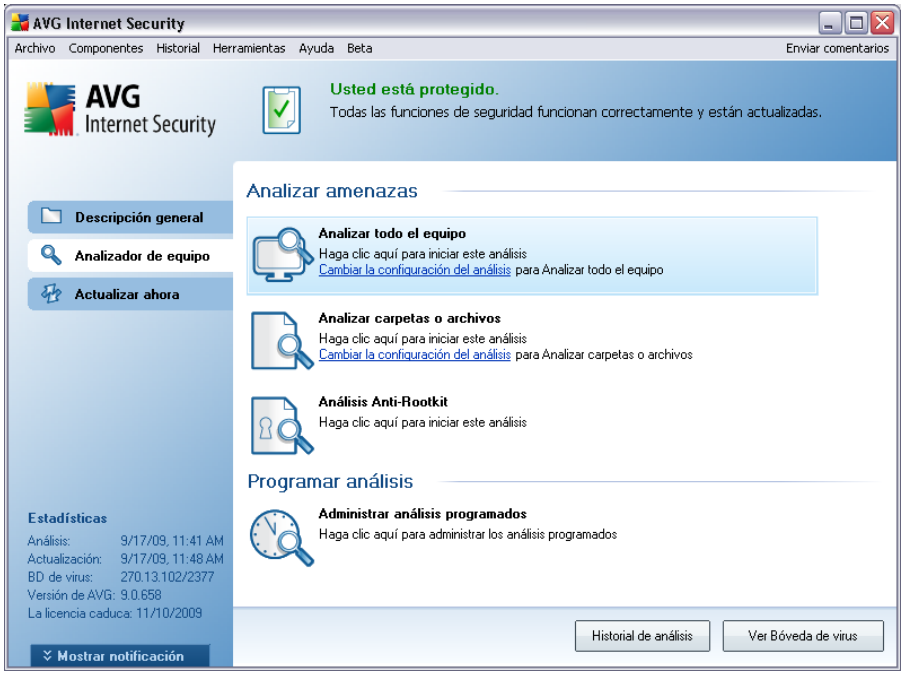
- ***Agregar/Editar*** : ambos botones bloquean el mismo diálogo, donde puede editar los parámetros de servicios del sistema. El botón ***Agregar*** abre un diálogo vacío y en el modo básico (*sin sección de configuración avanzada; sin embargo, puede abrir esta sección al seleccionar configuración avanzada para la acción de la aplicación*); el botón ***Editar*** abre el mismo diálogo con datos ya introducidos acerca del servicio de sistema seleccionado.

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

11. 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.

11.1. 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:

- Vista 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***
- 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.

11.2. 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.

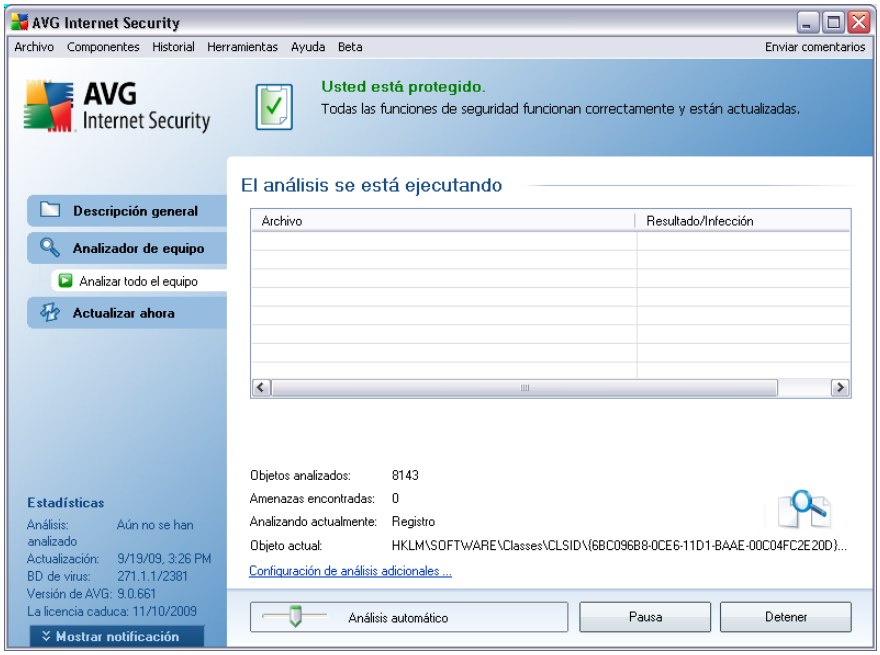
En el **Anti-Virus AVG 9 más Firewall** encontrará dos tipos de análisis predefinidos por el proveedor del software:

11.2.1. 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.

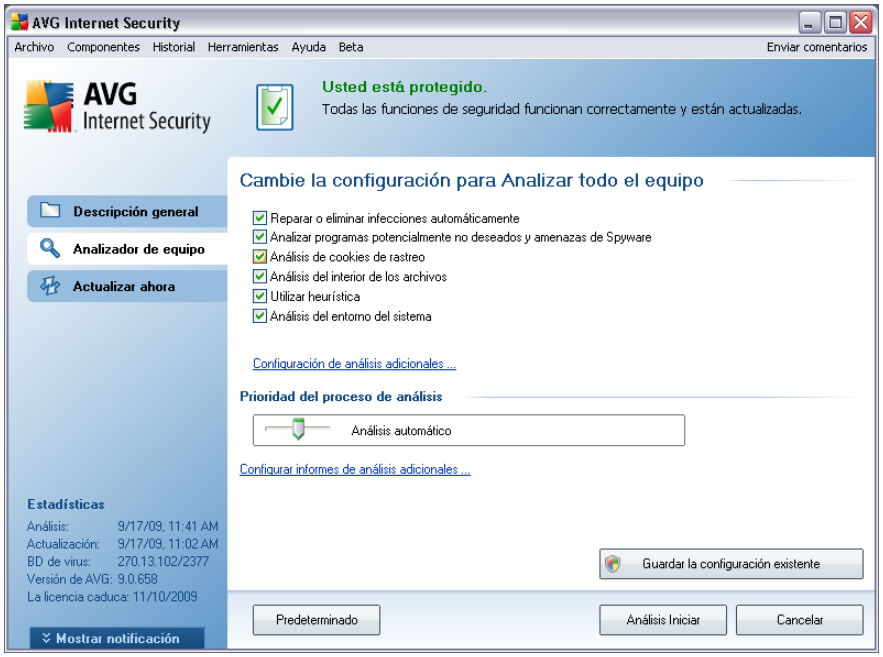
Ejecución de análisis

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 diálogo ***Se está ejecutando el análisis*** (*consulte la captura de pantalla*). El análisis puede interrumpirse temporalmente (***Pausa***) o se puede cancelar (***Detener***) si es necesario.



