

# Anti-Virus AVG 8.5

## Manual del usuario

### Revisión del documento 85.1 (26.1.2009)

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.

## Contenidos

<b>1. Introducción</b>	<b>7</b>
<b>2. Requisitos de instalación de AVG</b>	<b>8</b>
2.1 Sistemas de operación compatibles	8
2.2 Requerimientos mínimos de hardware	8
<b>3. Opciones de instalación de AVG</b>	<b>9</b>
<b>4. Administrador de descargas de AVG</b>	<b>10</b>
4.1 Selección del idioma	10
4.2 Verificación de conectividad	10
4.3 Configuración proxy	13
4.4 Seleccionar tipo de licencia	14
4.5 Descargar archivos para instalar	15
<b>5. Proceso de instalación de AVG</b>	<b>16</b>
5.1 Ejecución de la instalación	16
5.2 Contrato de licencia	17
5.3 Verificando el estado del sistema	18
5.4 Seleccionar el tipo de instalación	19
5.5 Activar su licencia AVG	19
5.6 Instalación personalizada: carpeta de destino	21
5.7 Instalación personalizada: selección del componente	22
5.8 Barra de herramientas AVG Security	23
5.9 Resumen de la instalación	24
5.10 Finalización de aplicación	24
5.11 Instalando	25
5.12 Se completó la instalación	26
<b>6. Asistente para la ejecución inicial de AVG</b>	<b>27</b>
6.1 Introducción del Asistente para la ejecución inicial de AVG	27
6.2 Programar análisis y actualizaciones automáticas	28
6.3 Ayúdenos a identificar nuevas amenazas en línea	28
6.4 Configurar la Barra de herramientas AVG Security	29
6.5 Actualizar protección AVG	30
6.6 Configuración de AVG finalizada	30

<b>7. Después de la instalación .....</b>	<b>32</b>
7.1 Registro del producto .....	32
7.2 Acceso a la interfaz de usuario .....	32
7.3 Análisis de todo el equipo .....	32
7.4 Análisis Eicar .....	32
7.5 Configuración predeterminada de AVG .....	33
<b>8. Interfaz del usuario de AVG .....</b>	<b>34</b>
8.1 Menú del sistema .....	35
8.1.1 Archivo .....	35
8.1.2 Componentes .....	35
8.1.3 Historial .....	35
8.1.4 Herramientas .....	35
8.1.5 Ayuda .....	35
8.2 Información del estado de seguridad .....	38
8.3 Vínculos rápidos .....	39
8.4 Descripción general de los componentes .....	40
8.5 Estadísticas .....	42
8.6 Icono en la bandeja de sistema .....	42
<b>9. Componentes de AVG .....</b>	<b>44</b>
9.1 Antivirus .....	44
9.1.1 Antivirus Principios de .....	44
9.1.2 Interfaz de Antivirus .....	44
9.2 Anti-Spyware .....	46
9.2.1 Anti-Spyware Principios de .....	46
9.2.2 Interfaz de Anti-Spyware .....	46
9.3 Anti-Rootkit .....	48
9.3.1 Principios de Anti-Rootkit .....	48
9.3.2 Interfaz de Anti-Rootkit .....	48
9.4 Licencia .....	50
9.5 Link Scanner .....	51
9.5.1 Principios de Link Scanner .....	51
9.5.2 Interfaz de Link Scanner .....	51
9.5.3 Protección de búsqueda AVG .....	51
9.5.4 Protección de navegación activa AVG .....	51
9.6 Web Shield .....	55
9.6.1 Principios de Web Shield .....	55

9.6.2	<i>Interfaz de Web Shield</i>	55
9.6.3	<i>Detección de Web Shield</i>	55
9.7	Protección residente	59
9.7.1	<i>Protección residente Principios de</i>	59
9.7.2	<i>Interfaz de protección residente</i>	59
9.7.3	<i>Detección de protección residente</i>	59
9.8	Administrador de actualización	63
9.8.1	<i>Principios de administrador de actualización</i>	63
9.8.2	<i>Interfaz de administrador de actualización</i>	63
9.9	Barra de herramientas AVG Security	65
<b>10.</b>	<b>Protección de Identidad</b>	<b>69</b>
10.1	Principios de Protección de Identidad	69
10.2	Interface de Protección de Identidad	69
<b>11.</b>	<b>Configuración avanzada de AVG</b>	<b>70</b>
11.1	Apariencia	70
11.2	Ignorar condiciones de falla	73
11.3	Bóveda de Virus	74
11.4	Excepciones de PPND	75
11.5	Web Shield	77
11.5.1	<i>Protección Web</i>	77
11.5.2	<i>Mensajería instantánea</i>	77
11.6	Link Scanner	81
11.7	Análisis	82
11.7.1	<i>Analizar todo el equipo</i>	82
11.7.2	<i>Análisis de extensión de la shell</i>	82
11.7.3	<i>Analizar carpetas o archivos específicos</i>	82
11.7.4	<i>Análisis de dispositivos extraíbles</i>	82
11.8	Programaciones	89
11.8.1	<i>Análisis programado</i>	89
11.8.2	<i>Programación de actualización de la base de datos de virus</i>	89
11.8.3	<i>Programación de actualización del programa</i>	89
11.8.4	<i>Programación de actualización de Anti-Spam</i>	89
11.9	Analizador de correos electrónicos	100
11.9.1	<i>Certificación</i>	100
11.9.2	<i>Filtro de correos electrónicos</i>	100
11.9.3	<i>Registros y resultados</i>	100

11.9.4 Servidores .....	100
11.10 Protección residente .....	108
11.10.1 Configuración avanzada .....	108
11.10.2 Excepciones .....	108
11.11 Anti-Rootkit .....	111
11.12 Actualización .....	112
11.12.1 Proxy .....	112
11.12.2 Conexión telefónica .....	112
11.12.3 URL .....	112
11.12.4 Administrar .....	112
<b>12. Análisis de AVG .....</b>	<b>119</b>
12.1 Interfaz de análisis .....	119
12.2 Análisis predefinidos .....	120
12.2.1 Analizar todo el equipo .....	120
12.2.2 Analizar carpetas o archivos específicos .....	120
12.3 Análisis en el Explorador de Windows .....	126
12.4 Análisis de línea de comandos .....	127
12.4.1 Parámetros del análisis de CMD .....	127
12.5 Programación de análisis .....	130
12.5.1 Configuración de programación .....	130
12.5.2 Cómo analizar .....	130
12.5.3 Qué analizar .....	130
12.6 Descripción general de los resultados del análisis .....	137
12.7 Detalles de los resultados del análisis .....	139
12.7.1 Pestaña Descripción general de los resultados .....	139
12.7.2 Pestaña Infecciones .....	139
12.7.3 Pestaña Spyware .....	139
12.7.4 Pestaña Advertencias .....	139
12.7.5 Pestaña Rootkits .....	139
12.7.6 Pestaña Información .....	139
12.8 Bóveda de virus .....	146
<b>13. Actualizaciones de AVG .....</b>	<b>148</b>
13.1 Niveles de actualización .....	148
13.2 Tipos de actualización .....	148
13.3 Proceso de actualización .....	148
<b>14. Historial de eventos .....</b>	<b>150</b>

**15. Preguntas frecuentes y soporte técnico ..... 152**

## 1. Introducción

Este manual del usuario proporciona documentación exhaustiva para **Anti-Virus AVG 8.5**

### **Enhorabuena por la compra de Anti-Virus AVG 8.5.**

**Anti-Virus AVG 8.5** 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 8.5** 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 8.5** 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 8.5** 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)

(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 8.5**:

- Equipo Intel Pentium de 1.2 GHz
- 70 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 último archivo de instalación del [sitio web de AVG](http://www.avg.com) ([www.avg.com](http://www.avg.com)).

**Antes de comenzar a instalar AVG, le recomendamos que visite el [sitio Web de AVG](http://www.avg.com) para verificar si existe algún archivo de instalación nuevo. Así, puede asegurarse de que estará instalando la última versión disponible de Anti-Virus AVG 8.5.**

**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

**AVG Download Manager** 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, **AVG Download Manager** procederá a descargar e iniciar el [proceso de instalación](#) adecuado.

A continuación encontrará una breve descripción de cada paso que necesita realizar dentro del **AVG Download Manager**:

### 4.1. Selección del idioma



En el primer paso de **AVG Download Manager** 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, **AVG Download Manager** intentará establecer una conexión a Internet para localizar las actualizaciones. No podrá continuar con el proceso de descarga hasta que **AVG Download Manager** 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 **AVG Download Manager** 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 **AVG Download Manager**.

#### 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 **AVG Download Manager** inicie la descarga del paquete de instalación e inicie el proceso de instalación. A continuación, avance hacia el [proceso de instalación de AVG](#).

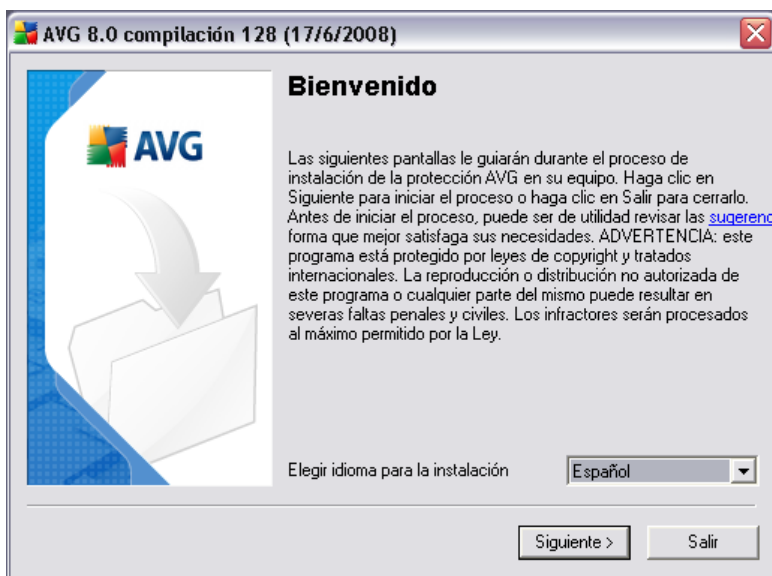
## 5. Proceso de instalación de AVG

Para instalar AVG en su equipo, necesita obtener el archivo de instalación más reciente. Puede utilizar el CD de instalación que forma parte de su edición en caja, pero este archivo puede no estar actualizado.

Por lo tanto, recomendamos obtener el archivo de instalación más reciente en línea. Puede descargar el archivo del [sitio web de AVG](http://www.avg.com) (en [www.avg.com](http://www.avg.com)) / sección **Descargas** O, puede utilizar nuestra nueva herramienta [AVG Download Manager](#) que 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



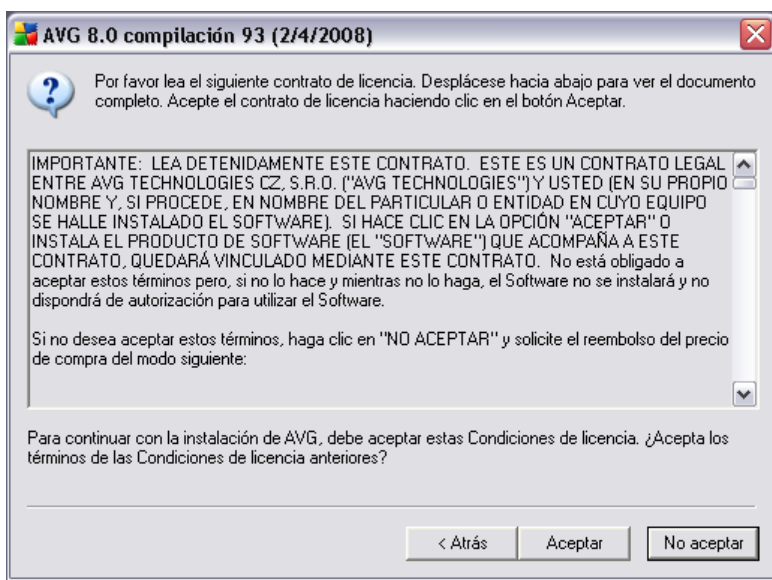
El proceso de instalación inicia con la ventana **Bienvenido al programa de instalación de AVG**. Aquí se selecciona el idioma empleado para el proceso de instalación. En la parte inferior de la ventana del diálogo, busque el elemento **Elegir idioma para la instalación** y seleccione el idioma deseado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



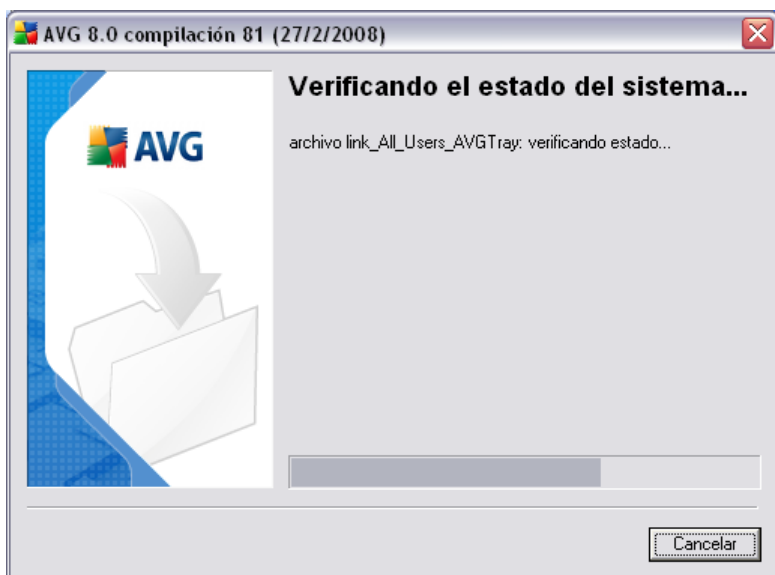
selecciona el idioma de la aplicación AVG, que se puede especificar más adelante en el proceso de instalación.

## 5.2. Contrato de licencia



El diálogo **Contrato de licencia** muestra íntegramente el contrato de licencia de AVG. Léalo con atención y confirme que lo ha leído, lo entiende y lo acepta 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/venta en el campo de texto **Número de licencia/venta**. El número de venta se puede encontrar en el empaquetado del CD en la caja del AVG. El número de licencia se encuentra en el correo electrónico de confirmación que recibió después de la compra en línea de su AVG. Debe escribir el

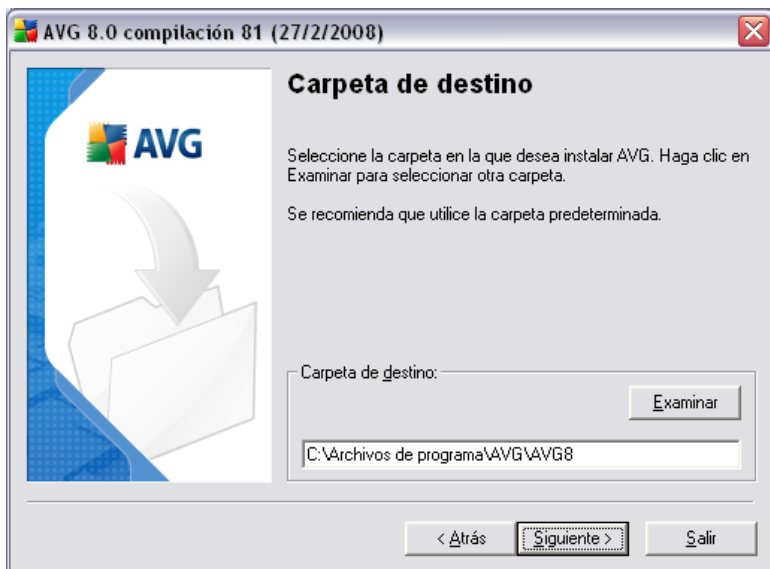
número exactamente como se muestra. Si está disponible el formulario digital del número de licencia (en el correo electrónico), se recomienda utilizar el método de copiar y pegar para insertarlo.



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

Si en el paso anterior seleccionó la instalación estándar, se le enviará directamente al diálogo [Resumen de la instalación](#) . 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 AVG. De modo predeterminado, AVG se instalará en la carpeta de archivos de programa de la unidad C:.. 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 AVG que se pueden instalar. Si la configuración predeterminada no se adecua a sus necesidades, puede quitar/agregar componentes específicos.

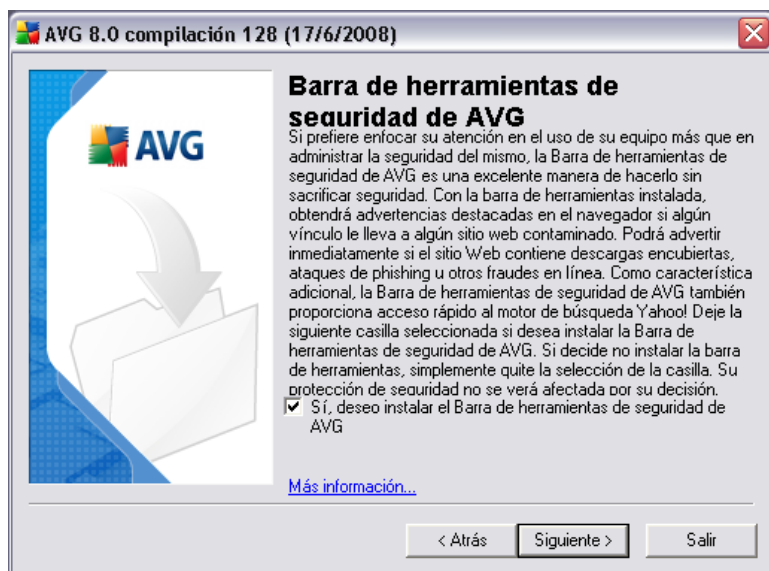
**Sin embargo, sólo puede seleccionar de entre los componentes incluidos en la edición del AVG que compró. Sólo se ofrecerá instalar estos componentes en el diálogo Selección de componentes.**

Dentro de la lista de componentes a instalar, puede definir el idioma (s) en que se instalará AVG. Marque el elemento **Otros idiomas instalados** y después seleccione los idiomas deseados del menú respectivo.

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.

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

## 5.8. Barra de herramientas AVG Security



En el diálogo de la **Barra de herramientas AVG Security**, decida si desea instalar la **Barra de herramientas AVG Security**; si no cambia la configuración predeterminada, este componente se instalará de forma automática en su navegador de Internet, en conjunto con las tecnologías AVG 8.0 y AVG XPL para proporcionarle una protección en línea exhaustiva mientras navega por Internet.

## 5.9. Resumen de la instalación



El diálogo **Resumen de la instalación** ofrece una descripción general de todos los parámetros del proceso de instalación. Compruebe que toda la información es correcta. En ese caso, presione el botón **Finalizar** para continuar. De lo contrario, puede emplear el botón **Atrás** para volver al diálogo correspondiente y corregir la información.

## 5.10. Finalización de aplicación

Antes de iniciar el proceso de instalación, se le solicitará finalizar algunas de las aplicaciones en ejecución que pueden interferir en el proceso de instalación de AVG. En dicho caso, verá el siguiente diálogo de **Finalización de aplicación**. Este diálogo es sólo informativo y no requiere ninguna intervención; si está de acuerdo en cerrar los programas enumerados de forma automática, presione **Siguiente** para continuar:

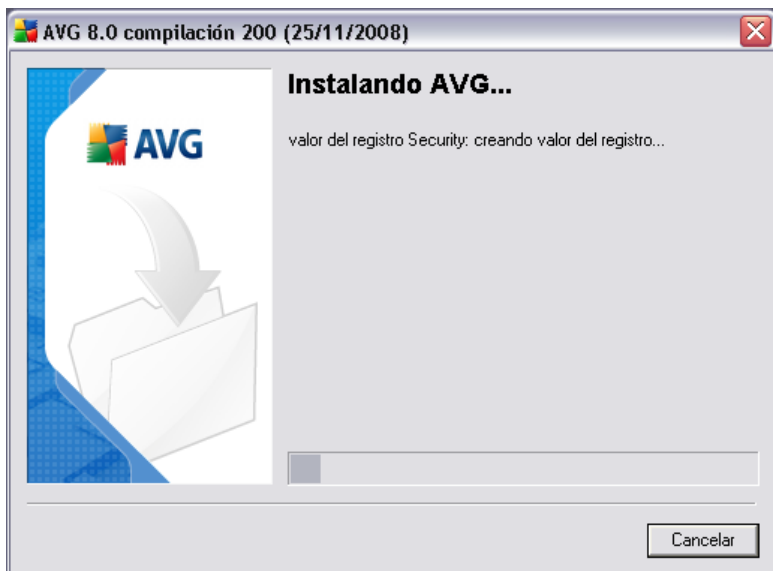




**Nota:** Asegúrese de haber guardado toda la información antes de confirmar el cierre de las aplicaciones en ejecución.

### 5.11. Instalando

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



Espera a que finalice la instalación; posteriormente será redirigido al diálogo [Se completó la instalación](#).

## 5.12. Se completó la instalación



El diálogo ***¡La instalación ha finalizado!*** es el paso final del proceso de instalación de AVG. El AVG ahora está instalado en su equipo y completamente funcional. El programa se está ejecutando en segundo plano de modo totalmente automático.

Después de la instalación, el [Asistente de configuración básica del AVG](#) se ejecutará automáticamente y en unos cuantos pasos lo guiará a través de la configuración básica de **Anti-Virus AVG 8.5**. A pesar del hecho de que la configuración del AVG está accesible en cualquier momento durante la ejecución del AVG, recomendamos encarecidamente que utilice esta opción e instale la configuración básica con la ayuda del asistente.

## 6. Asistente para la ejecución inicial de AVG

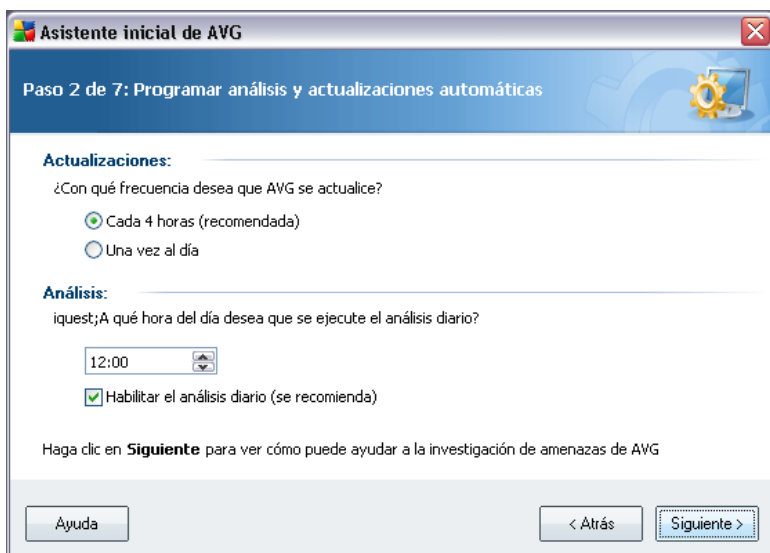
La primera vez que instale AVG en su equipo, aparecerá el **Asistente para la configuración básica de AVG** para ayudarle con la configuración **Anti-Virus AVG 8.5** inicial del programa. Si bien puede definir todos los parámetros sugeridos más adelante, se recomienda que realice el recorrido propuesto por el asistente para garantizar la protección anti-virus de su equipo de manera sencilla e inmediata. Realice los pasos descritos en cada una de las ventanas del asistente:

### 6.1. Introducción del Asistente para la ejecución inicial de AVG



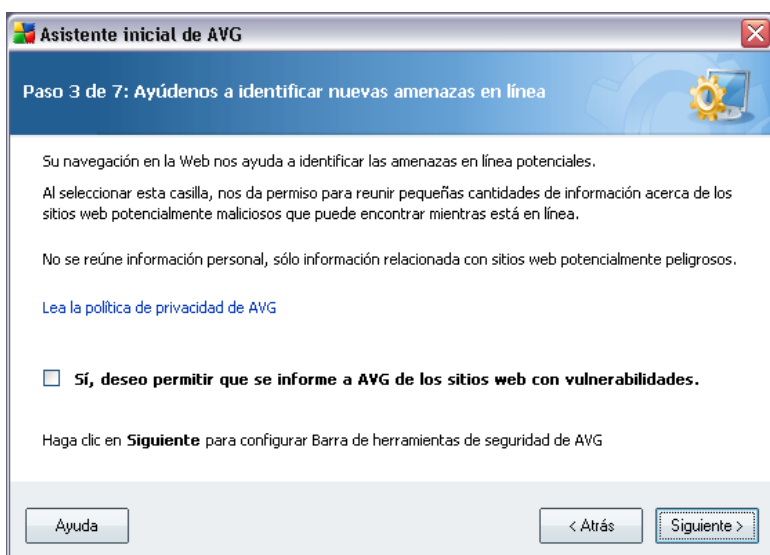
La ventana de bienvenida de **Presentación del Asistente para la ejecución inicial de AVG** resume brevemente el estado de AVG en su equipo y sugiere los pasos que se deben tomar para completar la protección. Haga clic en el botón **Siguiente** para continuar.

## 6.2. Programar análisis y actualizaciones automáticas



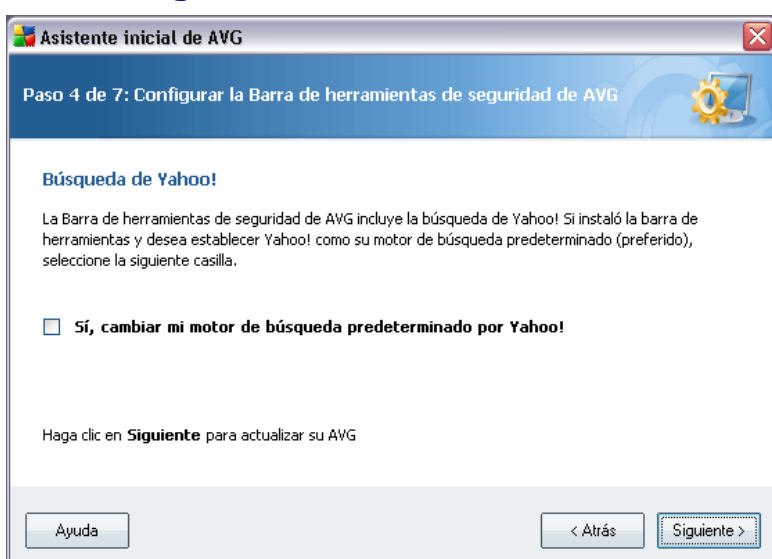
En el diálogo **Programar análisis y actualizaciones automáticas** configure el intervalo para comprobar la accesibilidad de los nuevos archivos de actualización, y defina la hora en que debe iniciarse el [análisis programado](#). Se recomienda mantener los valores predeterminados. Presione el botón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

## 6.3. Ayúdenos a identificar nuevas amenazas en línea



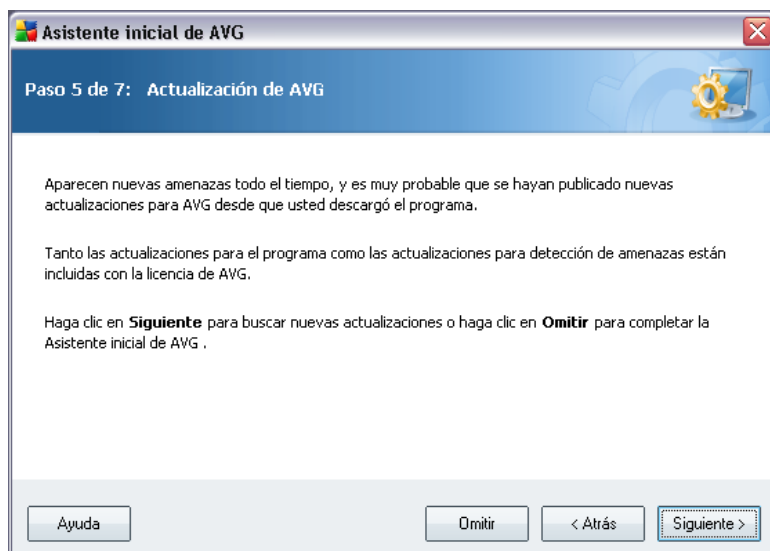
En el diálogo **Ayúdenos a identificar nuevas amenazas**, decida si desea activar la opción de informar de vulnerabilidades y sitios peligrosos que encuentren los usuarios a través de las funciones **Protección de navegación AVG / Protección de búsqueda AVG** del componente **LinkScanner** para alimentar la base de datos con la información recopilada sobre actividades maliciosas en la Web. Se recomienda mantener el valor predeterminado y tener los informes activados. Presione el botón **Siguiente** para continuar.

#### 6.4. Configurar la Barra de herramientas AVG Security



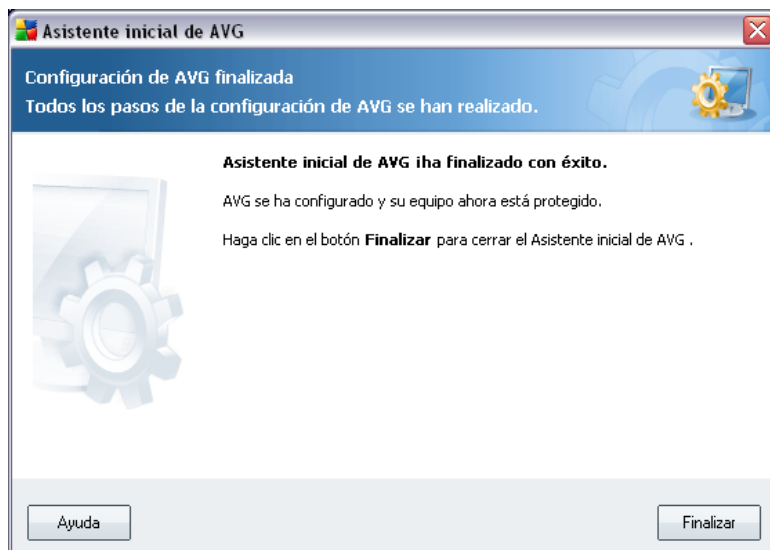
En el diálogo **Configurar la Barra de herramientas AVG Security** puede marcar la casilla de verificación para definir que desea que Yahoo! sea el motor de búsqueda predeterminado.

## 6.5. Actualizar protección AVG



El diálogo **Actualizar la protección AVG** comprobará y descargará automáticamente las [Actualizaciones de AVG](#) más recientes. Haga clic en el botón **Siguiente** para descargar los últimos archivos de actualización y realizar la actualización.

## 6.6. Configuración de AVG finalizada



Se ha configurado su **Anti-Virus AVG 8.5**; presione el botón **Finalizar** para comenzar a trabajar con AVG.

## 7. Después de la instalación

### 7.1. Registro del producto

Una vez finalizada la instalación de **Anti-Virus AVG 8.5**, registre su producto en línea en el [sitio web de AVG](#), en la página **Registro** ( *siga las instrucciones indicadas directamente en la página*). Tras el registro, dispondrá de pleno acceso a la cuenta de usuario AVG, el boletín de actualizaciones de AVG y otros servicios que se ofrecen exclusivamente para los usuarios registrados.

### 7.2. 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/Todos los programas/AVG 8.0/Interfaz de usuario de AVG**

### 7.3. 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 8.5**. 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](#).

### 7.4. Análisis Eicar

Para confirmar que **Anti-Virus AVG 8.5** 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](http://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.

## 7.5. Configuración predeterminada de AVG

La configuración predeterminada (*es decir, la configuración de la aplicación inmediatamente después de la instalación*) de **Anti-Virus AVG 8.5** 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.

## 8. Interfaz del usuario de AVG

Anti-Virus AVG 8.5 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 >>](#)

## 8.1. 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 8.5** 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:

### 8.1.1. Archivo

- **Salir:** cierra la interfaz de usuario de **Anti-Virus AVG 8.5**. Sin embargo, la aplicación de AVG continuará funcionando en segundo plano y su equipo seguirá estando protegido.

### 8.1.2. Componentes

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

- **Vista general del sistema:** permite ir al diálogo predeterminado de la interfaz de usuario con la [vista general de todos los componentes instalados y su estado](#).
- **Anti-Virus:** abre la página predeterminada del componente [Anti-Virus](#).
- **Anti-Rootkit:** abre la página predeterminada del componente [Anti-Rootkit](#).
- **Anti-Spyware:** abre la página predeterminada del componente [Anti-Spyware](#).
-

- 
- 
- **Analizador de correos electrónicos:** abre la página predeterminada del componente **Analizador de correos electrónicos**.
- **Licencia:** abre la página predeterminada del componente [Licencia](#).
- **LinkScanner:** abre la página predeterminada del componente [LinkScanner](#)
- **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](#).

### 8.1.3. 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 8.5** registradas.

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

#### 8.1.4. 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 8.5**
- **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 8.5** configuración. Generalmente, se recomienda mantener la configuración predeterminada de la aplicación como se encuentra definida por el distribuidor del software.
- 

#### 8.1.5. Ayuda

- **Contenido:** abre los archivos de ayuda AVG
- **Obtener ayuda en línea:** abre el sitio web de [AVG](#) en la página del centro de soporte al cliente
- **Su Web AVG:** abre la [página de inicio de AVG](#) (en [www.avg.com](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 su número de licencia para reemplazar el número de ventas (*el número con el que instaló AVG*), o reemplazar el número de licencia anterior (*por ejemplo, cuando actualiza hacia un producto más reciente de AVG*).
- **Registrar ahora:** conecta con el sitio web de registro en [www.avg.com](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**.

## 8.2. 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 8.5**. 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.



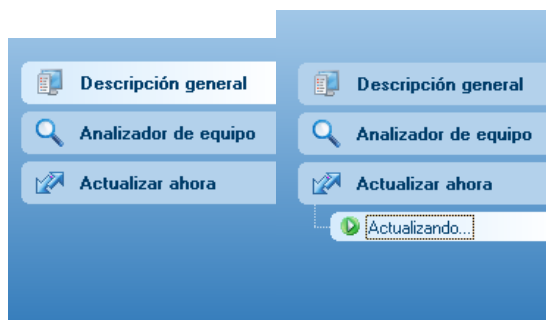
El icono rojo indica que AVG se encuentra en estado crítico. Uno o más componentes no funcionan correctamente y AVG no puede proteger su equipo. Preste atención de inmediato para corregir el problema notificado. Si no puede corregir el error sin ayuda, póngase en contacto con el equipo de [soporte técnico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

### 8.3. 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 Imagen 2*).

#### **8.4. 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 8.5** 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 >>](#)
- **Anti-Rootkit** detecta los programas y las tecnologías que intentan camuflar malware. [Detalles >>](#)
- **Analizador de correos electrónicos** verifica todo el correo entrante y saliente para ver si contiene virus. [Detalles >>](#)
- **Licencia** muestra el texto completo del contrato de licencia de AVG. [Detalles >>](#)
- **LinkScanner** comprueba los resultados de búsqueda visualizados en el navegador de Internet. [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](#).


## 8.5. 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.

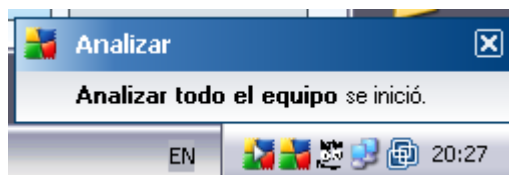
## 8.6. Icono en la bandeja de sistema

**El icono de la bandeja del sistema** (en la barra de tareas de Windows) indica el estado actual de **Anti-Virus AVG 8.5**. 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 [Ignorar 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 adicionalmente informa sobre las actividades actuales de AVG y los cambios posibles de estado en el programa (*por ejemplo inicio automático de un análisis o de una actualización programados, , cambio de estado de un componente, ocurrencia de estado de error, ...*) mediante una ventana emergente que se abre desde el icono de la bandeja de sistema AVG:



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

- **Abrir interfaz del usuario de AVG:** haga clic para abrir la [Interfaz del usuario de AVG](#).
- **Actualizar:** ejecuta una actualización [inmediata](#).
- **Salir:** haga clic para cerrar el programa AVG (*solo se cierra la interfaz de usuario, el programa AVG sigue ejecutándose en segundo plano y el equipo continúa estando totalmente protegido*).

## 9. Componentes de AVG

### 9.1. Antivirus

#### 9.1.1. 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.

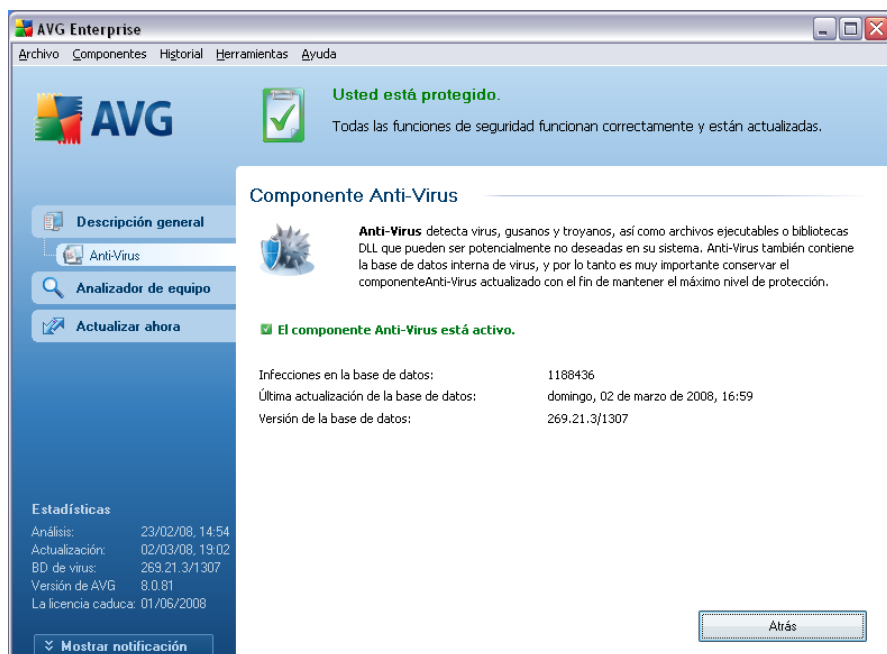
***La función esencial de la protección antivirus es que ningún virus conocido pueda ejecutarse en el equipo.***

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.

## 9.1.2. 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.

## 9.2. Anti-Spyware

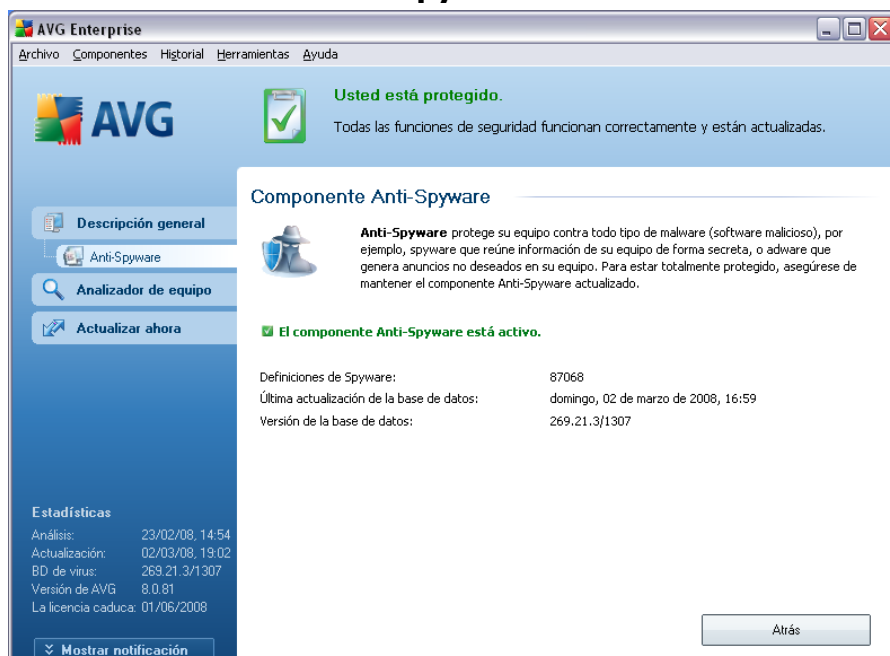
### 9.2.1. Anti-Spyware Principios de

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 8.5** actualizado con las últimas actualizaciones de la base de datos [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.

## 9.2.2. 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.

### 9.3. Anti-Rootkit

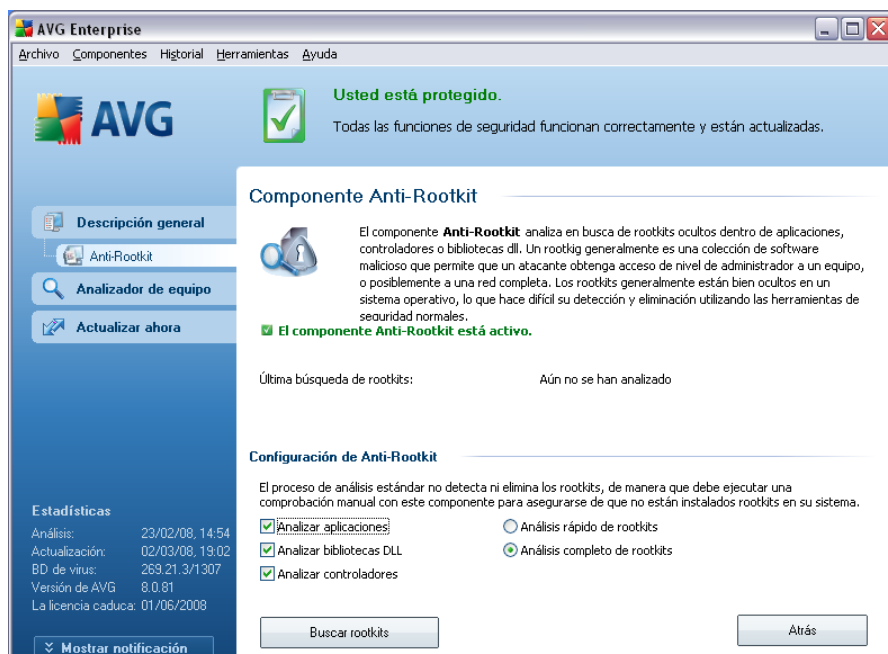
#### 9.3.1. Principios de Anti-Rootkit

**Anti-Rootkit** es una herramienta especializada que detecta y elimina con eficacia los rootkits peligrosos, es decir, los programas y las tecnologías que puede camuflar la presencia de software malicioso en el equipo.

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



### 9.3.2. Interfaz de Anti-Rootkit



La interfaz de usuario de **Anti-Rootkit** ofrece una breve descripción de las funciones del componente, información sobre su estado actual (El componente *Anti-Rootkit* está activo) e información sobre la última vez que se ha ejecutado el análisis de **Anti-Rootkit**.

En la parte inferior del diálogo, puede encontrar la sección **Configuración de Anti-Rootkit** donde puede configurar algunas funciones básicas del análisis de detección de rootkits. En primer lugar, marque las casillas de verificación respectivas para especificar los objetos que deben analizarse:

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

También puede seleccionar el modo de análisis de rootkits:

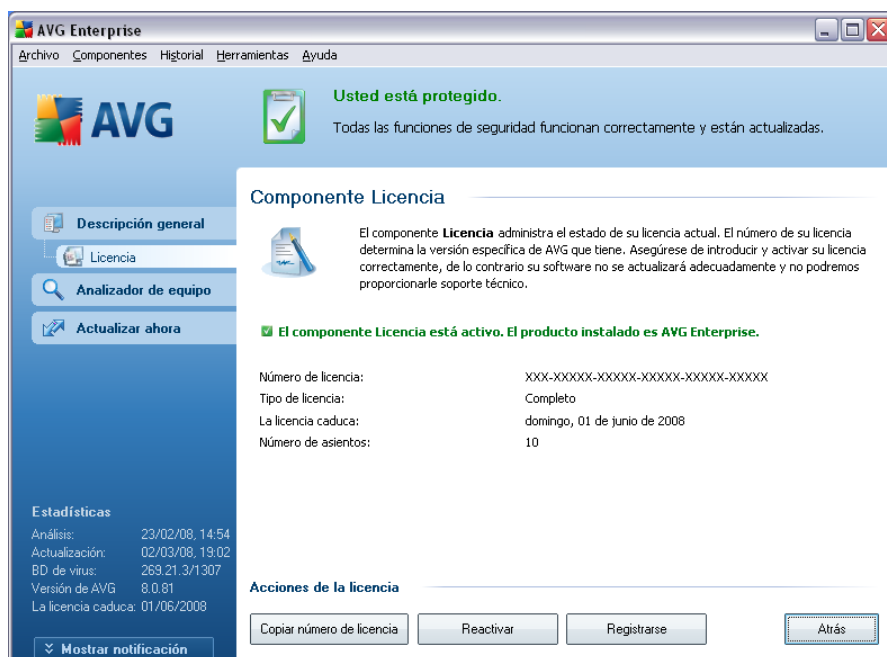
- **Análisis de rootkits rápido:** sólo analiza la carpeta del sistema (normalmente, *c:\Windows*).
- **Análisis de rootkits completo:** analiza todos los discos disponibles excepto

A: y B:.

Botones de control disponibles:

- **Buscar rootkits:** como el análisis de rootkits no es un elemento implícito de [Análisis de todo el equipo](#), puede ejecutar el análisis de rootkits directamente desde la interfaz de **Anti-Rootkit** con este botón.
- **Guardar cambios:** presione este botón para guardar y aplicar todos los cambios efectuados en esta interfaz y regresar a la [Interfaz del usuario de AVG](#) predeterminada (descripción general de los componentes)
- **Cancelar:** presione este botón para regresar a la [Interfaz del usuario de AVG](#) predeterminada (descripción general de los componentes) sin guardar los cambios realizados

## 9.4. 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. Para su comodidad, el diálogo **Licencia** ofrece el botón **Copiar número de licencia**: presione el botón para copiar el número de licencia en el portapapeles y después simplemente podrá pegarlo donde desee (**CTRL+V**).