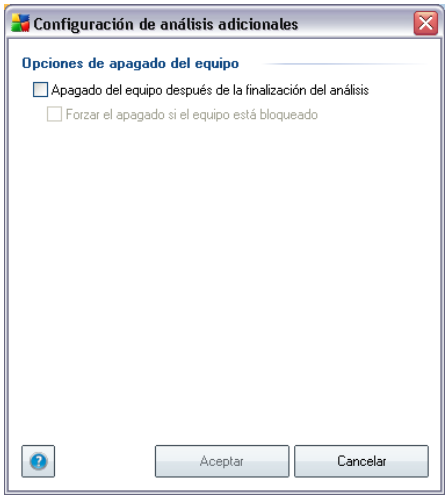
Edición de la configuración de análisis

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 diálogo ***Cambiar configuración del análisis de todo el equipo***. ***Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.***



- ***Configuración 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 diálogo nuevo de ***configuración de análisis adicional***, donde puede especificar los siguientes parámetros:



- ***Opciones de apagado del equipo***: decida si desea que el equipo se apague en forma automática una vez finalizado el proceso de análisis. Después de haber confirmado esta opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite al equipo apagarse 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 separadas por comas que no deben ser analizadas; o

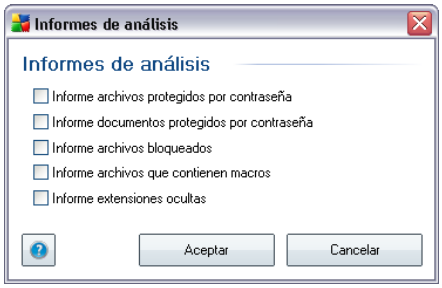
  - ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos infectables (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos de medios (*archivos 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 extensión***: 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* ***Analizar todo el equipo****, puede guardar la nueva configuración como la configuración predeterminada que se usará para todos los análisis de todo el equipo posteriores.*

11.2.2. Analizar carpetas o archivos específicos

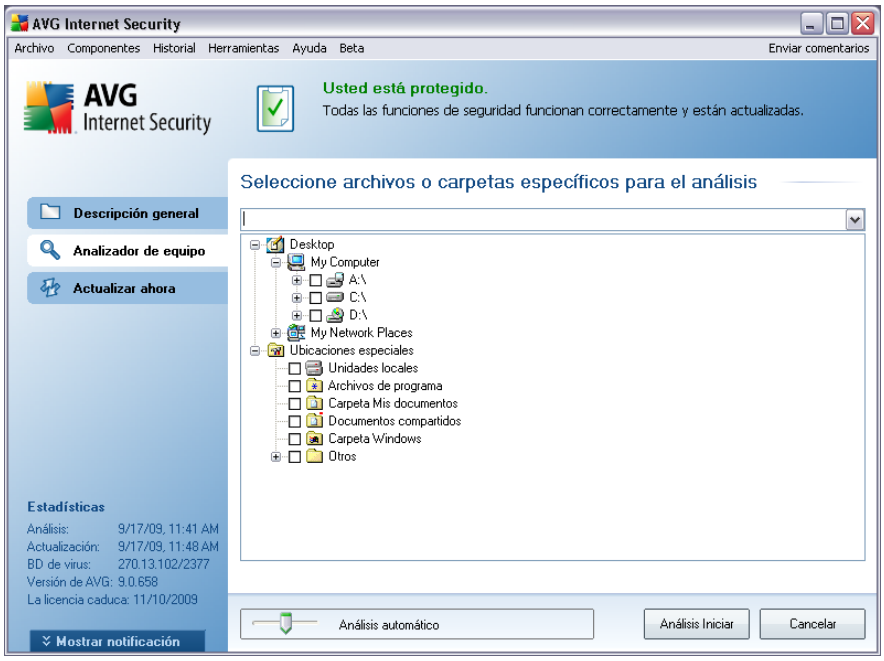
Analizar carpetas o archivos específicos: analiza únicamente las áreas del equipo que ha seleccionado que se analicen (carpetas, discos duros, discos flexibles, CD, etc.)). El procedimiento de análisis en caso de detección de virus y su tratamiento es el mismo que se realiza con el análisis de todo el 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.

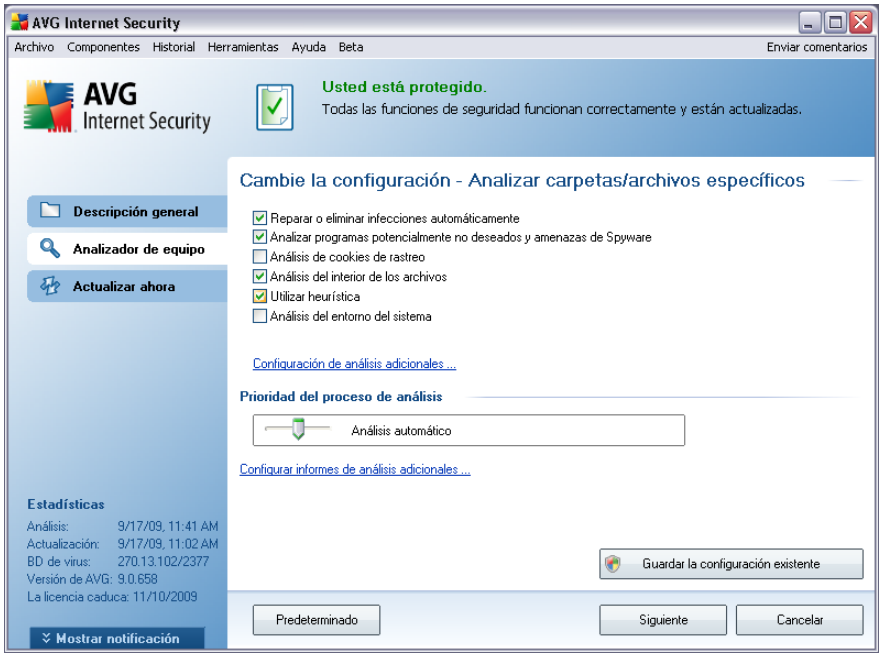
También existe la posibilidad de analizar una carpeta determinada y, a la vez, excluir de este análisis sus subcarpetas; para ello, escriba un signo menos "**-**" delante de la ruta generada automáticamente (*consulte la captura de pantalla*). Para excluir toda la carpeta del análisis utilice el signo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



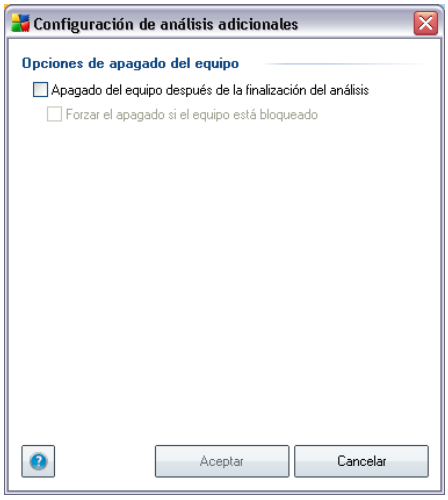
Edición de la configuración de análisis

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 cuadro de diálogo nuevo de configuración de análisis adicional, donde puede especificar los siguientes parámetros:



- ***Opciones de apagado del equipo***: decida si desea que el equipo se apague en forma automática una vez finalizado el proceso de análisis. Después de haber confirmado esta opción (***Apagado del equipo después de la finalización del análisis***), se activa una nueva opción, que permite al equipo apagarse 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 separadas por comas que no deben ser analizadas; o

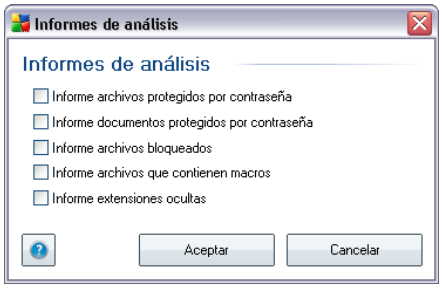
  - ***Los tipos de archivos seleccionados***: puede especificar que desea analizar sólo los tipos de archivos infectables (*los archivos que no pueden infectarse no se analizarán, por ejemplo, algunos archivos de texto sin formato u otros archivos no ejecutables*), incluyendo los archivos de medios (*archivos 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 extensión***: 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*).

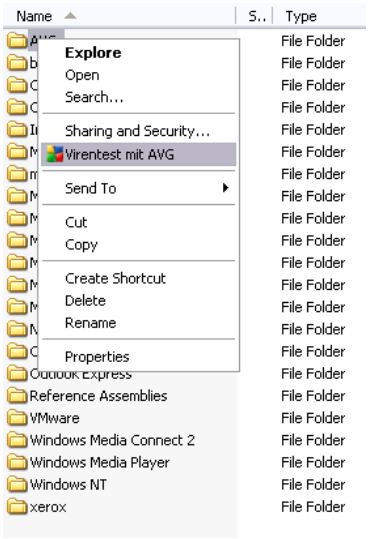
- ***Configurar informes de análisis adicionales***: el vínculo abre un nuevo diálogo de ***Informes de análisis***, donde puede seleccionar de qué tipos de posibles hallazgos se debería informar:



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 configuración 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).*

11.3. 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

11.4. Análisis de línea de comandos

En **Anti-Virus AVG 9 más Firewall** existe la opción de ejecutar 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 comas, por ejemplo: ***avgscanx /scan=C:\,D:***

Parámetros del análisis

Para mostrar una descripción completa de los parámetros disponibles, escriba el comando respetivo 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.

11.4.1. 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

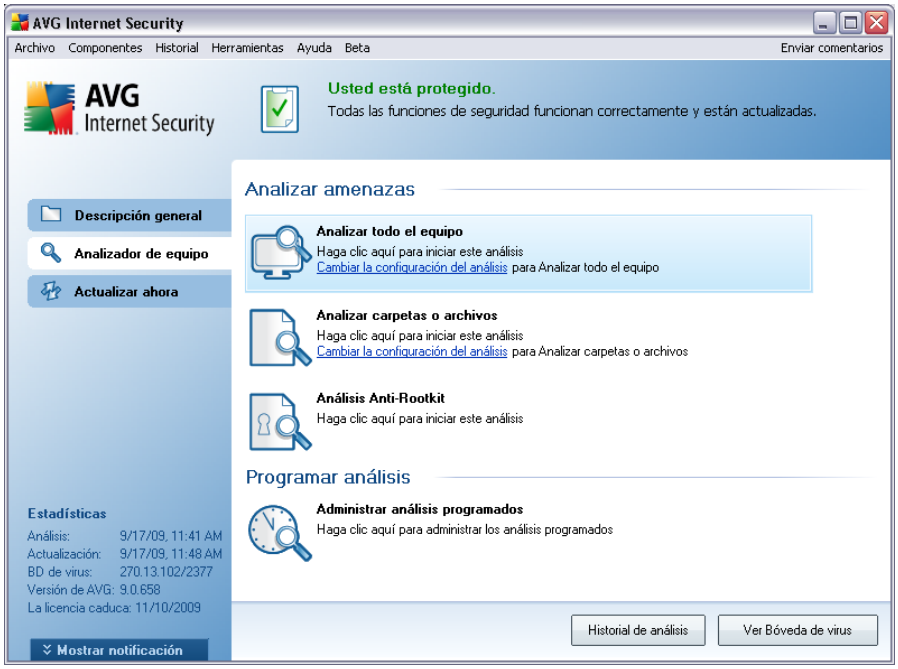
- ***/PUP*** Informar "Programas potencialmente no deseados"
- ***/REG*** Analizar registro
- ***/COO*** Analizar cookies
- ***/?*** Mostrar ayuda sobre este tema
- ***/HELP*** Visualizar ayuda sobre este tema
- ***/PRIORITY*** Establecer prioridad de análisis/Baja, Automática, Alta/ (consulte Configuración 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)

11.5. 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.