- **Tipo de licencia**: especifica la edición del producto definida por el número de licencia.
- **Caducidad de la licencia**: esta fecha determina el período de validez de la licencia. Si desea seguir utilizando AVG 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.
- **Número de puestos**: indica en cuántas estaciones de trabajo puede instalar el programa AVG.

### Botones de control

- **Copiar el número de licencia**: presione el botón para insertar el número de licencia utilizado actualmente en el portapapeles (*es igual que presionar CTRL+C*), y pegarlo donde lo requiera
- **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*).
- **Registrar**: conecta al sitio web de registro en [www.avg.com](http://www.avg.com). Introduzca su información de registro; sólo los clientes con productos AVG registrados pueden recibir soporte técnico gratuito.
- **Atrás**: presione este botón para volver a la [interfaz del usuario de AVG](#) predeterminada (vista general de componentes)

## 9.5. Link Scanner

### 9.5.1. Principios de Link Scanner

**LinkScanner** coopera con Internet Explorer y Firefox (1.5 y posterior), y consta de dos funciones: **Protección de navegación activa AVG** y **Protección para búsquedas AVG**.

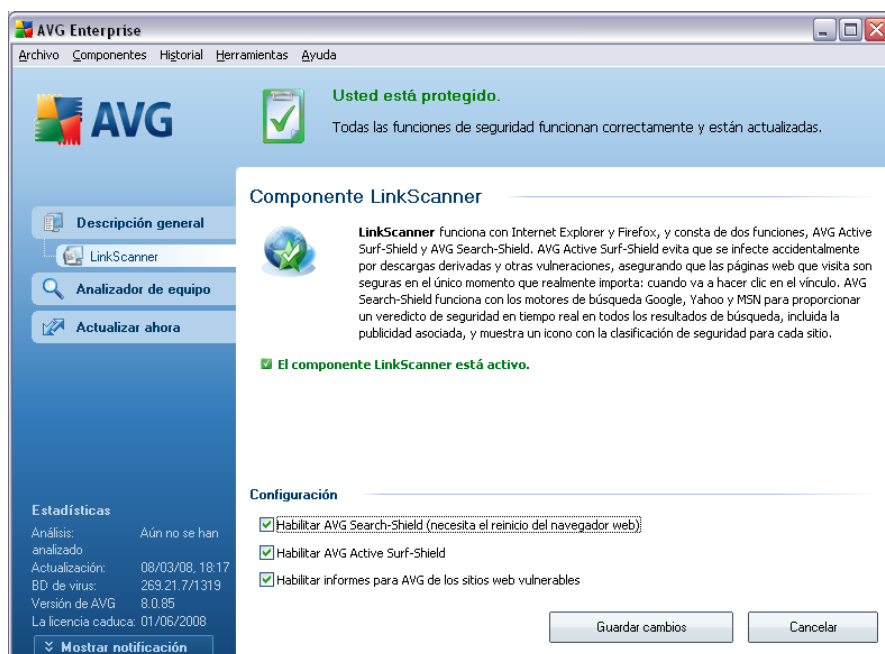
**La Protección de navegación activa AVG** evita que se infecte accidentalmente por descargas derivadas y otras vulneraciones, asegurando que las páginas Web que visita sean seguras en el único momento que realmente importa: cuando va a hacer clic en el vínculo.

**La Protección para búsquedas AVG** funciona con los motores de búsqueda Google, Yahoo! y MSN para proporcionar un veredicto de seguridad en tiempo real en todos los resultados de búsqueda, incluida la publicidad asociada, y muestra un icono con la clasificación de seguridad para cada sitio.

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

### 9.5.2. Interfaz de Link Scanner

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



- **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. Los exploradores compatibles son Internet Explorer y Firefox.


- **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 sitios maliciosos conocidos y su contenido de explotación se bloquean cuando el usuario tiene acceso a ellos mediante un explorador Web (*o cualquier otra aplicación que utilice HTTP*).
- **Informes de respaldo de sitios web vulnerables** : marque este elemento para permitir informes de respaldo de sitios vulnerables y peligrosos encontrados por el usuario mediante **Navegación segura** o **Búsqueda segura** con el fin de alimentar la base de datos con la información recopilada sobre la actividad maliciosa en la Web.

### 9.5.3. 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.

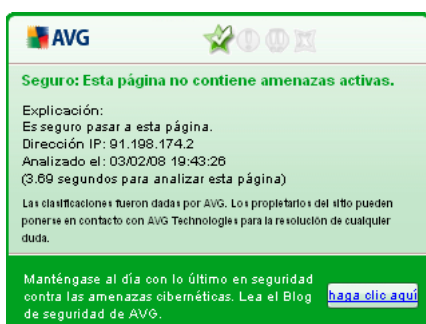
Mientras se evalúa un vínculo en la página de resultados de búsqueda, verá un símbolo situado junto a él para informarle de que la verificación del vínculo está en curso. Al finalizar la evaluación se mostrará el icono informativo respectivo:



-  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:



**Seguro: Esta página no contiene amenazas activas.**

Explicación:  
 Es seguro pasar a esta página.  
 Dirección IP: 91.198.174.2  
 Analizado el: 03/02/08 19:43:26  
 (3.69 segundos para analizar esta página)

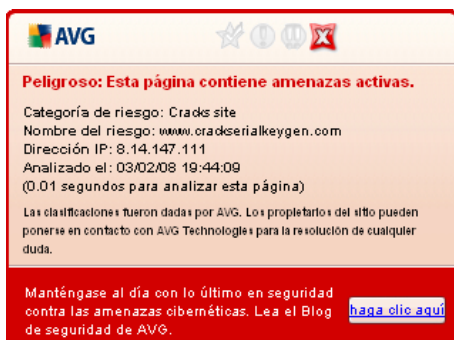
Las clasificaciones fueron dadas por AVG. Los propietarios del sitio pueden ponerse en contacto con AVG Technologies para la resolución de cualquier duda.

Manténgase al día con lo último en seguridad contra las amenazas cibernéticas. Lea el Blog [haga clic aquí](#) de seguridad de AVG.

#### 9.5.4. 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:



Si desea visitar la página infectada, existe un vínculo a la página en esta pantalla, **sin embargo, no se recomienda continuar con estas páginas.**

## 9.6. Web Shield

### 9.6.1. 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.*

### 9.6.2. Interfaz de Web Shield

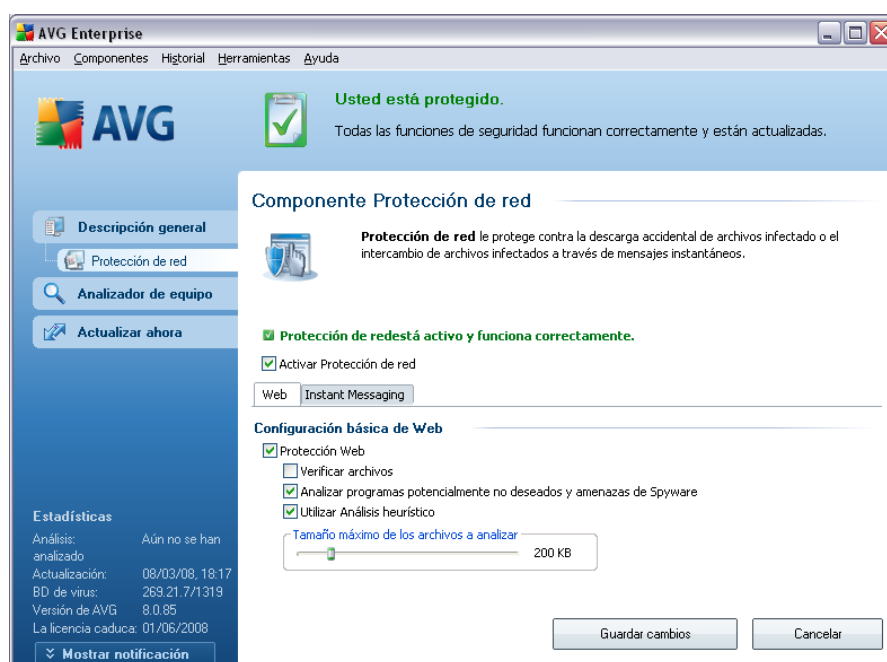
La interfaz del componente **Web Shield** describe el comportamiento de este tipo de protección. Adicionalmente puede encontrar información acerca del estado actual del componente (*Web Shield está activa y completamente funcional.*). En parte inferior del diálogo encontrará a continuación las opciones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

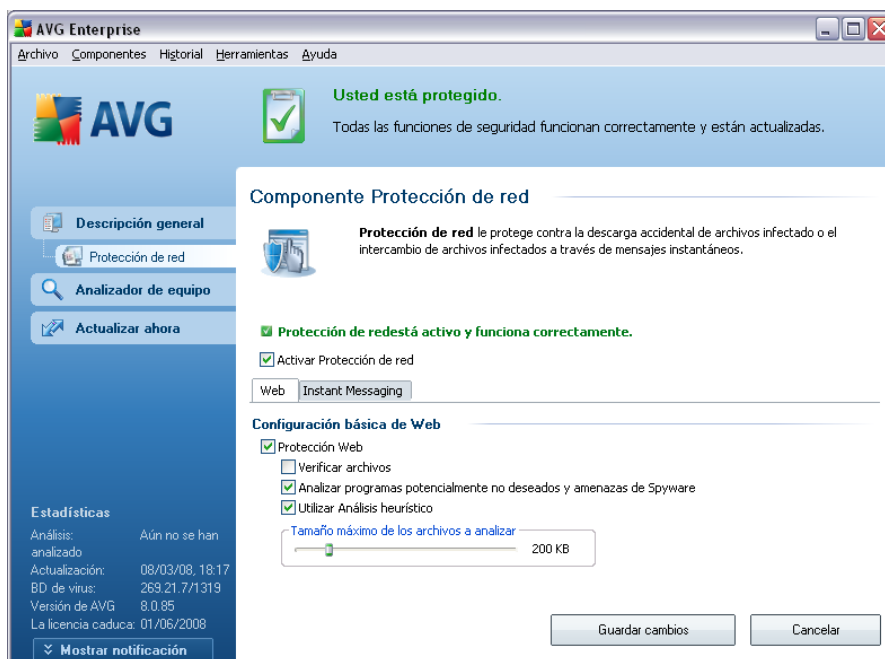


- **Web Shield**: esta opción confirma que **Web Shield** debe analizar el contenido de las páginas www. Mientras esta opción esté seleccionada (valor predeterminado), podrá activar o desactivar estos elementos:
  - **Examinar archivos**: analiza el contenido de los archivos que probablemente contenga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



- 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 8.5** 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*).

### 9.6.3. 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** (accesible mediante el menú de sistema *Historial /*

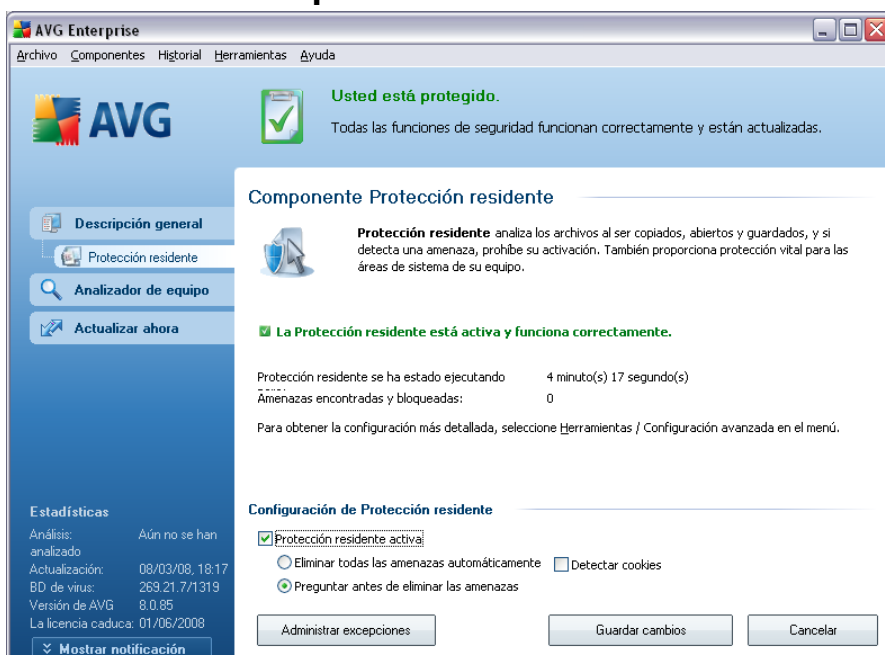
Hallazgos de Web Shield).

## 9.7. Protección residente

### 9.7.1. Protección residente Principios de

La **Protección residente** analiza archivos mientras éstos se copian, se abren o se guardan. 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. La **Protección residente**, que se carga en la memoria de su equipo durante el inicio del sistema, también proporciona protección vital para las áreas del sistema de su equipo.

### 9.7.2. 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 residente 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.

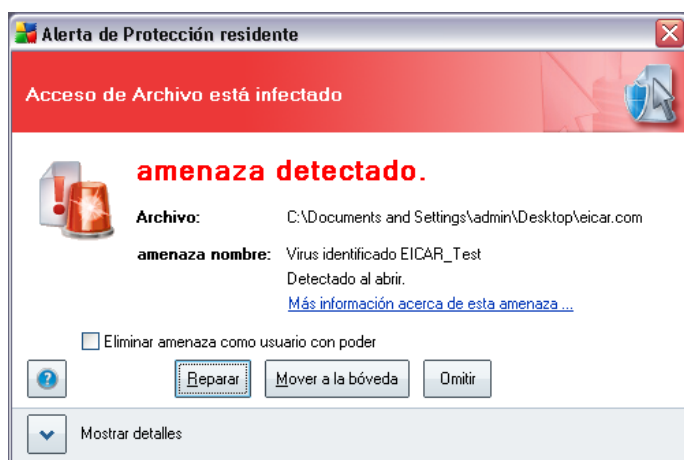
## Botones de control

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).

### 9.7.3. Detección de protección residente

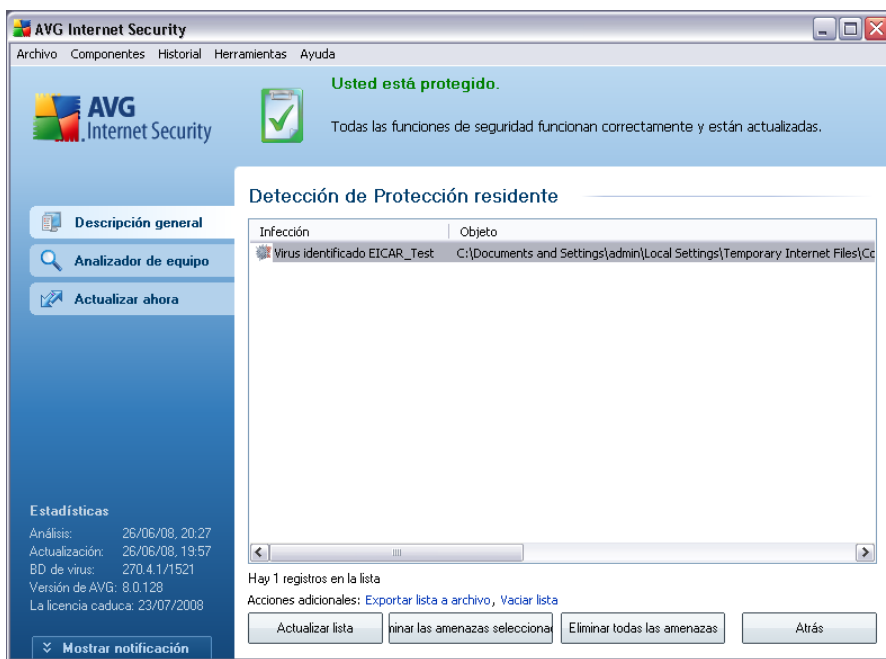
La **Protección residente** analiza los archivos mientras éstos se copian, se abren o se guardan. Cuando se detecta una amenaza de virus o de cualquier tipo, se le advertirá inmediatamente mediante este diálogo:



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**.

- **Ignorar:** recomendamos ampliamente NO utilizar esta opción, a menos que tenga una muy buena razón para hacerlo.



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:

- **Infeción:** descripción (probablemente aún el nombre) del objeto detectado
- **Objeto:** ubicación del objeto
- **Resultado:** acción realizada con el objeto 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).

## 9.8. Administrador de actualización

### 9.8.1. Principios de administrador de actualización

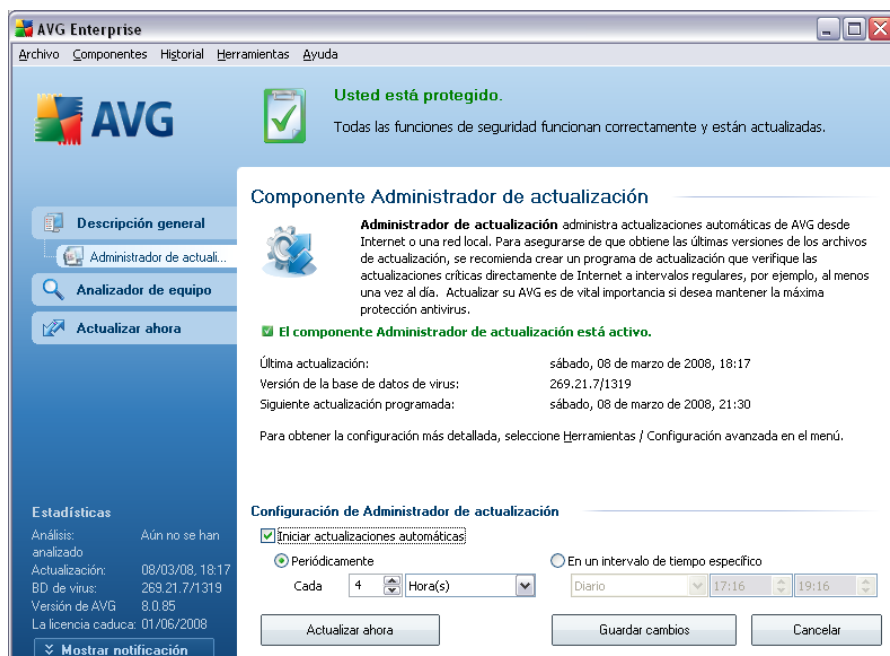
Ningún software de seguridad puede garantizar una verdadera protección ante los diversos tipos de amenazas si no se actualiza periódicamente. Los desarrolladores de virus siempre buscan nuevas fallas que explotar en el software y el sistema operativo. Diariamente aparecen nuevos virus, nuevo malware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

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

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

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

## 9.8.2. 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.

### 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).

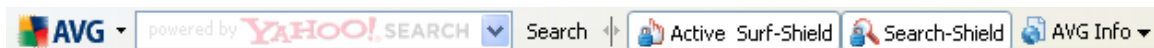
## 9.9. Barra de herramientas AVG Security

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 instalada la **barra de herramientas AVG Security**, se colocará de forma

predeterminada debajo de la barra de dirección de su navegador:

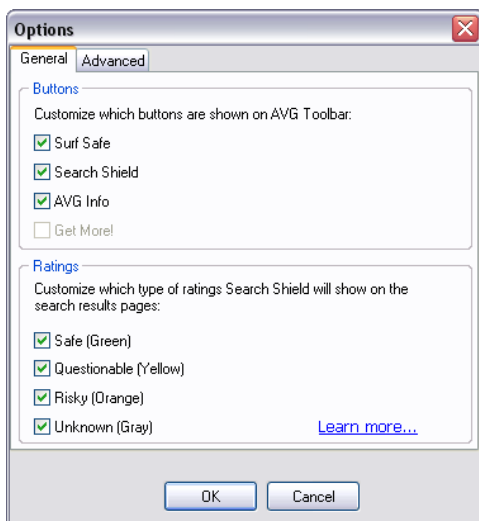


La **barra de herramientas AVG Security** consta de los siguientes elementos:

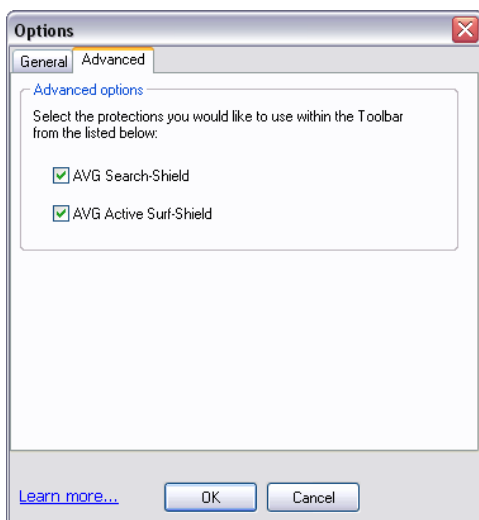
- **Botón del logo AVG** : proporciona acceso a los elementos generales de la barra de herramientas. Haga clic en el botón del logo AVG para ir al sitio web de AVG ([www.avg.com](http://www.avg.com)). Al hacer clic con el puntero al lado del icono AVG se abrirán las siguientes opciones:
  - **Información 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 8.0**: abre la [interfaz del usuario de AVG 8](#)
  - **Opciones**: abre un diálogo de configuración donde puede ajustar la configuración de la **barra de herramientas AVG Security** para adaptarla a sus necesidades; el diálogo se divide en dos pestañas:
    - **General**: en esta pestaña puede encontrar dos secciones denominadas **Botones** y **Clasificaciones**.

La sección **Botones** permite configurar qué botones son visibles o están ocultos en la **barra de herramientas AVG Security**. De manera predeterminada, todos los botones son visibles.

La sección **Clasificaciones** permite determinar el tipo de clasificaciones que se deben mostrar para los resultados de búsqueda. De manera predeterminada, todas las clasificaciones son visibles, pero puede ocultar algunas de ellas (*al buscar desde el cuadro de búsqueda de Yahoo!, sólo aparecen los resultados seguros*).



- **Avanzadas:** en esta pestaña puede editar las funciones de protección de la **barra de herramientas AVG Security**. De manera predeterminada, las funciones **Protección de búsqueda AVG** y **Protección de navegación activa AVG** están activadas.



- **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 fácil y segura de buscar en la Web utilizando 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](#)
- **Botón Información AVG:** proporciona vínculos a información de seguridad importante ubicada en el sitio web de AVG ([www.avg.com](http://www.avg.com))

## 10. Protección de Identidad

**Protección de Identidad** es un componente independiente anteriormente conocido como Sana que ha sido incorporado recientemente **Anti-Virus AVG 8.5**. Es instalado desde el archivo de instalación con el número de licencia correspondiente (*para más detalles acerca de la selección del programa y licenciamiento por favor vea [AVG Administrador de Descargas](#)*).

**Protección de Identidad** está disponible únicamente en Inglés.

### 10.1. Principios de Protección de Identidad

Software de prevención de robo de identidad

Sana proviene de software basado en comportamiento. Debido a que lee las características y comportamiento del código malicioso/amenazas, el software versátil y único de Sana previene el ataque emergente y futuras amenazas desconocidas en tiempo real (protección de día cero). Como dice el equipo de Sana: "Protección instantánea y continua".

### 10.2. Interface de Protección de Identidad

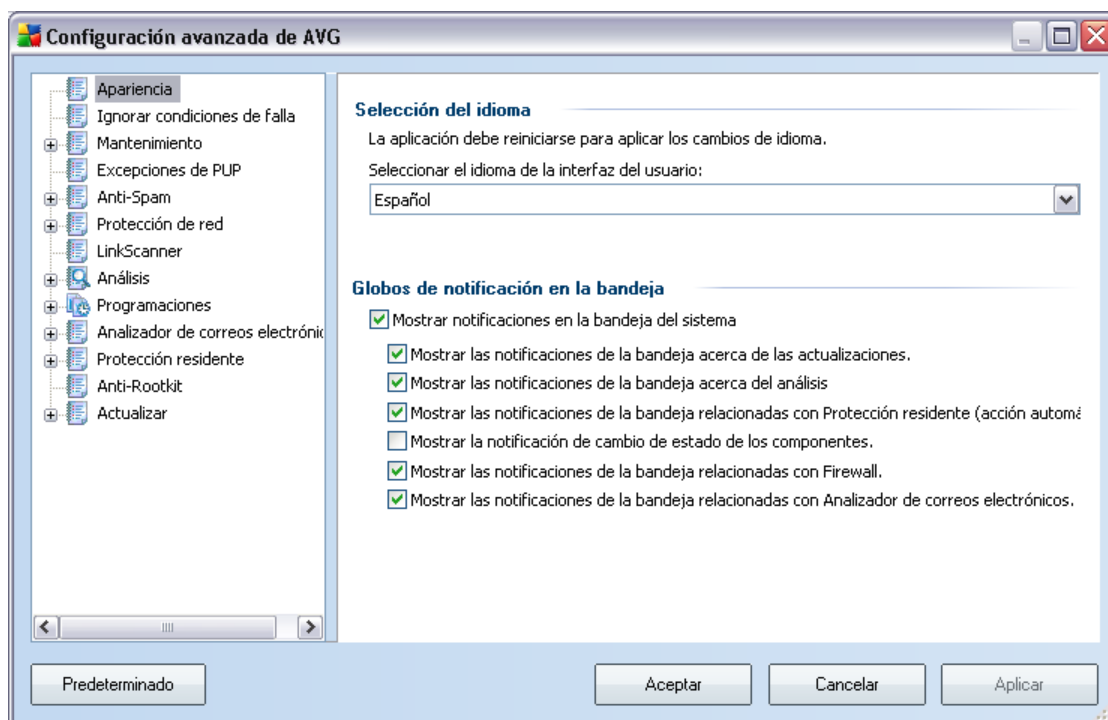
Introduzca el texto del tema aquí.

## 11. Configuración avanzada de AVG

El diálogo de configuración avanzada de **Anti-Virus AVG 8.5** 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.

### 11.1. 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 cerrar el diálogo de edición **Configuración avanzada de AVG**
- Cierre la [Interfaz del usuario de AVG](#) mediante la opción del elemento [de menú del sistema Archivo/Salir](#)
- Vuelva a abrir la [interfaz del usuario de AVG](#) mediante una de estas opciones: haga doble clic en el [icono de la bandeja del sistema AVG](#), haga doble clic en el icono AVG en su escritorio, o a través del menú **Inicio/Todos los programas/AVG 8.0/Interfaz del usuario de AVG** (consulte el capítulo [Acceso a la interfaz de usuario](#)). A continuación se mostrará la interfaz de usuario en el idioma recientemente seleccionado.

### 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**

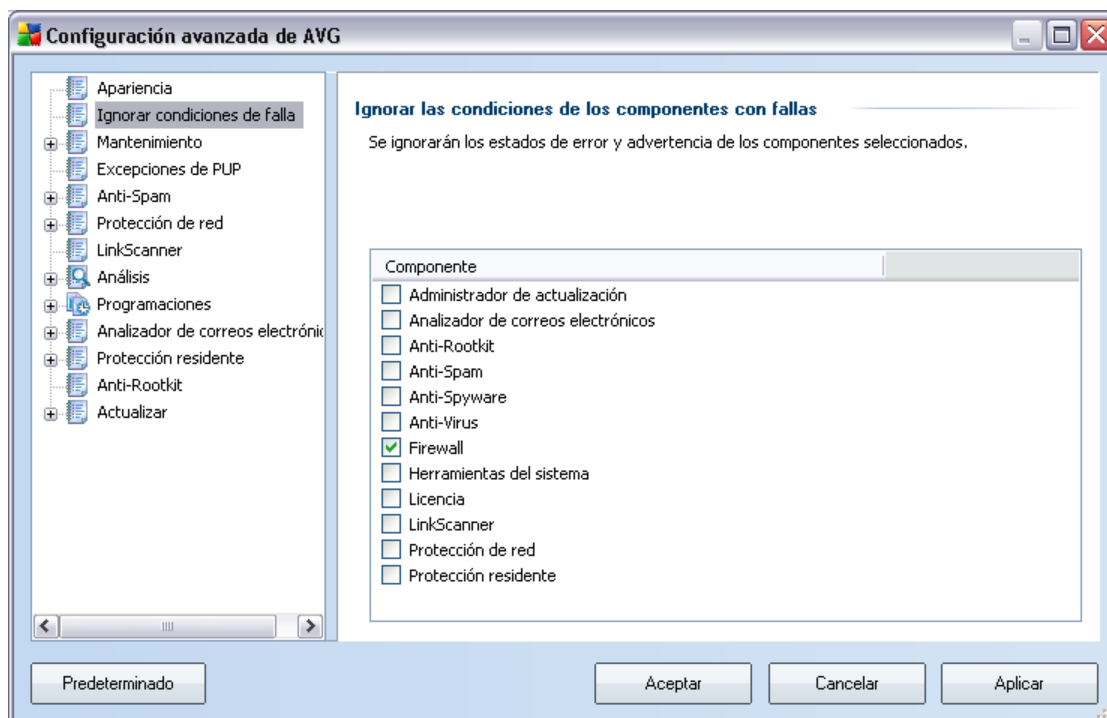
**actualizaciones**: decida si debe visualizarse información sobre la ejecución, el progreso y la finalización del proceso de actualización de AVG;

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



## 11.2. 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:

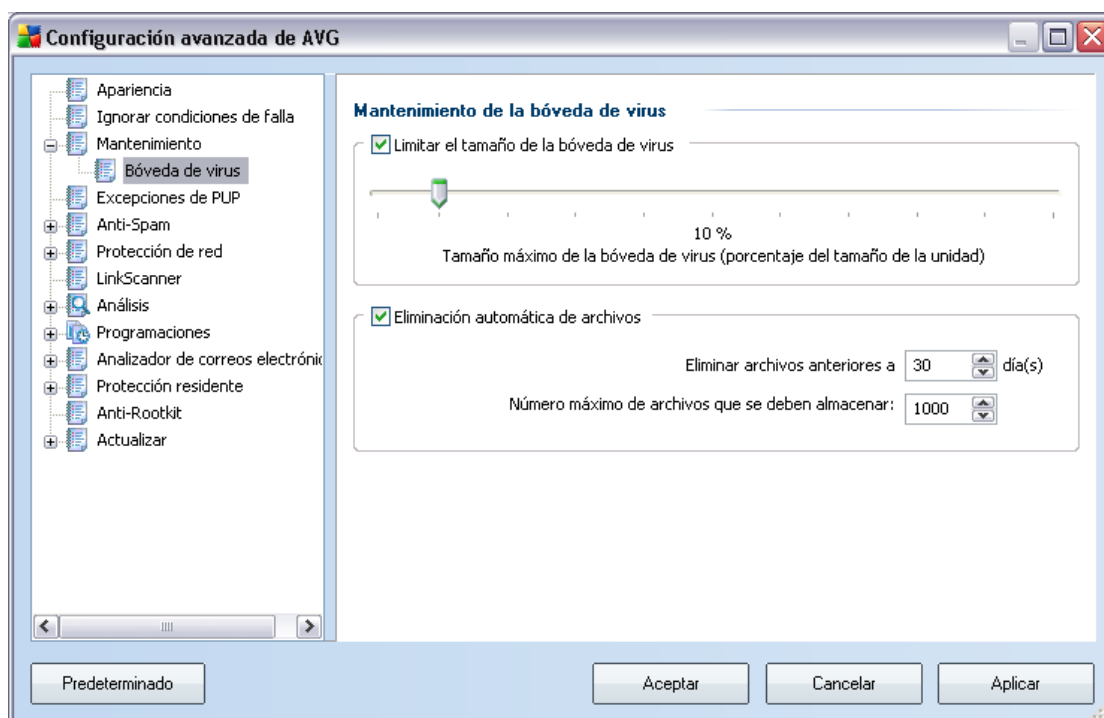
- **el icono en la bandeja de sistema** (mientras todas las partes de AVG estén trabajando correctamente, el icono se muestra en cuatro colores; sin embargo, si ocurre un error, el icono cambia a color gris con un signo de admiración de color rojo,
- la descripción de texto del problema existente en 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](#).

### 11.3. Bóveda de Virus



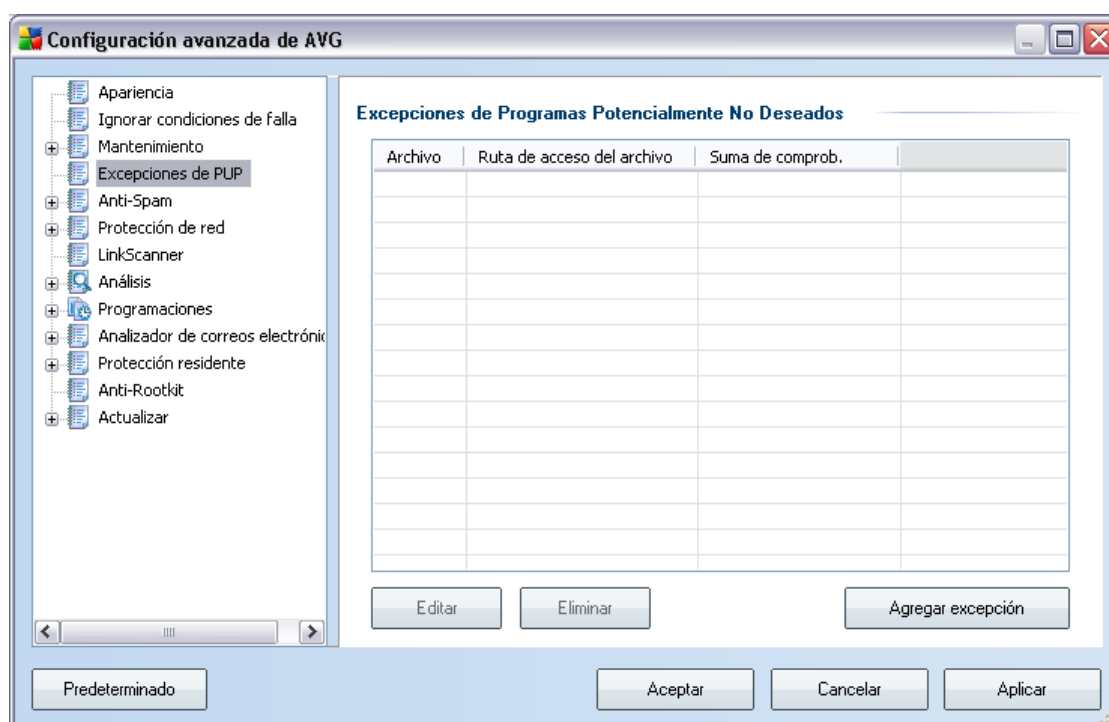
El diálogo **Mantenimiento de la Bóveda de Virus** permite definir varios parámetros relacionados con la administración de objetos almacenados en la [Bóveda de Virus](#):

- **Límite de 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**).

## 11.4.Excepciones de PPND

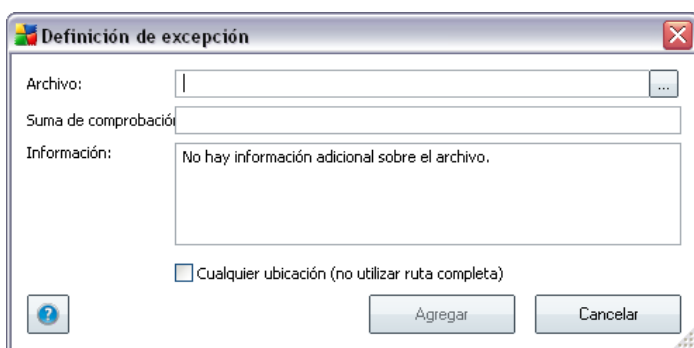
AVG puede analizar y detectar aplicaciones ejecutables o bibliotecas DLL que podrían ser potencialmente no deseadas dentro del sistema. En algunos casos, el usuario puede querer mantener ciertos programas no deseados en el equipo (programas que fueron instalados intencionalmente). Algunos programas, 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, eliminar o agregar nuevas excepciones.

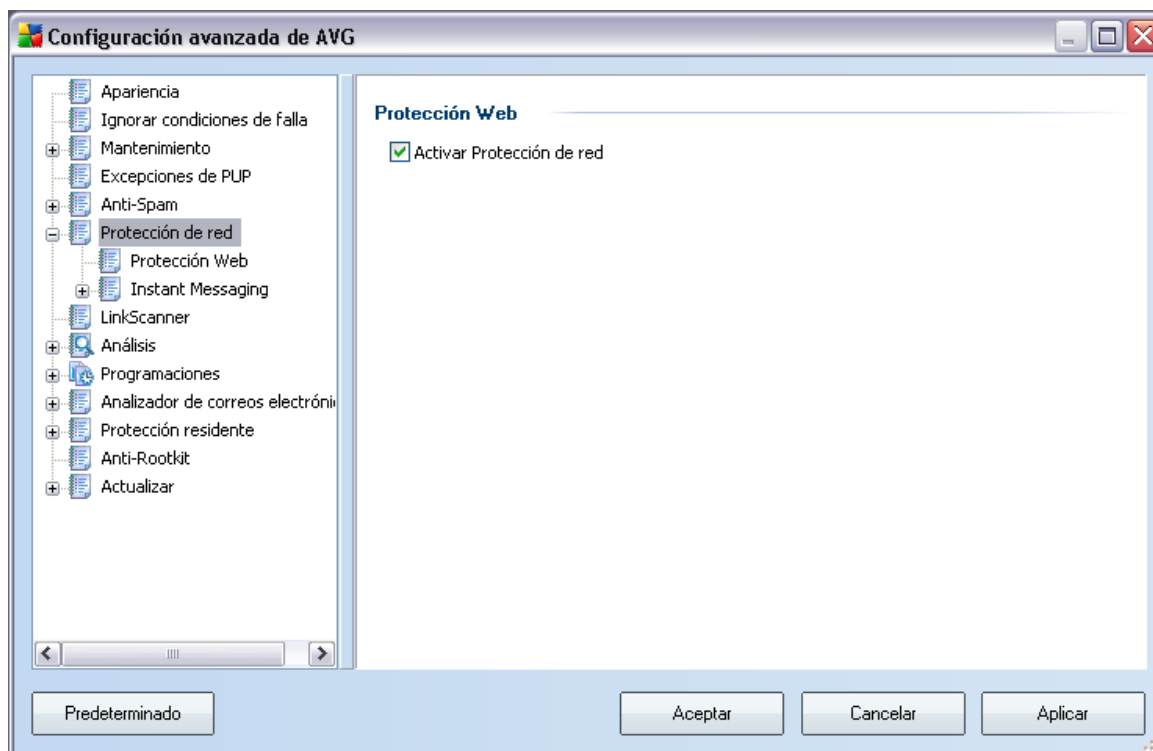
## Botones de control

- **Editar** : abre un diálogo de edición (*idéntico al 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

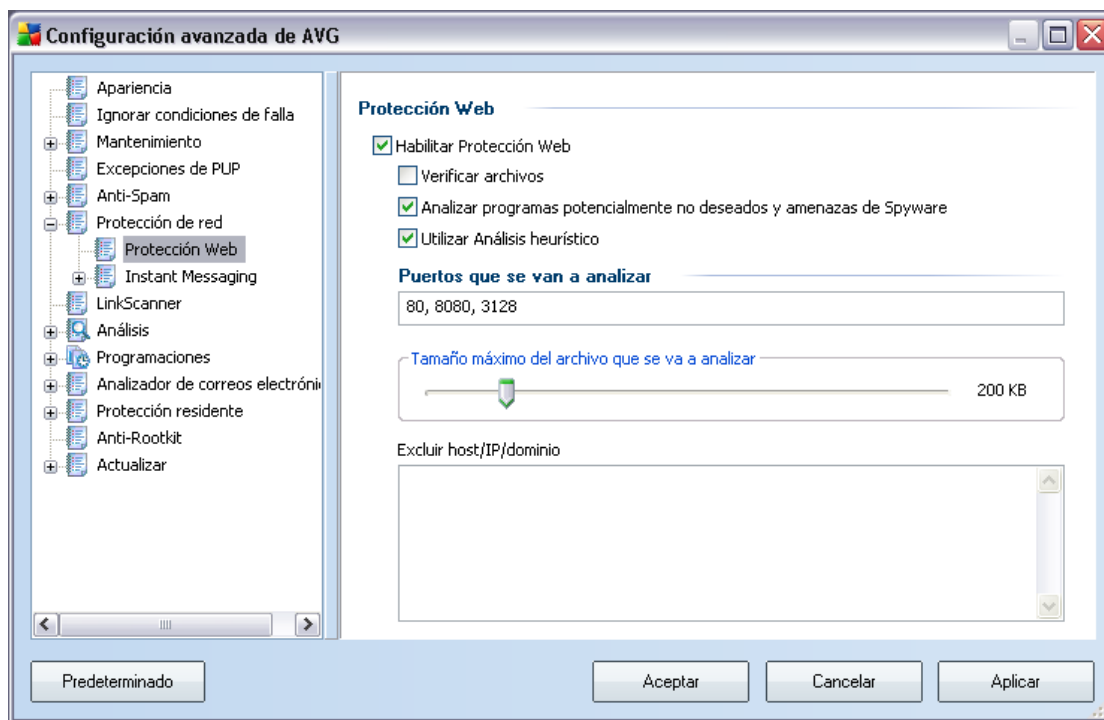
## 11.5. Web Shield



El diálogo **protección Web** permite activar o desactivar el componente **Web Shield** completo (*activado de forma predeterminada*). Para la configuración avanzada adicional de este componente, continúe a los diálogos posteriores que se muestran en la navegación de árbol.

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

### 11.5.1. Protección Web



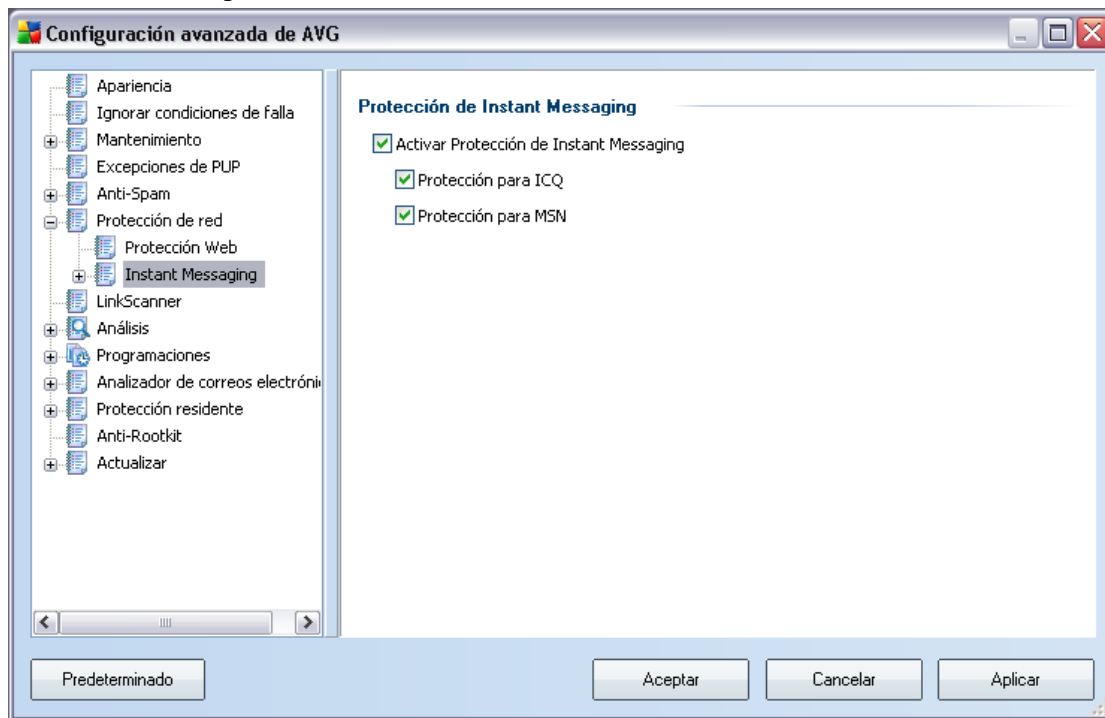
En el cuadro de diálogo **Protección Web** puede editar la configuración del componente en relación con el análisis del contenido de sitios web. La interfaz de edición permite configurar las opciones básicas siguientes:

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

## 11.5.2. Mensajería instantánea

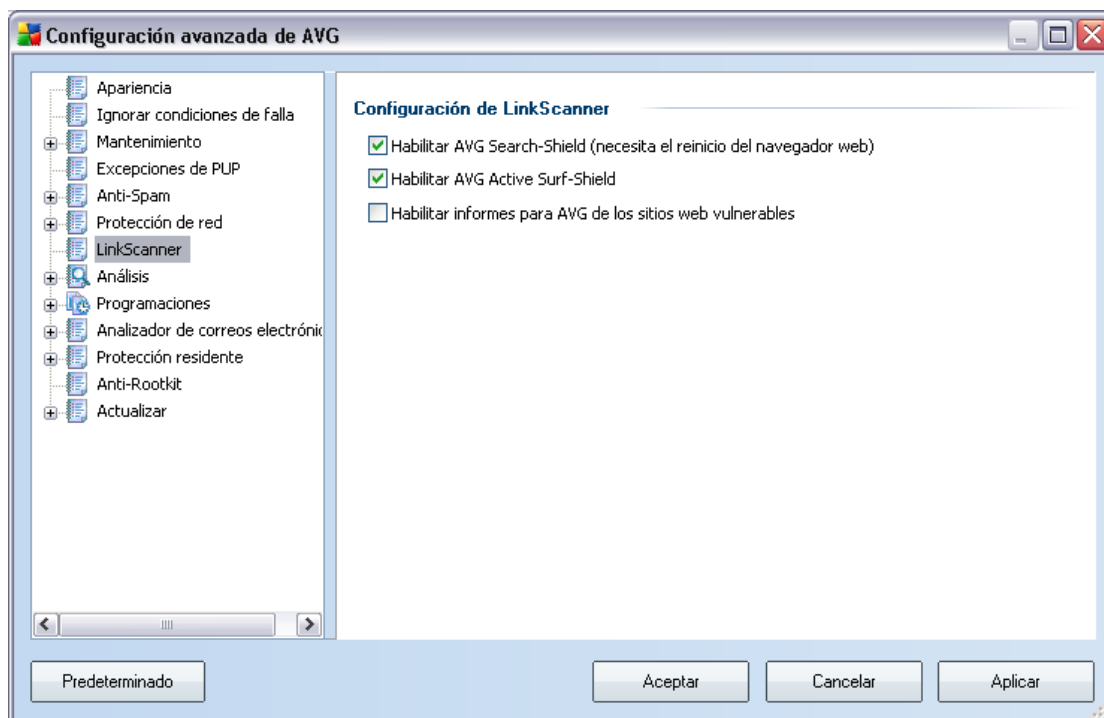


En el diálogo **Protección de mensajería instantánea** puede editar la configuración del componente **Web Shield** relativa al análisis de la mensajería instantánea. Actualmente sólo se admiten tres programas de mensajería instantánea: **ICQ**, **MSN** y **Yahoo**: marque el elemento correspondiente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

Para una especificación más detallada de los usuarios permitidos y bloqueados, puede ver y editar el diálogo correspondiente (**Opciones avanzadas de ICQ** y **Opciones avanzadas de MSN**) 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).