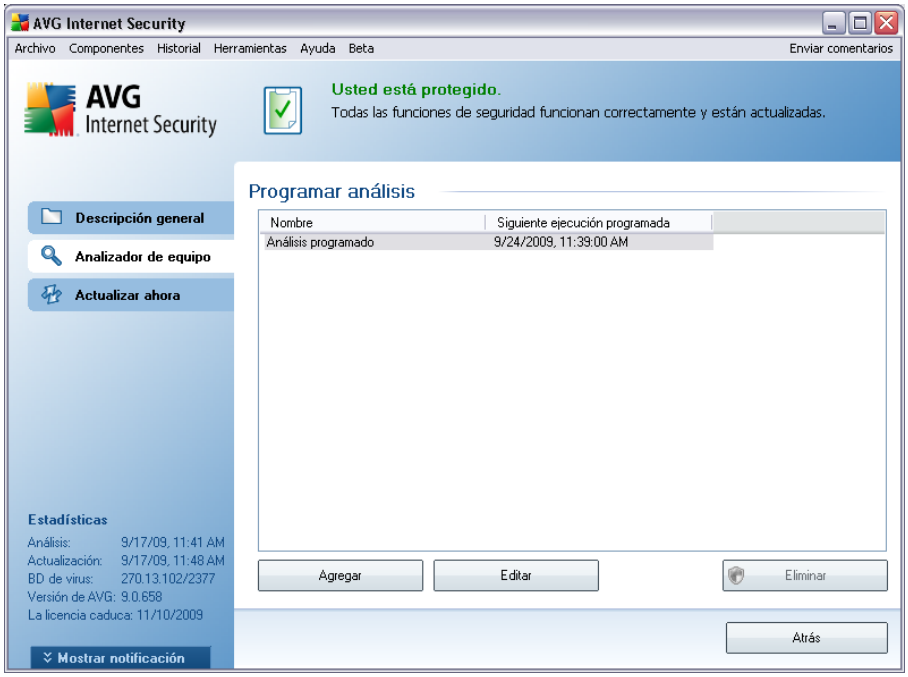
Se debe ejecutar el ***Análisis de todo el equipo*** periódicamente, al menos una vez a la semana. Sin embargo, si es posible, ejecute el análisis de todo su equipo diariamente, como está establecido en la configuración predeterminada de programación del análisis. Si el equipo siempre está encendido, 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.

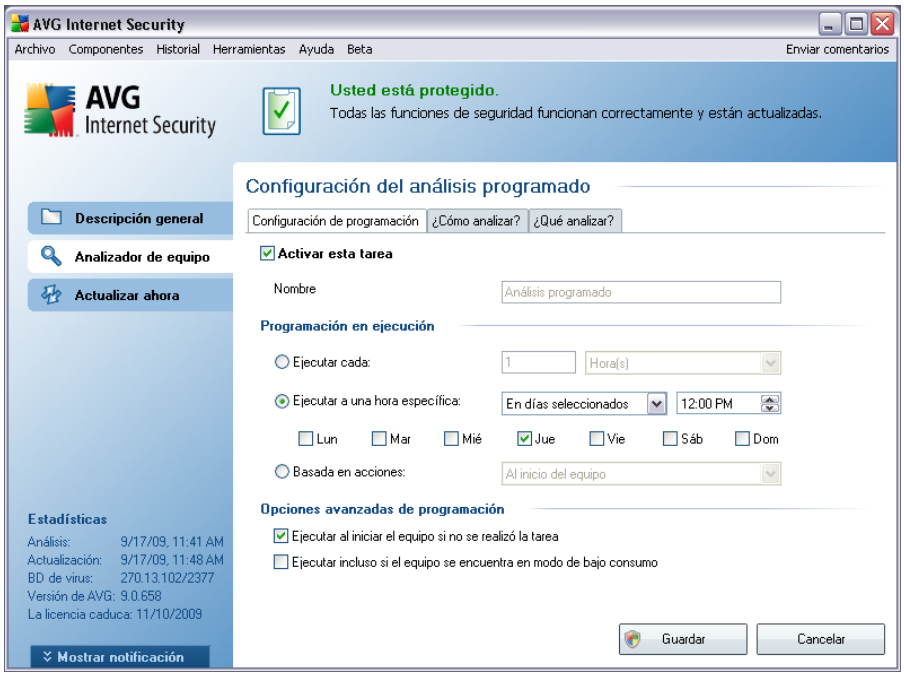
- ***Editar la programación de análisis***: este botón sólo se puede emplear si ha seleccionado previamente un análisis existente en la lista de análisis programados. En ese caso el botón aparece como activo y puede hacer clic en él para cambiar al diálogo ***Configuración del análisis programado***,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

11.5.1. 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 redirigirá 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.

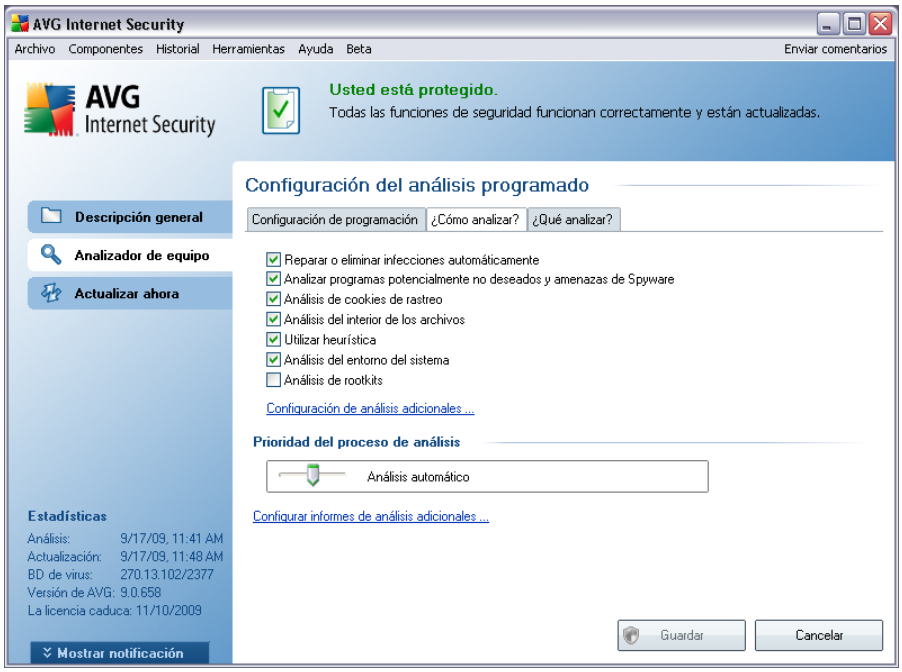
Botones de control del diálogo Configuración del análisis programado.

Hay dos botones de control en cada una de las tres pestañas del diálogo ***Configuración del análisis programado Configuración de programación***, ***¿Cómo analizar?*** ***y*** ***¿Qué analizar?***, y funcionan igual sin importar en qué pestaña se encuentre:

- ***Guardar***: guarda todos 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. 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.