## 11.6.Link Scanner



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

- **Habilitar la búsqueda segura**, (activada de manera predeterminada): iconos asesores de notificación en las búsquedas efectuadas en Google, Yahoo o MSN que verifican por adelantado el contenido de los sitios devueltos por el motor de búsqueda. Los exploradores compatibles son Internet Explorer y Firefox.
- **Activar la navegación segura**: (activada de manera predeterminada): protección (*en tiempo real*) activa contra sitios de explotación cuando se accede 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 los informes para AVG de los sitios Web de explotación** : (activado de forma predeterminada): marque este elemento para permitir que los informes de respaldo de los sitios de explotación y riesgosos que encontraron los usuarios mediante **Navegación segura** o **Búsqueda segura**

se alimenten a la información de recolección de la base de datos acerca de actividad maliciosa en la Web.

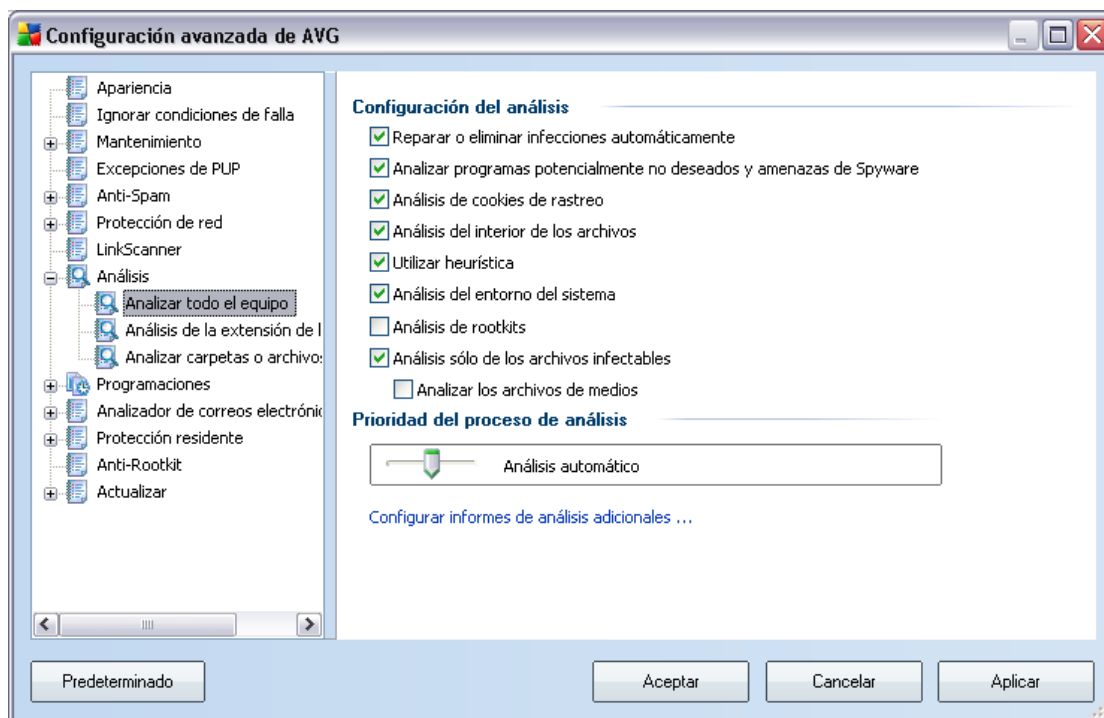
### **11.7.Análisis**

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

### 11.7.1. 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:** este parámetro controla la función [Anti-Virus](#) 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:** 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.
- **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](#);
- **Analizar sólo archivos infectables:** con esta opción seleccionada, no se analizarán los archivos que no se pueden infectar. Por ejemplo, algunos archivos de sólo texto o algún otro tipo de archivo no ejecutable.
  - **Analizar los archivos de medios :** seleccione esta casilla para analizar los archivos de medios (video, audio, etc.). Si deja esta casilla sin seleccionar, reducirá aún más el tiempo de análisis, ya que estos archivos generalmente son de gran tamaño y no son demasiado propensos a estar infectados por virus.

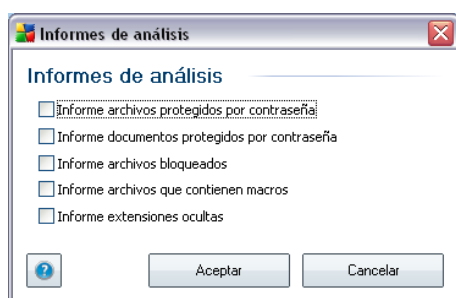
### Prioridad del proceso de análisis

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.

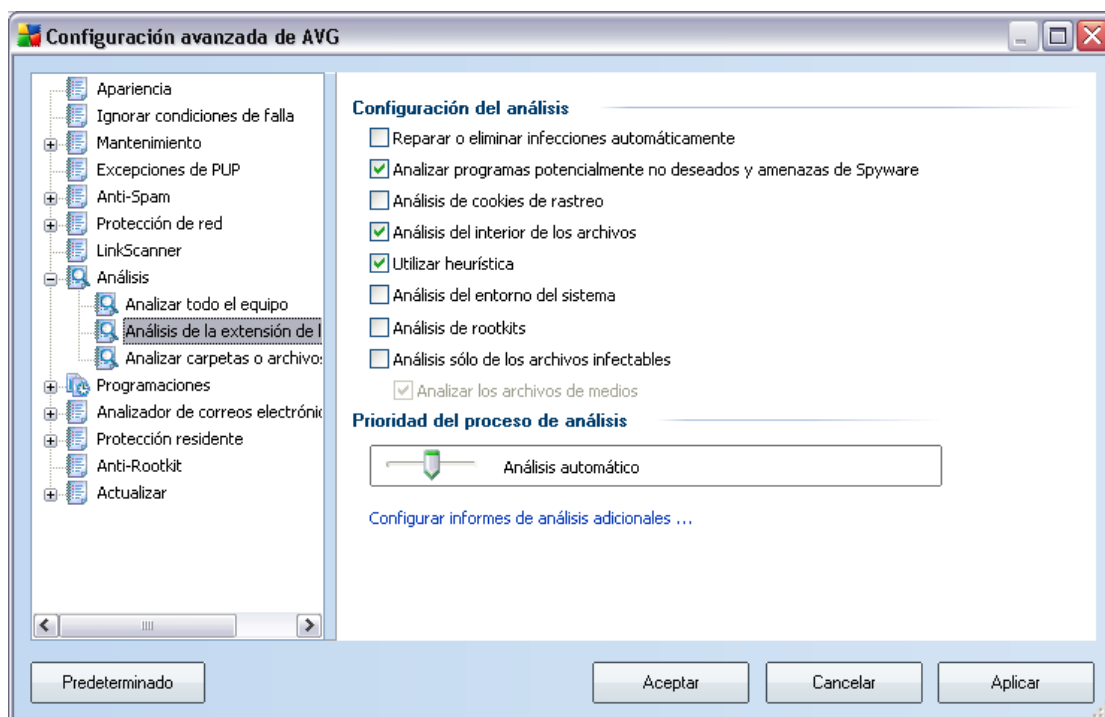
### Configurar informes de análisis adicionales ...

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:



#### 11.7.2. Análisis de extensión de la shell

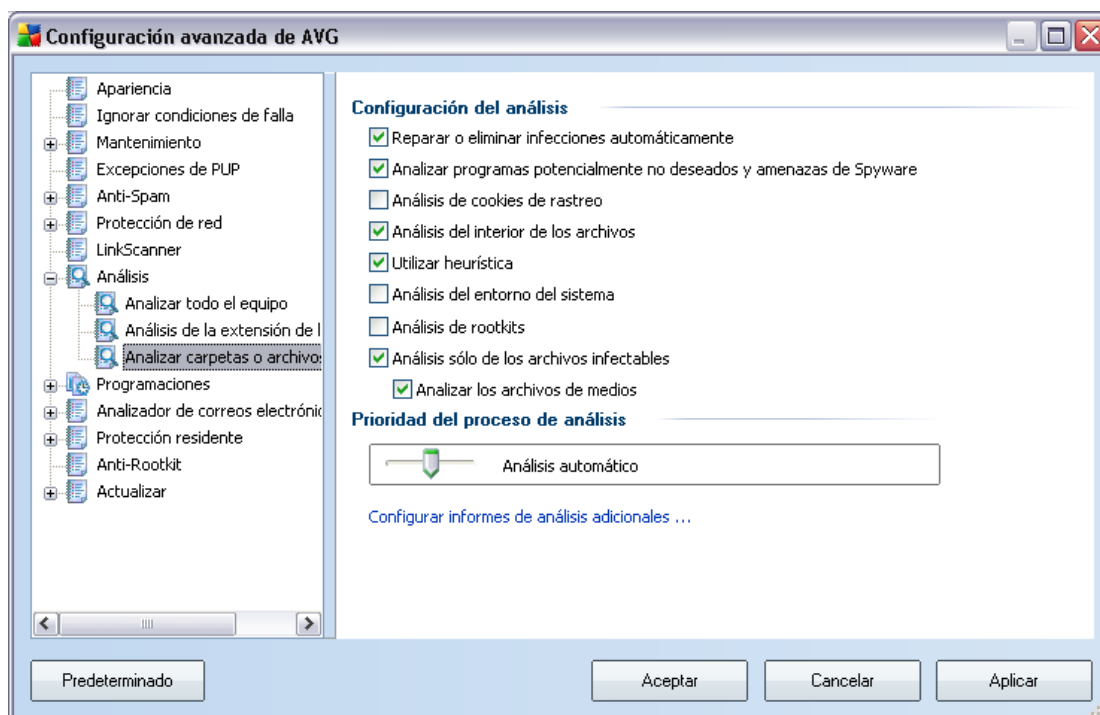
De modo parecido al anterior elemento [Analizar todo el equipo](#), este elemento denominado **Análisis de extensión de la shell** también ofrece varias opciones para editar el análisis predefinido por el proveedor de software. En esta ocasión, la configuración está relacionada con el [análisis de objetos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

### 11.7.3. 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](#):

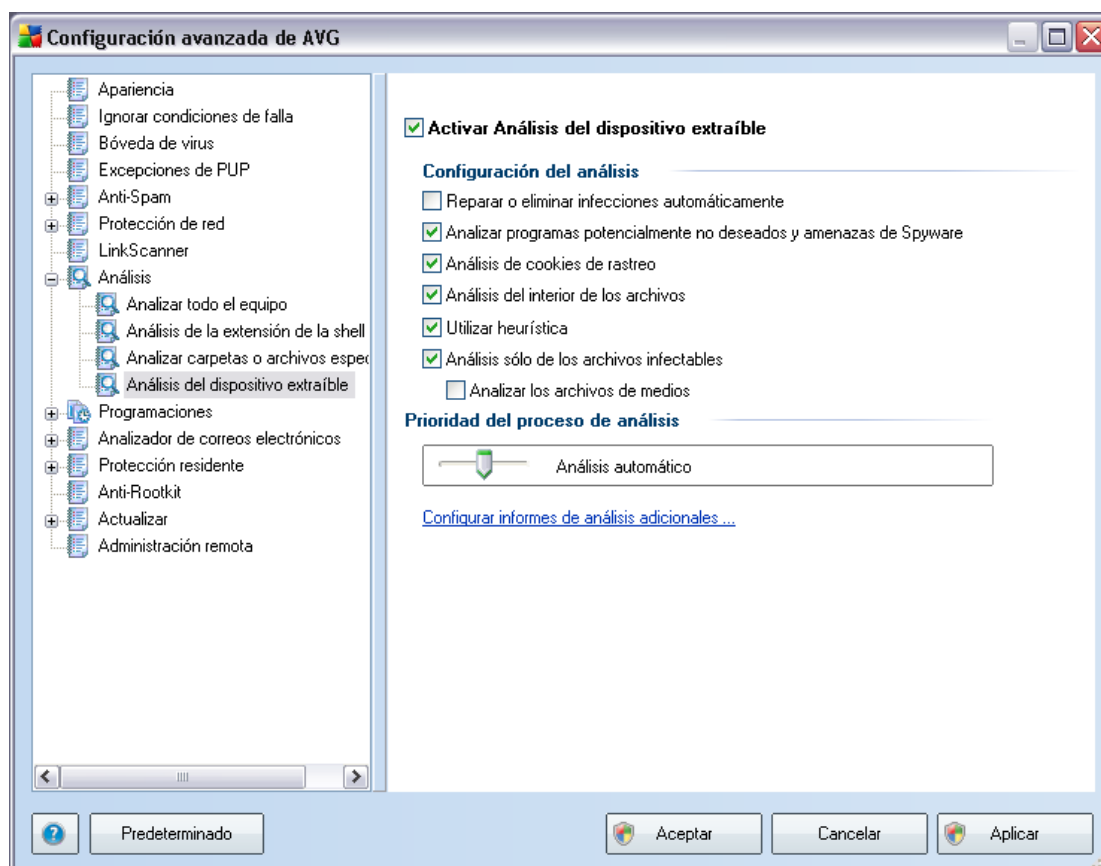


Todos los parámetros definidos en este diálogo de configuración se aplican únicamente a las áreas seleccionadas para el análisis con **Análisis de archivos o carpetas específicos**. Si marca la opción **Analizar en busca de rootkits** de este diálogo de configuración, sólo se llevará a cabo un análisis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

### 11.7.4. 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](#)



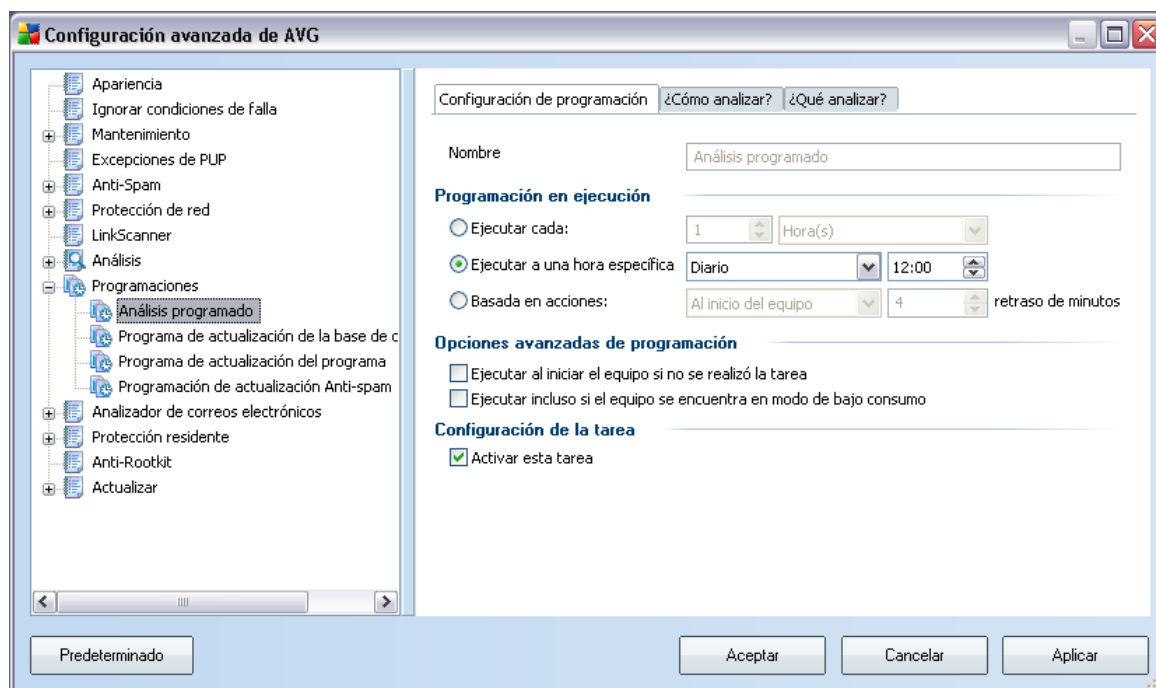
## 11.8. Programaciones

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](#)
- [Programación de actualización de Anti-Spam](#)

### 11.8.1. 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.

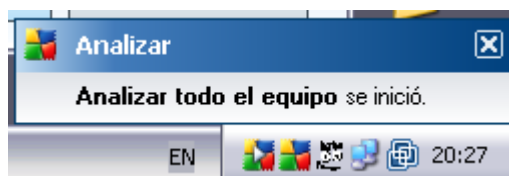
A continuación, dé un nombre al análisis que está a punto de crear y programar. Escriba el nombre en el campo de texto mediante el elemento **Nombre**. Intente utilizar nombres cortos, descriptivos y adecuados para los análisis a fin de distinguirlos después fácilmente.

**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](#).

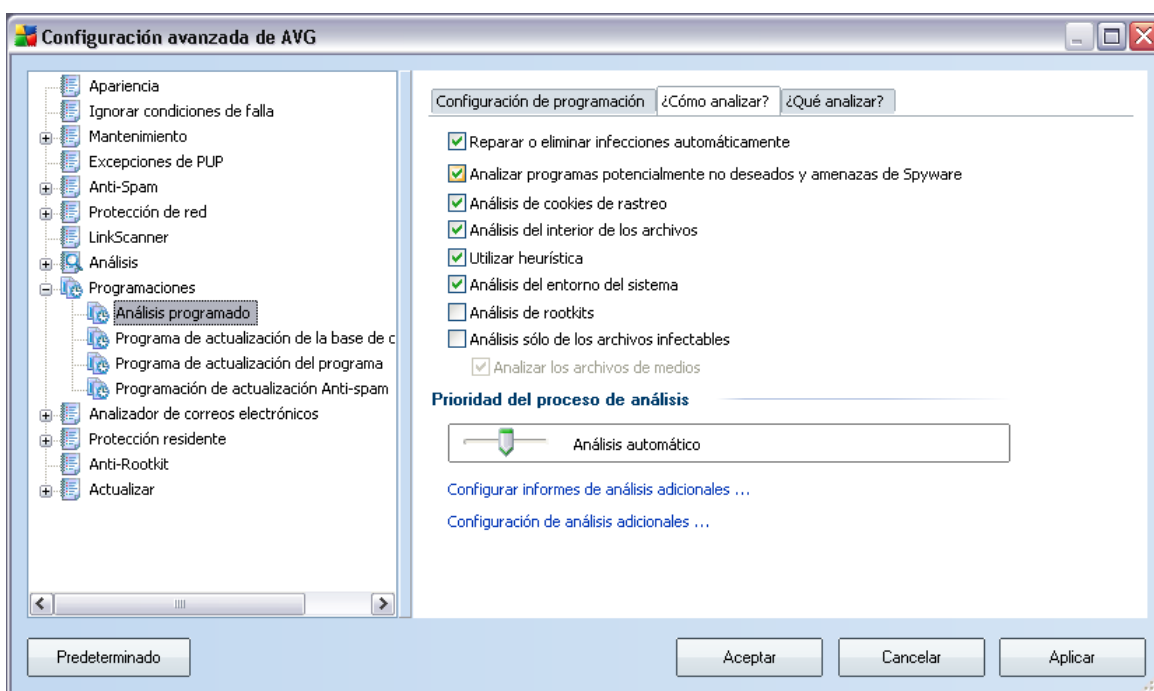
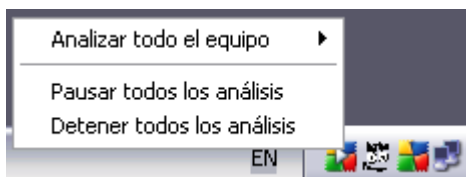
En este diálogo puede definir con más detalle los siguientes parámetros del análisis:

- **Ejecución de programación:** especifique los intervalos de tiempo de la ejecución de 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.

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:



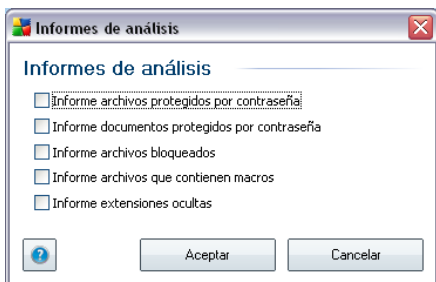
En la pestaña **Cómo analizar** se encontrará una lista de parámetros de análisis que de manera opcional se pueden activar/desactivar. De manera predeterminada, la mayoría de los parámetros están activados y su funcionamiento se aplicará durante el análisis. A menos que se cuente con una razón válida 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](#).

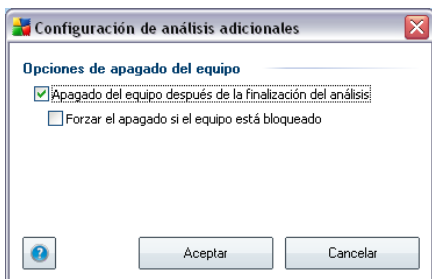
- **Analizar programas potencialmente no deseados:** (activado, de manera predeterminada): este parámetro controla la función [Anti-Virus](#) que permite [la detección, bloqueo y eliminación de archivos ejecutables de programas potencialmente no deseados](#) que se pueden ejecutar como spyware o adware ;
- **Analizar cookies :** (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](#);
- **Analizar sólo archivos infectables :** (desactivado, de manera predeterminada): con esta opción activada, no se analizarán los archivos que no se pueden infectar. Por ejemplo, algunos archivos de sólo texto o algún otro tipo de archivo no ejecutable.

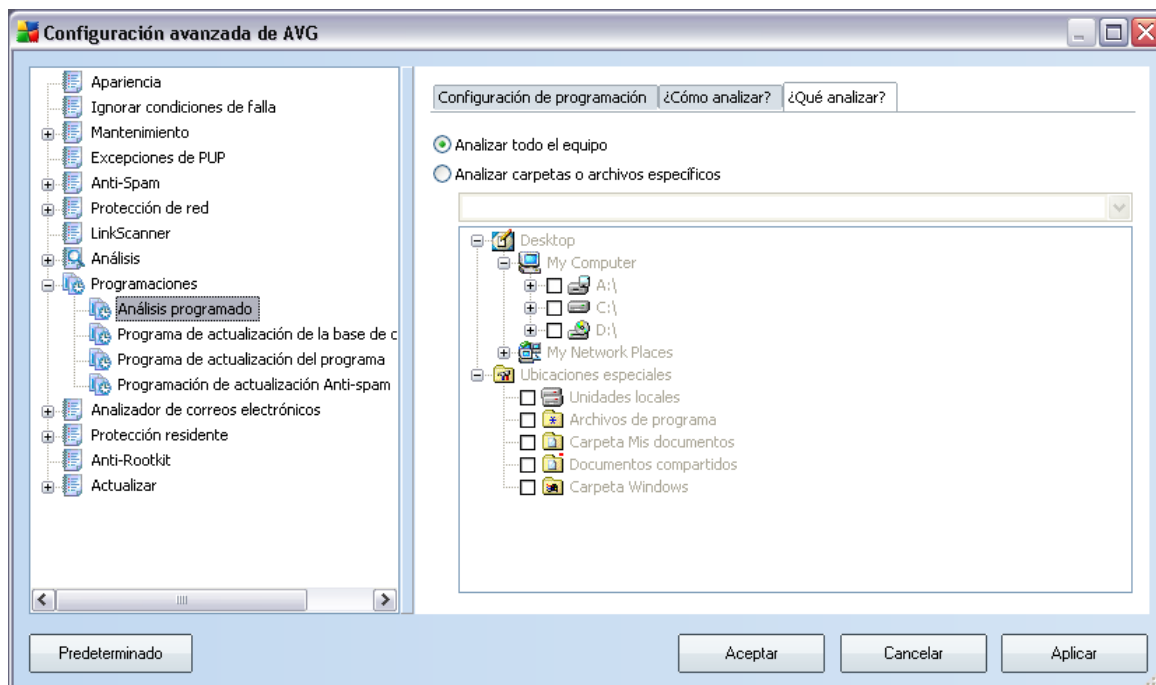
Dentro de la sección **Prioridad del proceso de análisis** se puede especificar de manera adicional la velocidad de análisis deseada dependiendo del empleo de recursos del sistema. De manera predeterminada, esta opción está establecida en el nivel medio de empleo automático de recursos. Si desea que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



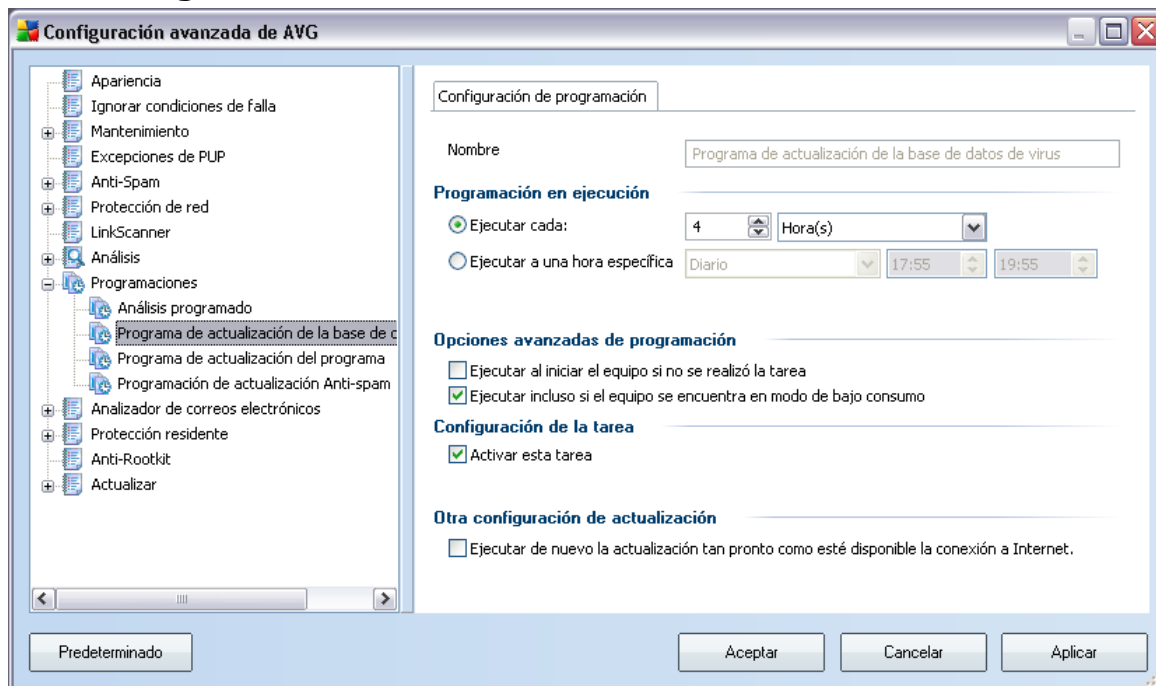
Haga clic en **Configuración de análisis adicional** para abrir un nuevo diálogo de **Opciones de apagado del equipo**, donde puede decidir si el equipo se debería apagar automáticamente en cuanto haya finalizado el proceso de análisis en ejecución. Después de haber confirmado esta opción (**Apagado 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.

## 11.8.2. 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:

Dé un nombre al programa de actualización de la base de datos de virus que está por crear. Escriba el nombre en el campo de texto mediante el elemento **Nombre**. Intente utilizar nombres de programaciones de actualización cortos, descriptivos y pertinentes para que posteriormente la programación se pueda distinguir con facilidad de las demás.

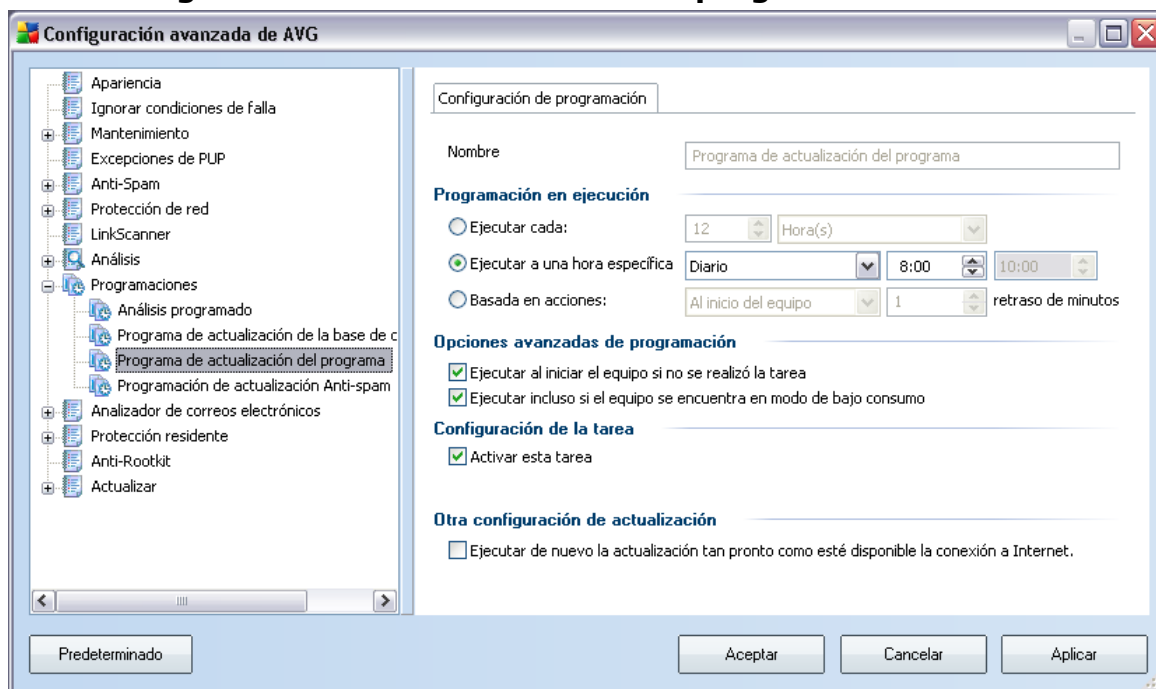
- **Ejecución de programación** - especifique los intervalos de tiempo para la ejecución de de la actualización recién programada de la Base de datos de virus. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto período de tiempo (**Ejecutar cada ...**) o definiendo 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 de programación avanzadas** : 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**: seleccione esta opción para asegurarse de que si la conexión a Internet se daña y el proceso de actualización falla, se volverá a ejecutar inmediatamente después de que se restaure la conexión a Internet.

Una vez que se inicia el análisis programado 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 diálogo ***Configuración avanzada/Apariencia***).

### 11.8.3. 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.

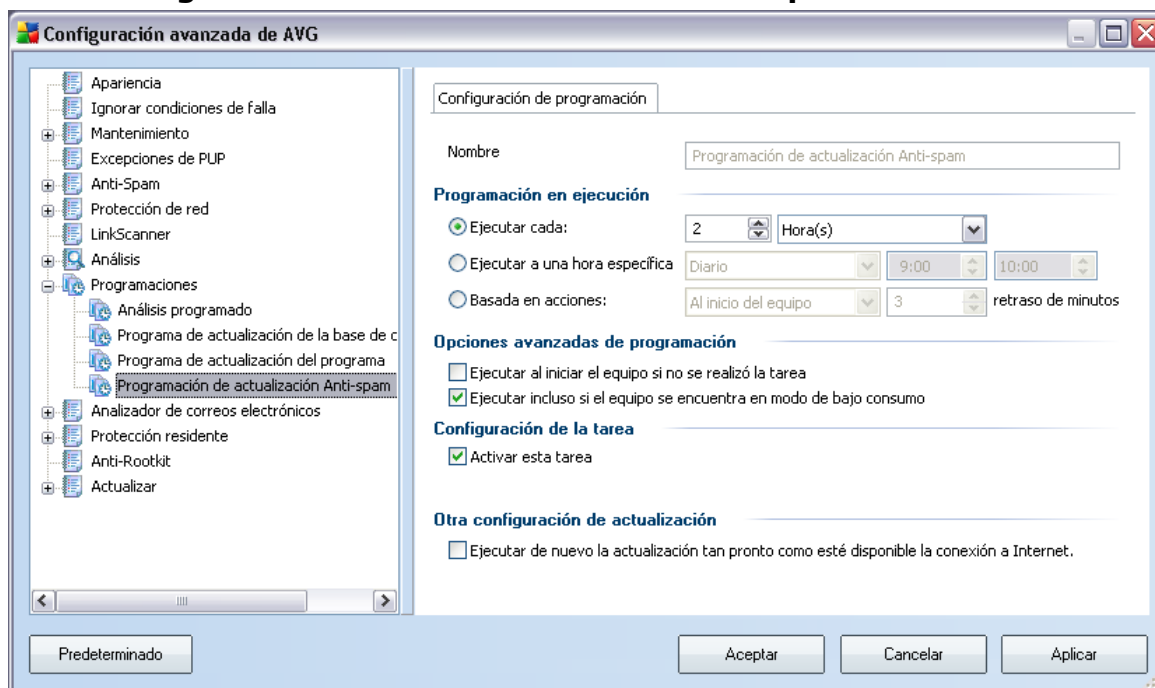


A continuación, dé un nombre al programa de actualización que está por crear. Escriba el nombre en el campo de texto mediante el elemento **Nombre**. Intente utilizar nombres de programaciones de actualización cortos, descriptivos y pertinentes para que posteriormente la programación se pueda distinguir con facilidad de las demás.

- **Ejecución de programación**: especifique los intervalos de tiempo de la ejecución de análisis recién programada. El tiempo se puede definir con la ejecución repetida de la actualización después de un cierto período 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 de programación avanzada** : 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 esta opción para asegurarse de que si la conexión a Internet se daña y el proceso de actualización falla, se volverá a ejecutar inmediatamente después de que se restaure la conexión a Internet.

Una vez que se inicia el análisis programado 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 diálogo **Configuración avanzada/Apariencia**).

## 11.8.4. Programación de actualización de Anti-Spam



En la pestaña **Configuración de programación** puede seleccionar o cancelar la selección del elemento **Activar esta tarea** simplemente para desactivar temporalmente la actualización programada del **Anti-Spam** y volver a activarla cuando sea necesario.

La programación de actualización básica del **Anti-Spam** está formado por el componente **Administrador de actualizaciones**. En este diálogo puede configurar algunos parámetros detallados de la programación de actualización:

A continuación, dé un nombre al programa de actualización de **Anti-Spam** que está por crear. Escriba el nombre en el campo de texto mediante el elemento **Nombre**. Intente utilizar nombres de programaciones de actualización cortos, descriptivos y pertinentes para que posteriormente la programación se pueda distinguir con facilidad de las demás.

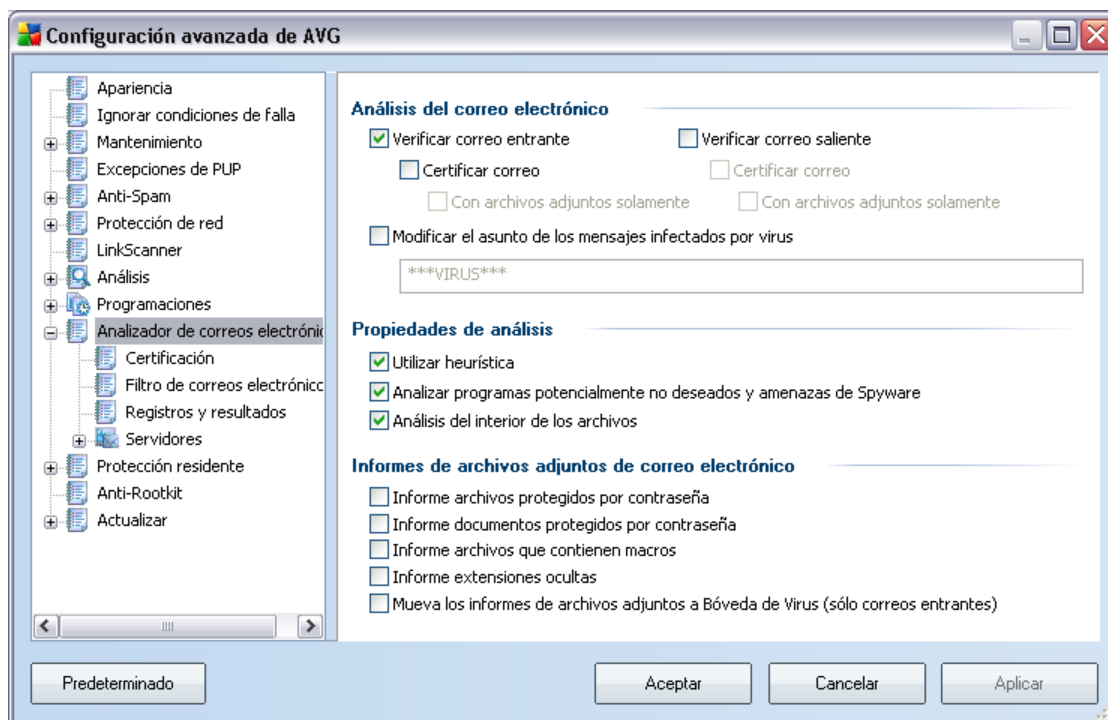
- **Ejecución de programación:** especifique los intervalos de tiempo de la actualización recién programada del **Anti-Spam**. El tiempo se puede definir con la ejecución repetida de la actualización del **Anti-Spam** tras un período de tiempo determinado (**Ejecutar cada...**), estableciendo una fecha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

*basada en el inicio del equipo).*

- **Opciones de programa avanzadas:** esta sección permite definir en qué condiciones debe o no ejecutarse la actualización del **Anti-Spam** si el equipo se encuentra en modo de alimentación baja o totalmente apagado.
- **Configuración de la tarea:** en esta sección puede cancelar la selección del elemento **Activar esta tarea** simplemente para desactivar la actualización programada temporalmente del **Anti-Spam** y volver a activarla cuando sea necesario.
- **Otra configuración de actualización:** seleccione esta opción para asegurarse de que si la conexión a Internet está dañada y el proceso de actualización del **Anti-Spam** falla, se volverá a ejecutar inmediatamente después de que se restaure la conexión a Internet.

Una vez que se inicia el análisis programado 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 diálogo **Configuración avanzada/Apariencia**).

## 11.9. Analizador de correos electrónicos

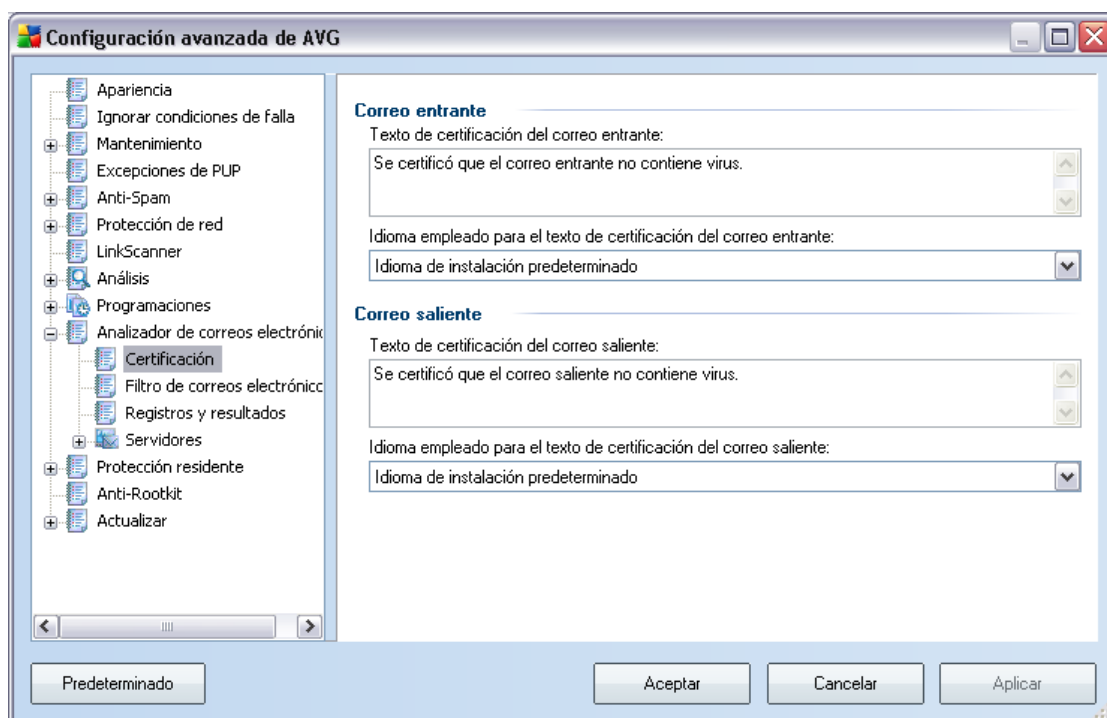


El diálogo **Analizador de correos electrónicos** se divide en tres secciones:

- **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](#) (**Analizar programas potencialmente no deseados**), y si también se deben analizar los archivos (**Análisis del interior de los archivos**).
- **Informes de archivos adjuntos de correo electrónico**: especifique si

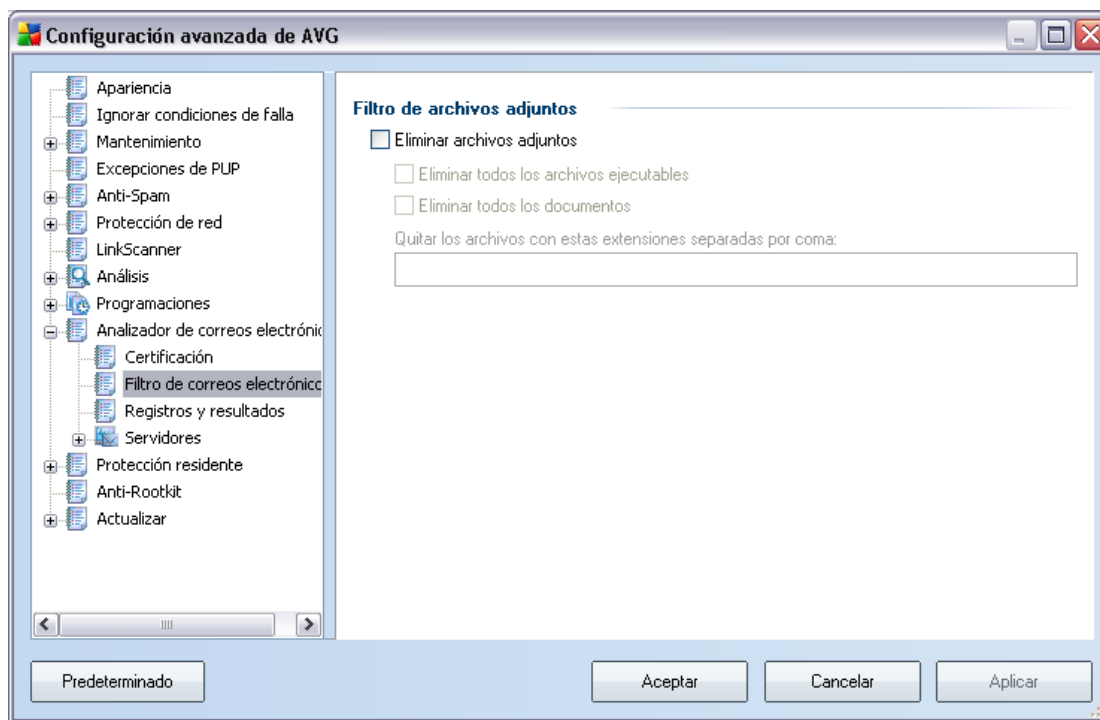
desea que se le notifique mediante correo electrónico acerca de los archivos protegidos con contraseña, los documentos protegidos con contraseña, los archivos que contienen macros y los archivos con extensión oculta detectados como un dato adjunto del mensaje del correo electrónico analizado. Si durante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