11.5.2. 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***: *activado, de manera predeterminada*: si se identifica un virus durante el análisis, éste se puede reparar automáticamente si está disponible una vacuna. 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***: (*activado de forma predeterminada*): este parámetro controla la función ***antivirus*** que permite la detección de programas potencialmente no deseados (*archivos ejecutables que se pueden ejecutar como spyware o adware*) para su posterior bloqueo o eliminación;

- ***Analizar cookies de rastreo***: (*activado, de manera predeterminada*): este

parámetro del componente ***Anti-Spyware*** define qué cookies deben detectarse 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*);

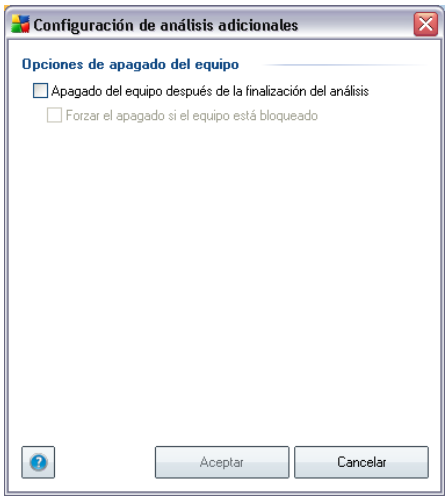
- ***Análisis del interior de los archivos*** (*activado, de manera predeterminada*): este parámetro defíne que el análisis debe comprobar todos los archivos, incluso aquellos que se encuentran comprimidos dentro de algún tipo de archivo, por ejemplo ZIP, RAR, ...

- ***Utilizar método heurístico*** (*activado, de manera predeterminada*): la emulación dinámica del análisis heurístico (*de las instrucciones del objeto analizado en 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*** en el cual puede especificar los siguientes parámetros:



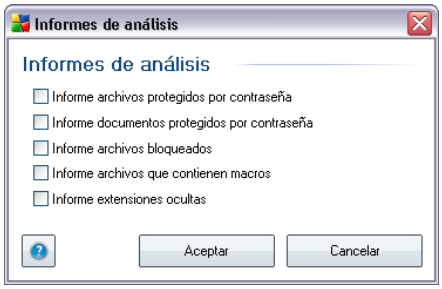
o ***Opciones de apagado del equipo***: decida si el equipo se debe apagar automáticamente una vez finalizado el proceso de ejecución del análisis. Después de haber confirmado esta opción (***Apagado del equipo***

después de la finalización del análisis), se activa una nueva opción, que permite al equipo apagarse aunque esté bloqueado (***Forzar el apagado si el equipo está bloqueado***).

- ***Defina los tipos de archivo para el análisis***: además debe decidir lo que desea que se analice:
  - ***Todos los tipos de archivos*** con la posibilidad de definir excepciones del análisis al proporcionar una lista de extensiones de archivo separadas por coma que no se deben analizar; o
  - ***Los tipos de archivos seleccionados***: puede especificar que sólo desea analizar los archivos que posiblemente se puedan infectar (*los archivos que no se pueden infectar no se analizarán, por ejemplo algunos archivos de texto sin formato, o algunos otros archivos no ejecutables*), incluidos los archivos multimedia (*archivos de video, audio; si deja estas casillas sin seleccionar, se reducirá el tiempo de análisis aún más, debido a que, con frecuencia, estos archivos son muy grandes y es poco probable que se infecten con un virus*). Nuevamente, puede especificar las extensiones de los archivos que siempre deben analizarse.
  - De forma opcional, puede decidir que desea ***Analizar archivos sin extensiones***: esta opción está activada de forma predeterminada, y se recomienda que la conserve así a menos que tenga una razón real para cambiarla. 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:



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*** *.*

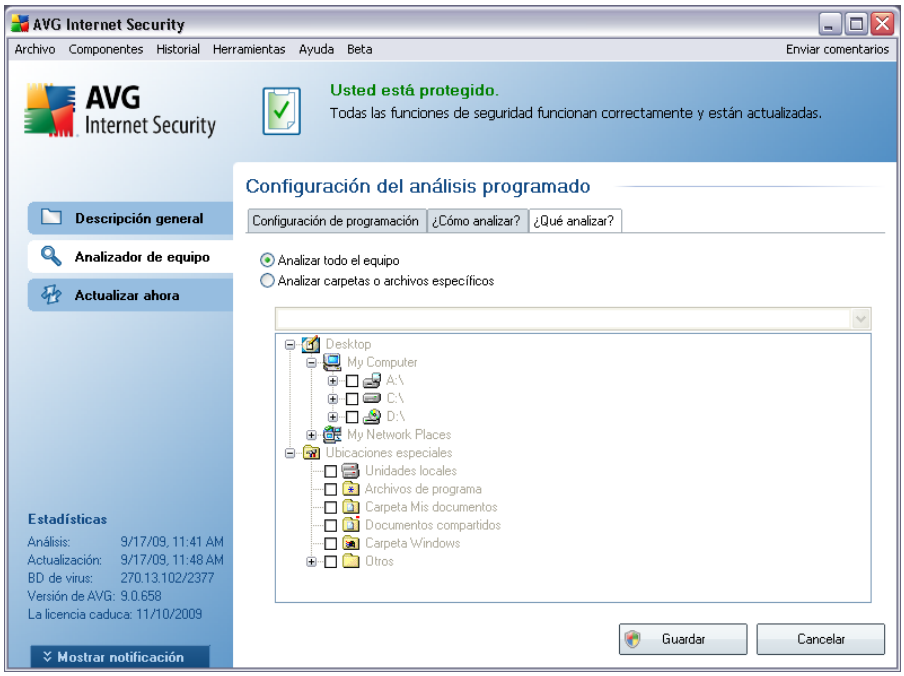
Botones de control

Hay dos botones de control en cada una de las tres pestañas del 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 diálogo y vuelve al 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.

11.5.3. 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 diálogo se activará la estructura de árbol visualizada y podrá especificar las carpetas que se analizarán.

Botones de control del diálogo Configuración del análisis programado.

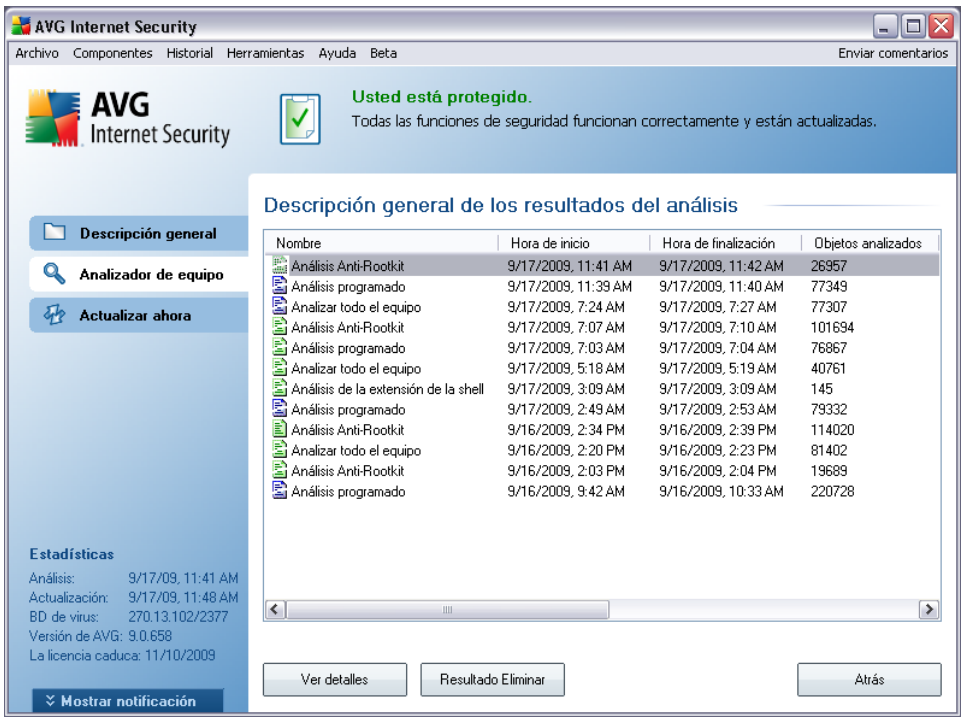
Hay dos botones de control en cada una de las tres pestañas del diálogo ***Configuración del análisis programado*** ***Configuración de programación***, ***Cómo analizar*** *y* Qué analizar y tienen el mismo funcionamiento sin importar en cuál pestaña se encuentre:

- ***Guardar***: guarda todos los cambios efectuados en esta pestaña o en cualquier otra pestaña de este diálogo y vuelve al 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.

11.6. 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 informa que durante el análisis no se detectó ninguna infección

  - el icono azul anuncia que durante el análisis se detectó una infección, pero que el objeto infectado se eliminó automáticamente.

  - el icono rojo advierte 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
- ***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*** : este botón solo está activo si se selecciona un análisis específico en la descripción general anterior; presiónelo para cambiar al diálogo ***Resultados del análisis*** y ver los datos detallados sobre el análisis seleccionado
- ***Eliminar resultado***: este botón sólo está activo si se selecciona un análisis específico en la descripción general anterior; presiónelo para eliminar el elemento seleccionado de la descripción general de resultados
- ***Atrás***: regresa al diálogo predeterminado de la interfaz de análisis de AVG

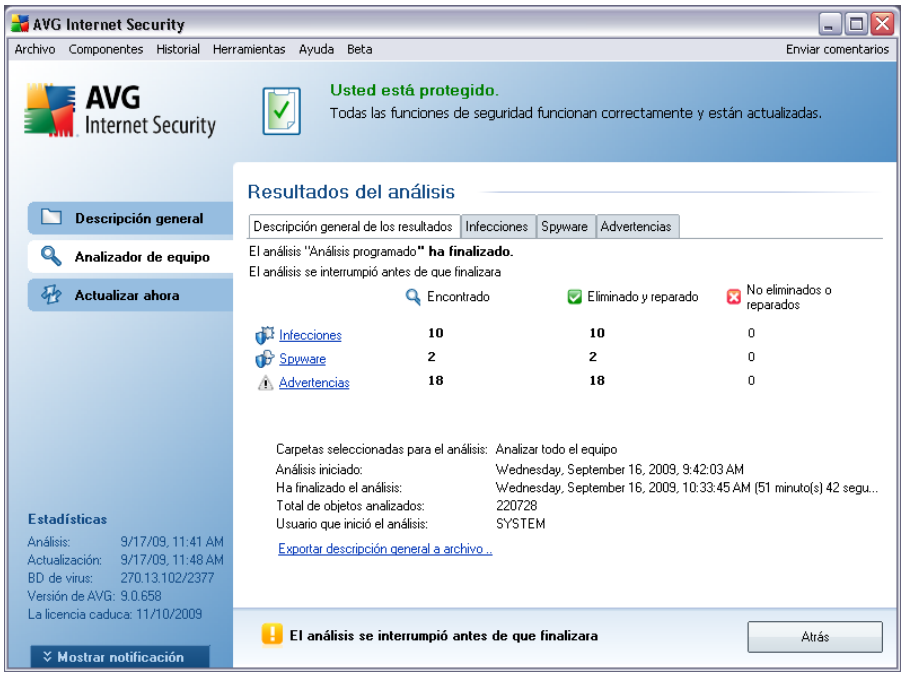
11.7. Detalles de los resultados del análisis

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 visualiza sólo si durante el análisis se detectaron algunos objetos que no se pudieron analizar.
- ***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.

11.7.1. Pestaña Descripción general de los resultados



En la pestaña ***Resultados del análisis*** puede consultar estadísticas detalladas con información sobre:

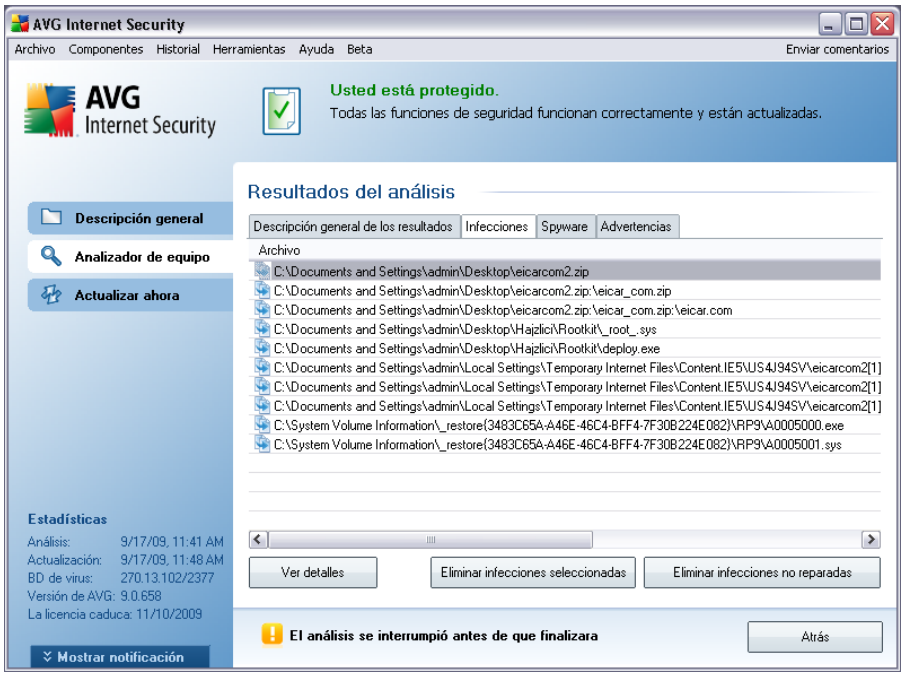
- Infecciones de virus/spyware detectadas
- Infecciones de virus/spyware eliminadas
- Infecciones de virus/spyware que no se han podido eliminar ni reparar

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***.