### 11.9.1. 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***.

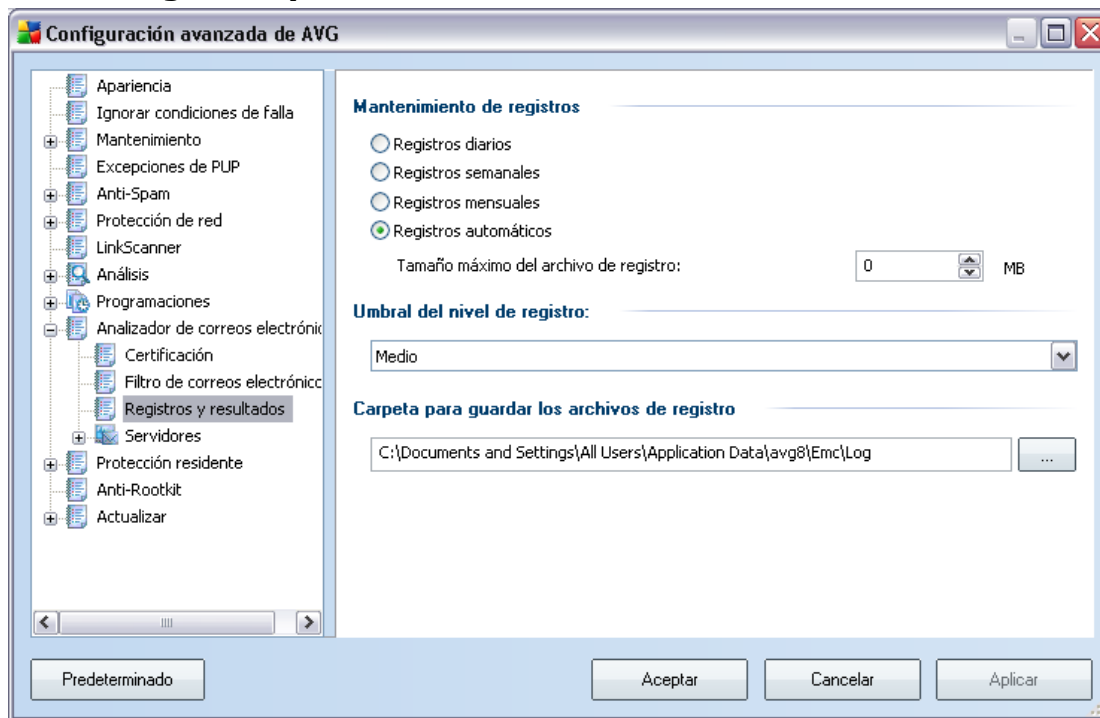
## 11.9.2. Filtro de correos electrónicos



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
- **Quitar archivos con las siguientes extensiones:** se eliminarán todos los archivos con las extensiones definidas

### 11.9.3.Registros y resultados

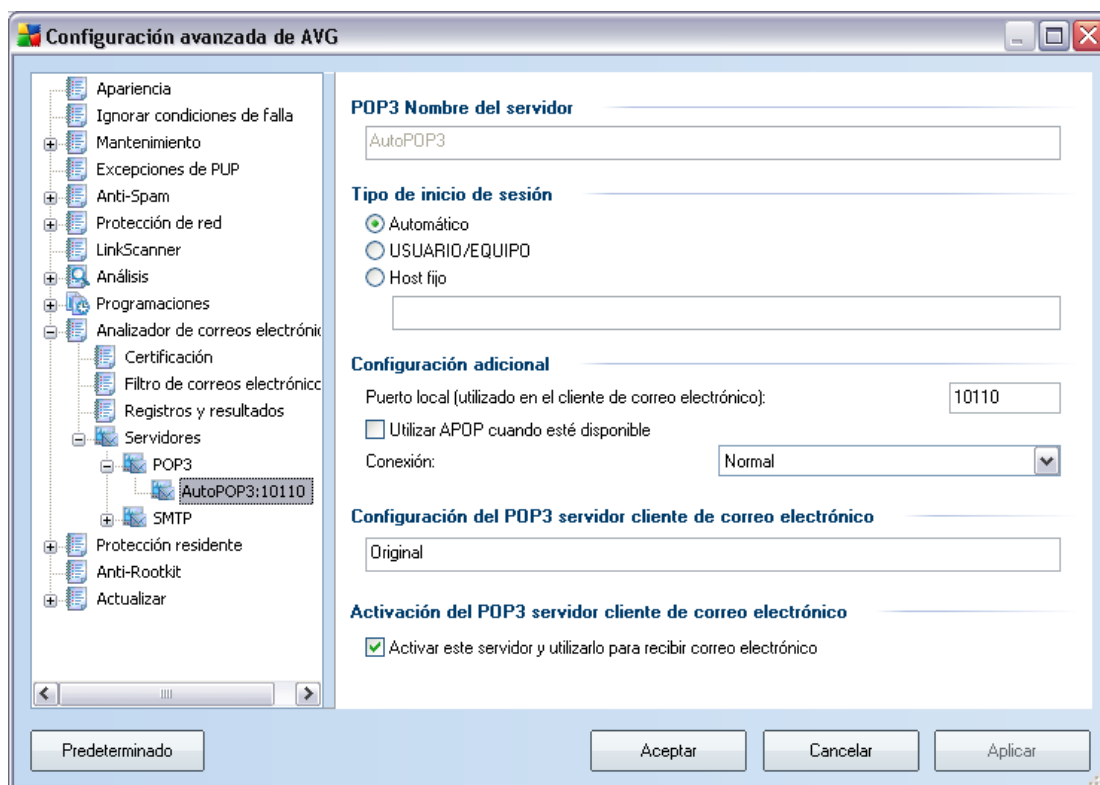


El diálogo abierto mediante el elemento de navegación **Registros y resultados** permite especificar los parámetros para el mantenimiento de los resultados del análisis de los correos electrónicos. El diálogo se divide en varias secciones:

- **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

### 11.9.4. 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.



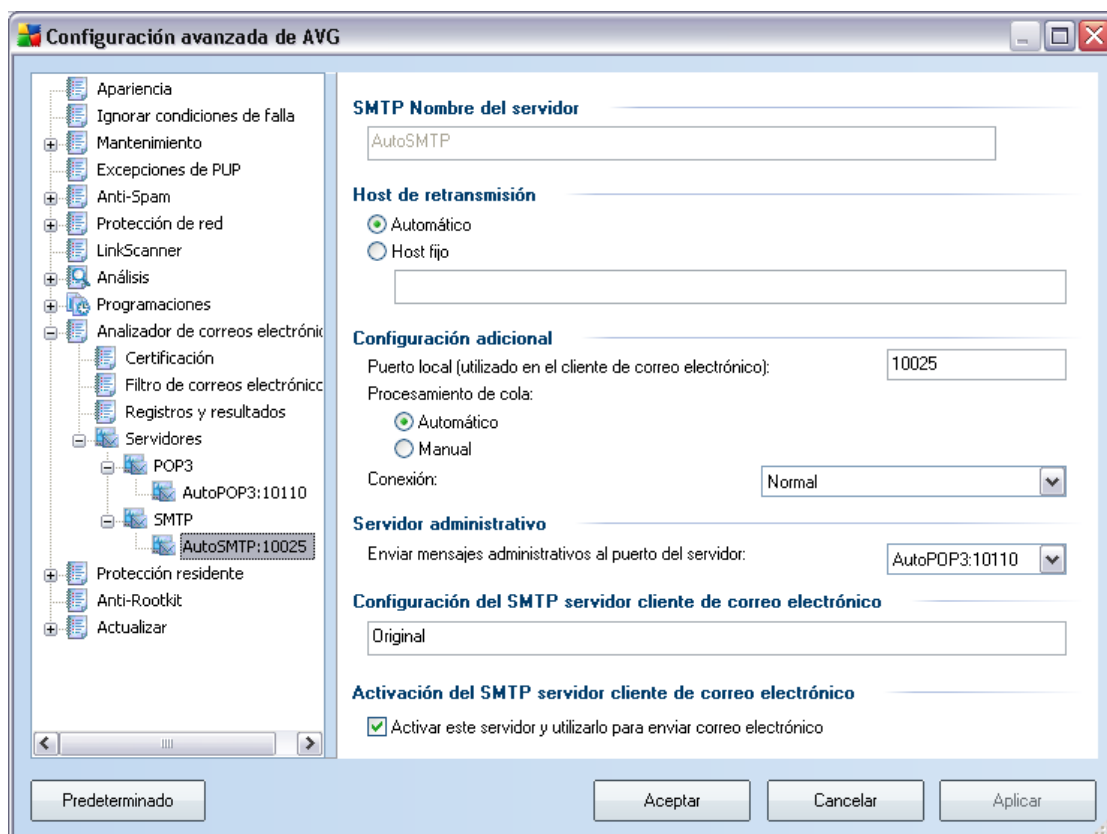
- USUARIO/EQUIPO: el método más simple y más frecuente para determinar el servidor de correo de destino es el método proxy. Para utilizar este método, especifique el nombre o la dirección (o también el puerto) como parte del nombre de usuario de inicio de sesión para el servidor de correo dado, separándolos 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 la opción APOP cuando se encuentre disponible: esta opción proporciona un inicio de sesión del servidor de correo más segura. 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.



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.

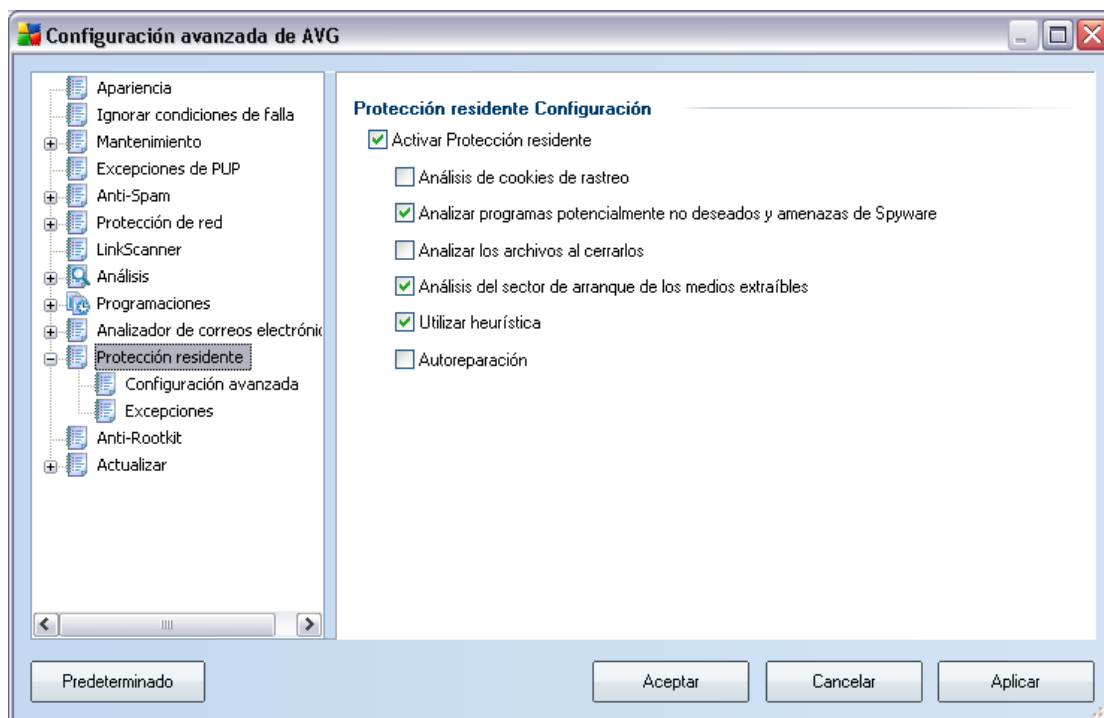
- Servidor fijo: en este caso, el programa siempre usará el servidor especificado en este campo. Especifique la dirección o el nombre de su servidor de correo. Como nombre, puede utilizar un nombre de dominio (por ejemplo, smtp.acme.com) así como también una dirección IP (por ejemplo, 123.45.67.89). 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.

## 11.1(Protección residente

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



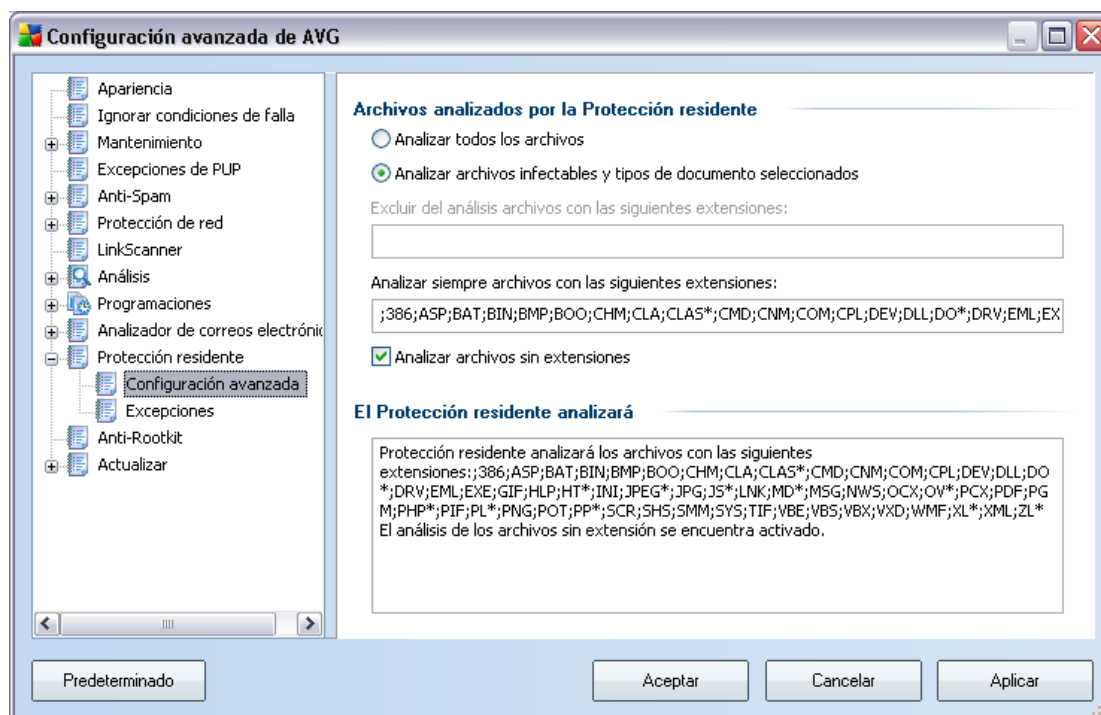
En el diálogo **Configuración de Protección residente** puede activar o desactivar la **Protección residente** por completo seleccionando o deseleccionando el elemento **Activar Protección residente** (esta opción está seleccionada de modo predeterminado). También puede seleccionar las funciones de **Protección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

- **Analizar cookies:** este parámetro define qué cookies deben detectarse 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:** (opción seleccionada de modo predeterminado) analiza los [programas potencialmente no deseados](#) (aplicaciones ejecutables que pueden actuar como diversos tipos de spyware o adware).

- **Analizar al cerrar proceso:** el análisis al cerrar garantiza que el programa AVG analiza los objetos activos (por ejemplo, aplicaciones, documentos...) 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.

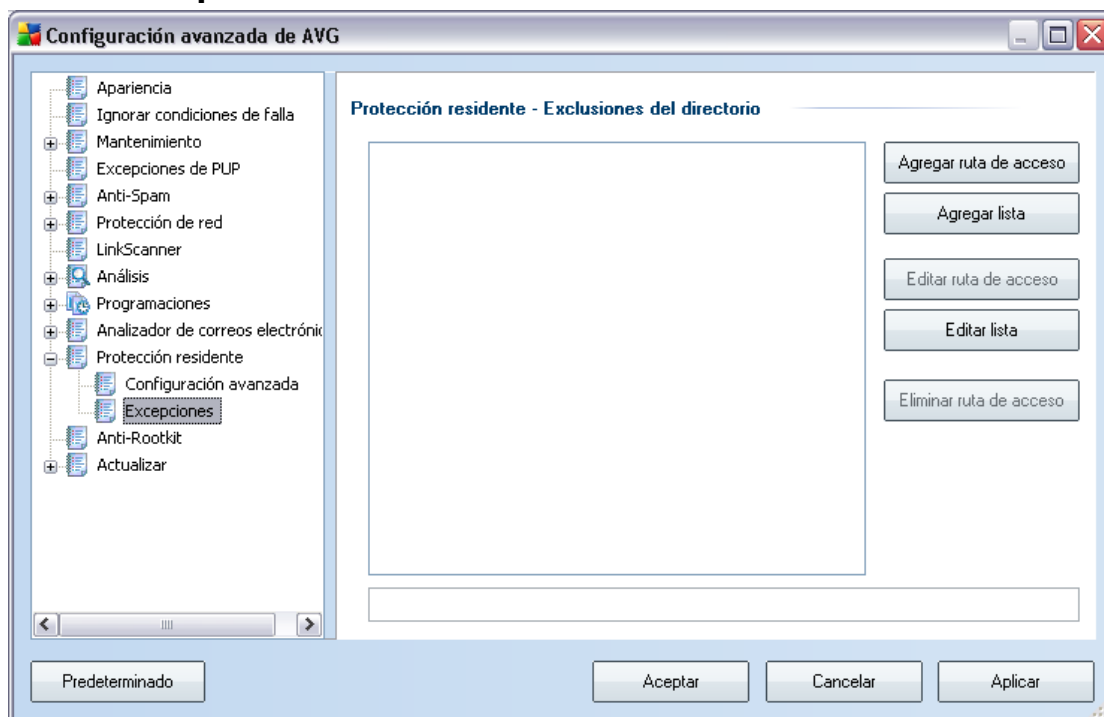
## 11.10. Configuración avanzada

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.

## 11.10. Excepciones



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. Si decide excluir una carpeta del análisis de la **Protección residente**, la nueva configuración sólo tendrá efecto después de reiniciar el equipo

El diálogo proporciona los siguientes botones de control:

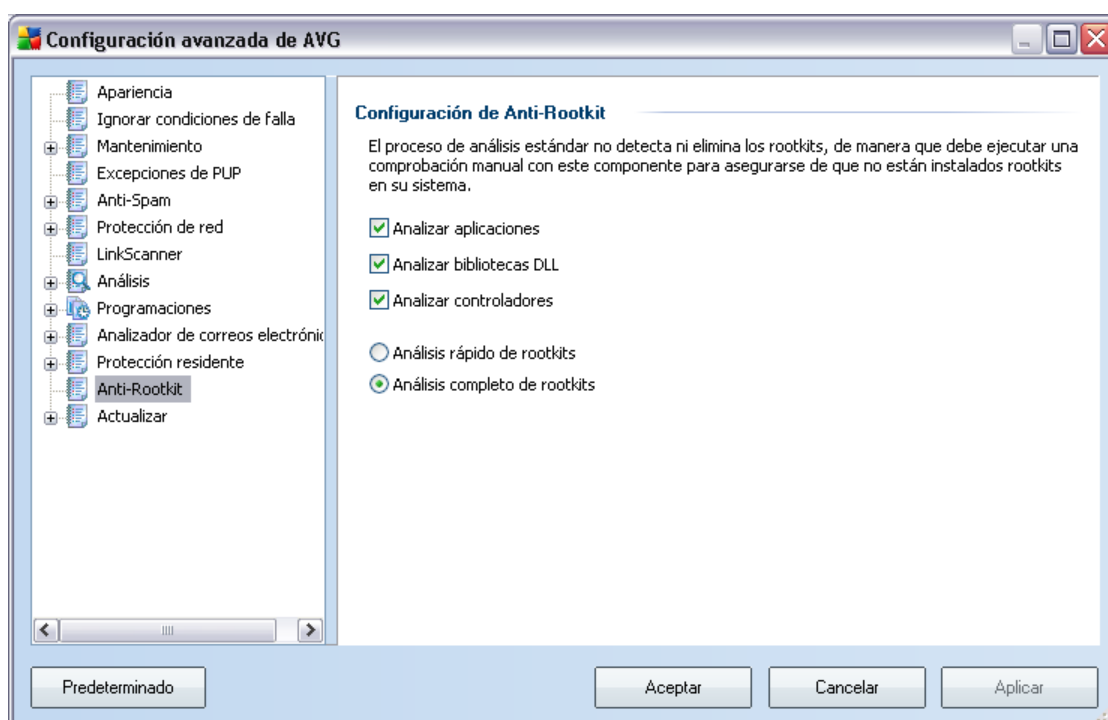
- **Agregar ruta** : especifica los directorios que deben excluirse del análisis seleccionándolos uno por uno desde el árbol de navegación del disco local.
- **Agregar lista** : le permite introducir una lista completa de directorios que desea excluir del análisis de la **Protección residente**
- **Editar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

### 11.1 Anti-Rootkit

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



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

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

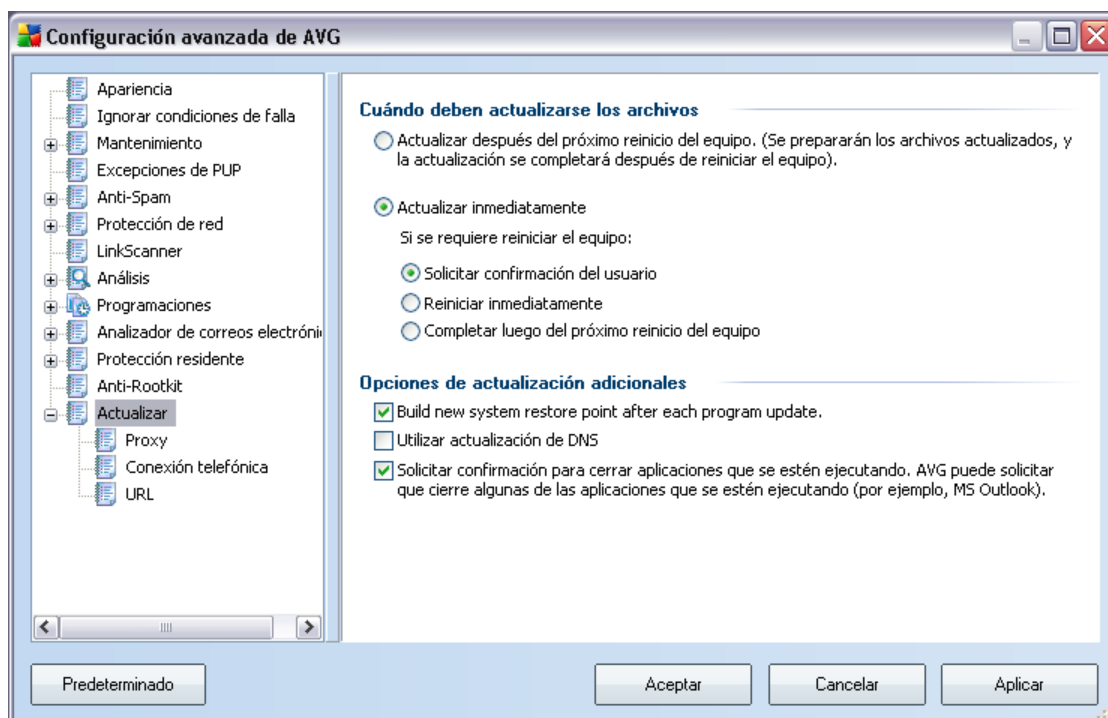
- **Analizar aplicaciones**
- **Analizar bibliotecas DLL**

- **Analizar controladores**

También puede seleccionar el modo de análisis de rootkits:

- **Análisis de rootkits rápido:** sólo analiza la carpeta del sistema (normalmente, *c:\Windows*).
- **Análisis de rootkits completo:** analiza todos los discos disponibles excepto A: y B:.