11.7.2. 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:

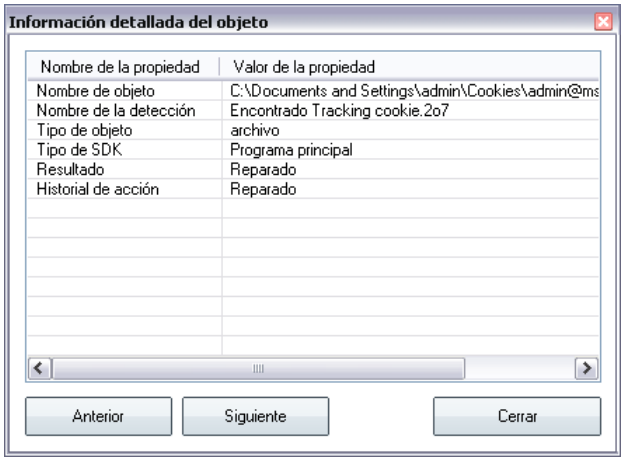
- ***Archivo***: ruta completa de la ubicación original del objeto infectado.
- ***Infecciones***: nombre del virus detectado (*para obtener detalles sobre virus específicos, consulte la Enciclopedia de Virus en línea*).
- ***Resultado***: define el estado actual del objeto infectado detectado durante 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***.

11.7.3. 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.

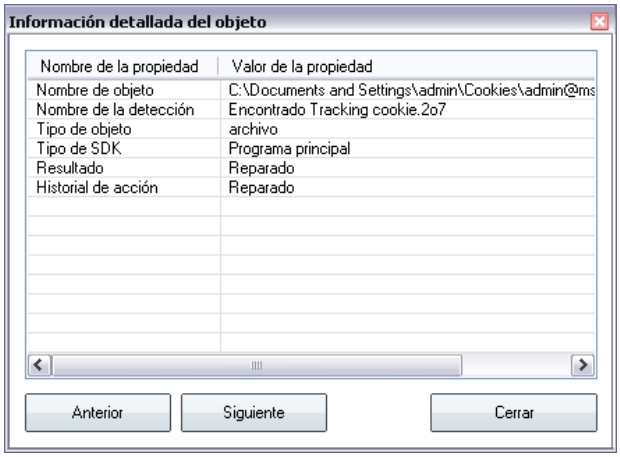
- ***Objeto potencialmente peligroso***: el objeto se ha detectado como potencialmente peligroso pero no infectado (por ejemplo, puede contener macros); la información es solo una advertencia.

- ***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.***

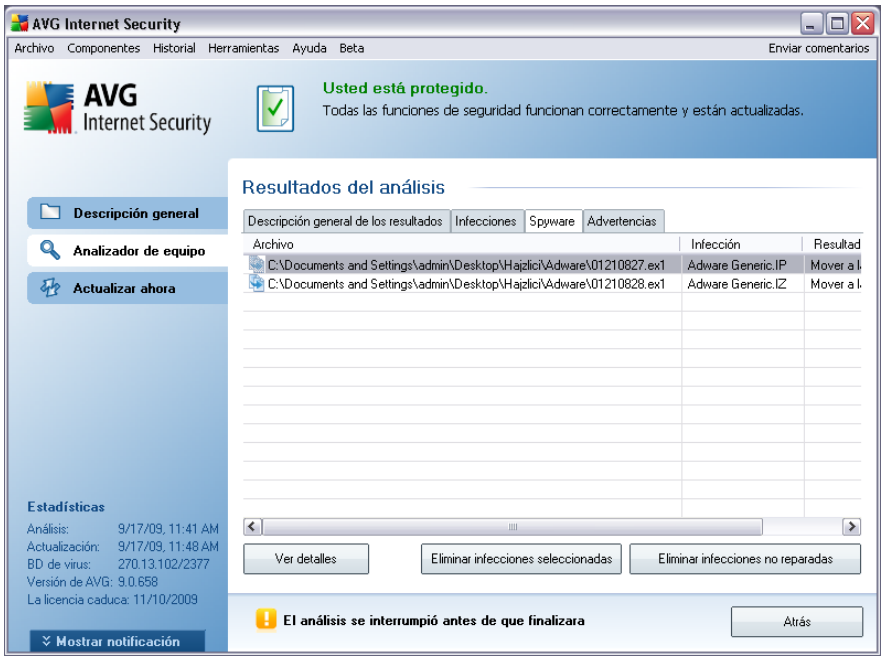
- ***Eliminar todas las infecciones sin reparar***: este botón elimina todos los hallazgos que no se pueden reparar o mover a la ***Bóveda de Virus.***

- ***Cerrar resultados***: termina la vista general de información detallada y permite volver al diálogo ***Descripción general de los resultados del***

análisis.

11.7.4. 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 alguna 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.

11.7.5. 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.

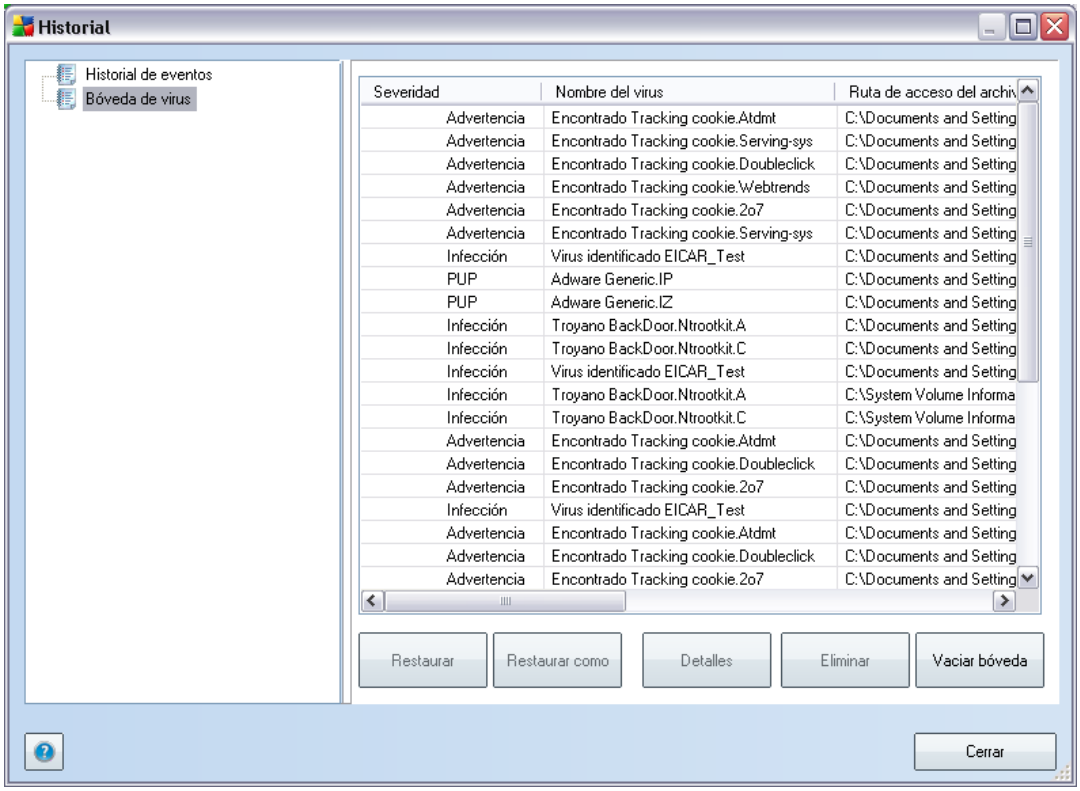
- ***Extensión oculta***: los archivos con la extensión oculta pueden aparentar que son, por ejemplo, imágenes, pero en realidad son archivos ejecutables (*por ejemplo, imagen.jpg.exe*). La segunda extensión no es visible en Windows de forma predeterminada, y AVG reporta estos archivos para prevenir 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*).

11.8. 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.

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***: proporciona identificación gráfica de la severidad de los hallazgos en una escala de cuatro niveles que van desde inobjetable (■□□□) hasta muy

peligroso (■■■■)

- ***Tipo de infección***: distingue los tipos de hallazgos según el nivel de infección (*todos los objetos de la lista pueden estar positivamente 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.

- ***Eliminar***: elimina el archivo infectado de la ***Bóveda de Virus*** por completo.

- ***Vaciar Bóveda de Virus*** - elimina todo el contenido de la ***Bóveda de Virus*** permanentemente

12. Actualizaciones de AVG

Mantener AVG actualizado es crucial para asegurar que todos los virus recién descubiertos se detecten tan pronto sea posible. Debido a que las actualizaciones de AVG no se liberan 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 su base de virus de AVG esté actualizada durante el día.

12.1. Niveles de actualización

AVG permite seleccionar dos niveles de actualización:

- ***Actualización de definiciones*** contiene los cambios necesarios para una protección antivirus, 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.

12.2. 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.

12.3. Proceso de actualización

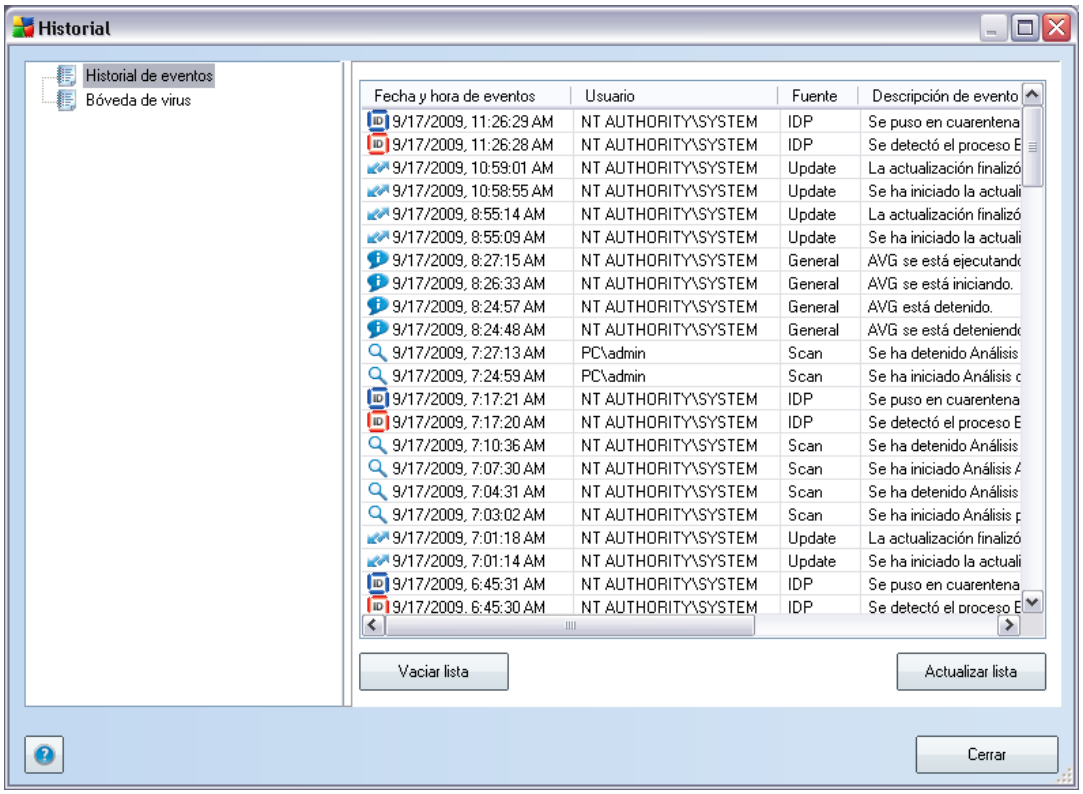
El proceso de actualización se puede iniciar inmediatamente cuando se necesite, mediante el vínculo rápido ***Actualizar ahora***. Este vínculo está disponible en todo momento desde cualquier diálogo de la Interfaz del usuario de AVG . Sin embargo, es altamente recomendable llevar a cabo las actualizaciones 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 el progreso del proceso en su representación gráfica, así como en una descripción general de los parámetros estadísticos relevantes (*tamaño del archivo actualizado, datos recibidos, velocidad de descarga, tiempo transcurrido, ...*).

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. Se puede tener acceso a esta opción a través de Inicio/Todos los programas/ Accesorios/Herramientas del sistema/ Restaurar sistema. ¡Recomendado sólo para usuarios avanzados!*

13. 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.

14. 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 departamento 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***.