## 11.1 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.

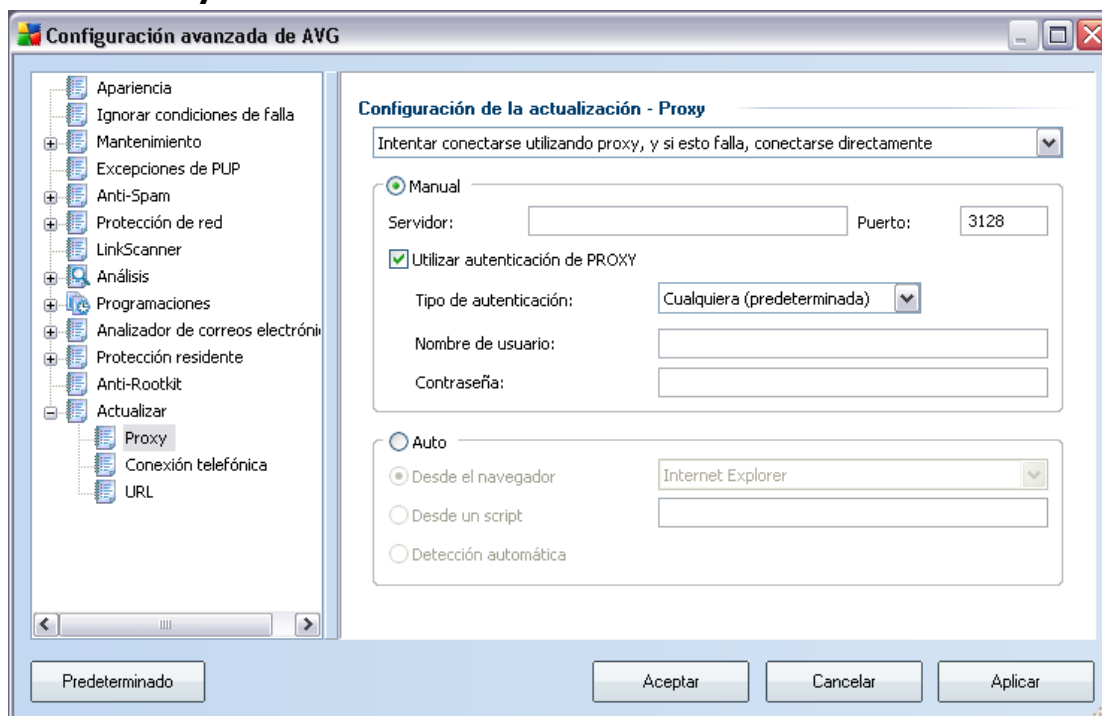
- **Solicitar confirmación del usuario:** se le pedirá que apruebe un reinicio del equipo, necesario para finalizar el [proceso de actualización](#)
- **Reiniciar inmediatamente:** el equipo se reiniciará inmediatamente de forma automática después de que el [proceso de actualización](#) haya finalizado, 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.

### 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 manera predeterminada) estará seguro 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.

## 11.12. 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*).

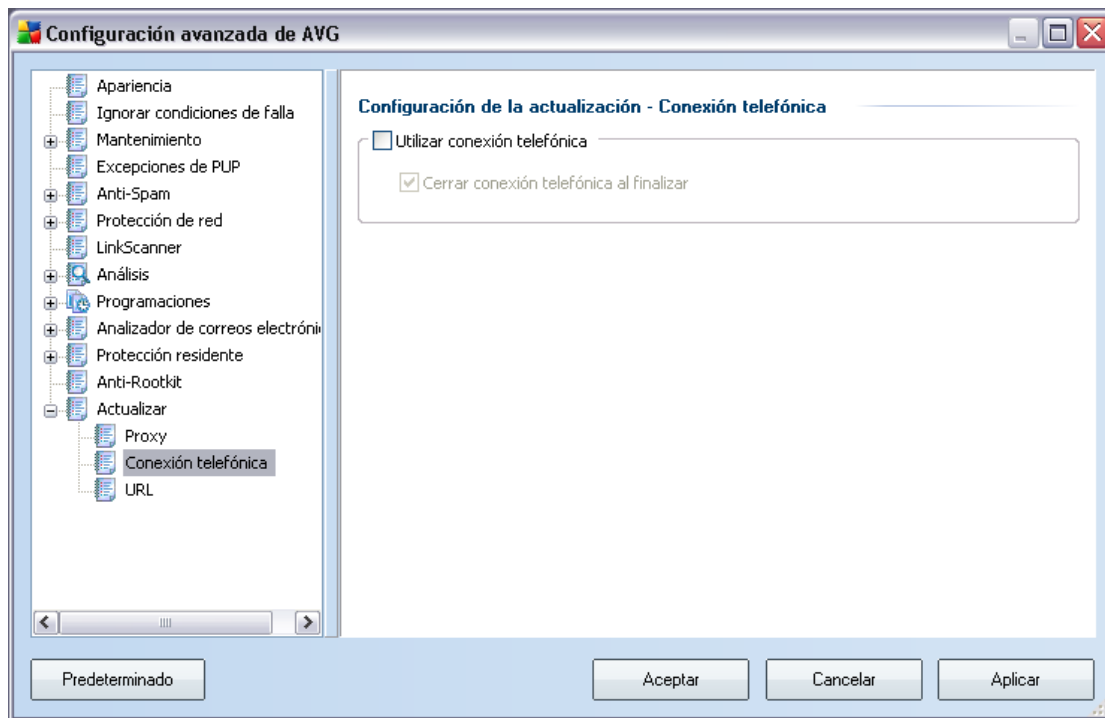
El servidor proxy también puede tener reglas específicas configuradas para cada usuario. Si el servidor proxy está configurado de este modo, seleccione la opción **Utilizar autenticación de PROXY** para verificar que el nombre de usuario y la contraseña sean válidos para la conexión a Internet mediante 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 explorador**: la configuración se leerá del explorador de Internet predeterminado (*los exploradores permitidos son Internet Explorer, Firefox, Mozilla y Opera*).
- **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

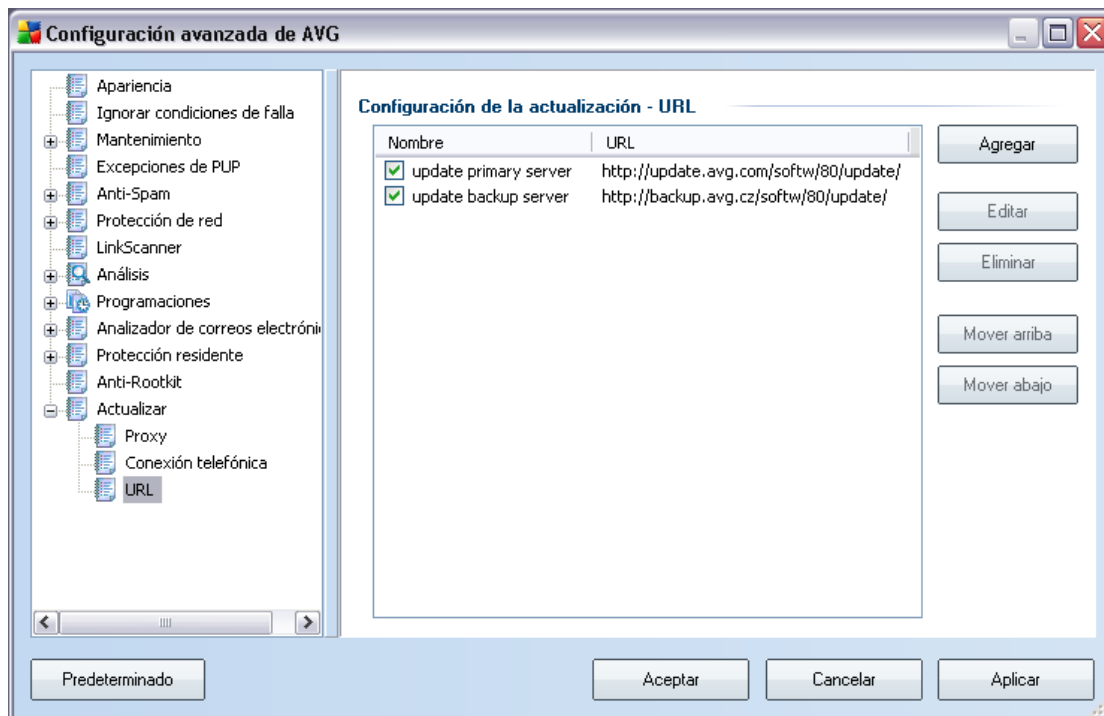
## 11.12. Conexión telefónica



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**).

## 11.12. 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.
- **Predeterminado**: permite volver a la lista predeterminada de URL.
- **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.

### 11.12. Administrar

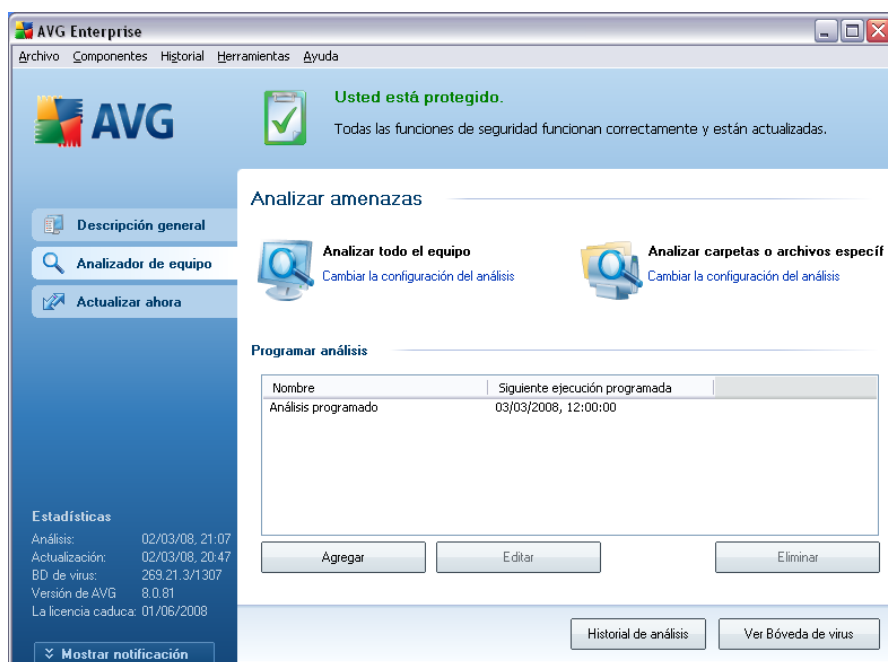
El diálogo **Administrar** ofrece dos opciones accesibles mediante dos botones:

- **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*).

## 12. Análisis de AVG

El análisis es una parte crucial de la funcionalidad de **Anti-Virus AVG 8.5**. Puede realizar análisis a petición o [programarlos para que se ejecuten periódicamente](#) en los momentos apropiados.

### 12.1. Interfaz de análisis



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

- Vista general de los [análisis predefinidos](#): hay dos tipos de análisis (definidos por el proveedor de software) preparados para su uso inmediato a pedido o programados;
- [Sección de programación de análisis](#): en ella puede definir nuevos análisis y crear nuevas programaciones según convenga.

### Botones de control

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

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

## 12.2. Análisis predefinidos

Una de las funciones principales de AVG 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 8.5** encontrará dos tipos de análisis predefinidos por el proveedor del software:

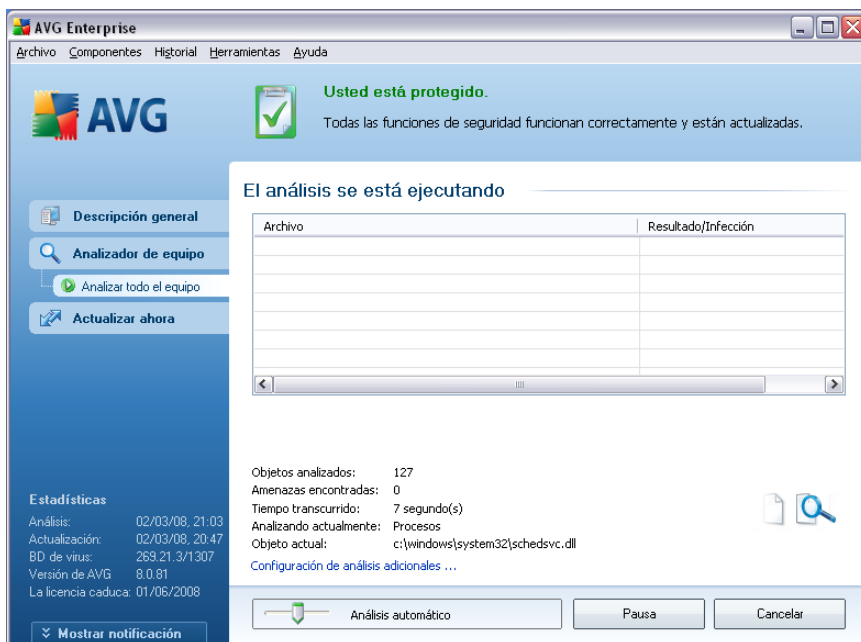
### 12.2.1. Analizar todo el equipo

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

### Ejecución de análisis

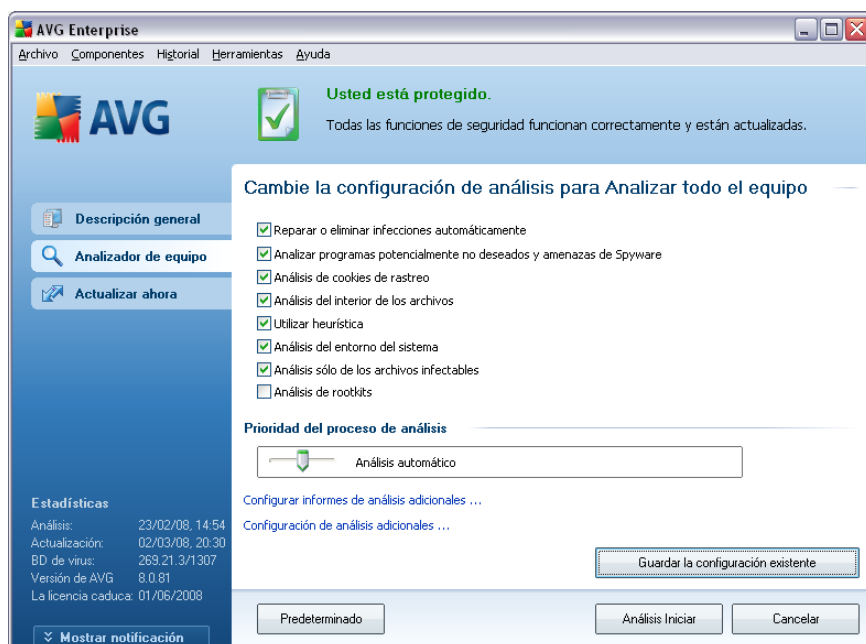
El **análisis de un equipo completo** se puede ejecutar directamente desde la [interfaz de análisis](#) haciendo clic en el icono de análisis. No se deben configurar más parámetros específicos para este tipo de análisis; el análisis empezará inmediatamente en el diálogo **Se está ejecutando el análisis**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



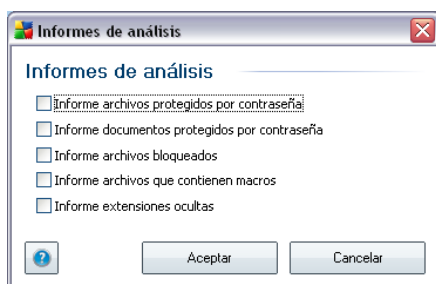


## Edición de la configuración de análisis

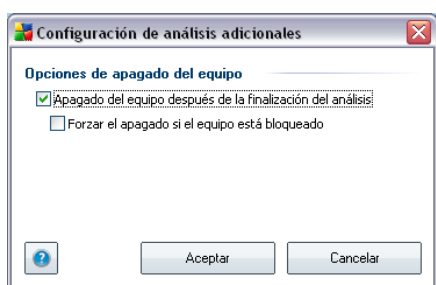
Tiene la opción de editar la configuración predeterminada predefinida de **Análisis de todo el equipo**. Presione el vínculo **Cambiar la configuración del análisis** para ir al diálogo **Cambiar configuración del análisis de todo el equipo**. **Se recomienda mantener la configuración predeterminada 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.
- **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:



- **Configuración de análisis adicional:** el vínculo abre 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**).



**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.

### 12.2.2. Analizar carpetas o archivos específicos

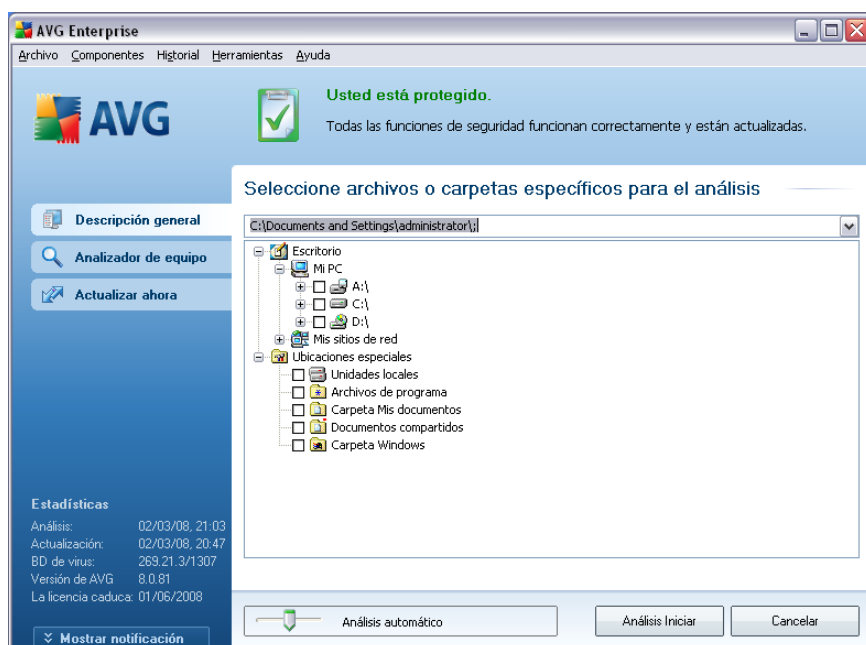
**Analizar archivos o carpetas específicos:** analiza únicamente las áreas del equipo que ha seleccionado que se analicen (carpetas, discos duros, discos flexibles, CD... concretos). El procedimiento de análisis en caso de detección de virus y su tratamiento es el mismo que se realiza con el análisis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

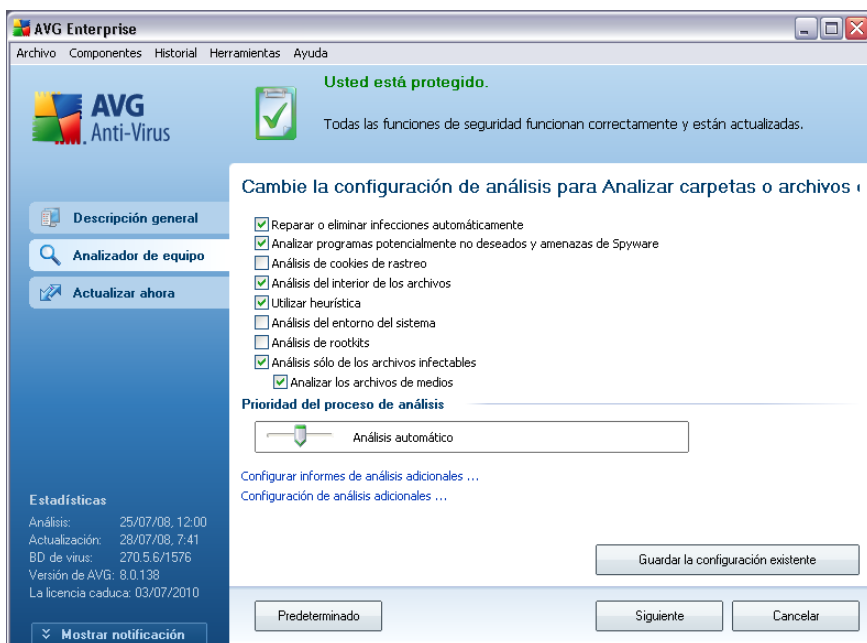
Finalmente, para iniciar el análisis, presione el botón **Iniciar análisis**; el proceso de análisis es básicamente idéntico al [análisis de todo un equipo](#).



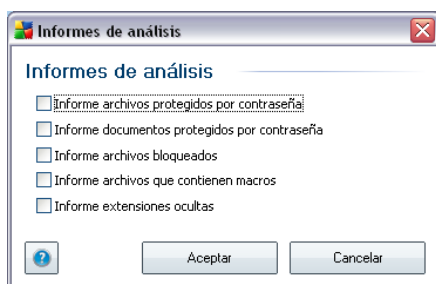
## Edición de la configuración de análisis

Tiene la opción de editar la configuración predeterminada predefinida de **Análisis de archivos o carpetas específicos**. Presione el vínculo **Cambiar la configuración**

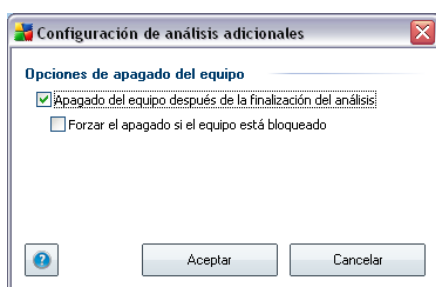
**del análisis** para ir al diálogo **Cambiar configuración de análisis de archivos o carpetas específicos**. **Se recomienda mantener la configuración predeterminada salvo que exista un motivo válido para cambiarla.**



- **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](#)*.
- **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:



- **Configuración de análisis adicional:** el vínculo abre 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**).



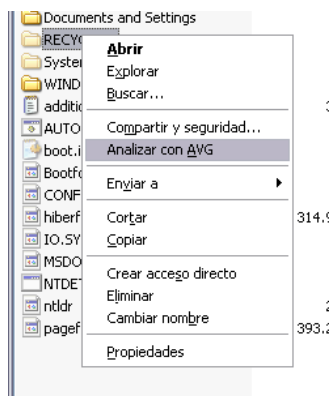
**Advertencia:** estos parámetros de análisis son idénticos a los de un nuevo análisis definido, tal como se describe en el capítulo [Análisis de AVG/Programación de análisis/Cómo analizar](#).

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](#)).

### 12.3. Análisis en el Explorador de Windows

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

estos pasos:



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

## 12.4. Análisis de línea de comandos

En **Anti-Virus AVG 8.5** 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, pulse **Intro**. Durante el análisis, puede detener el proceso mediante **Ctrl+C** o **Ctrl+Pausa**.

### Análisis de CMD iniciado desde la interfaz gráfica

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

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

#### 12.4.1. Parámetros del análisis de CMD

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

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



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

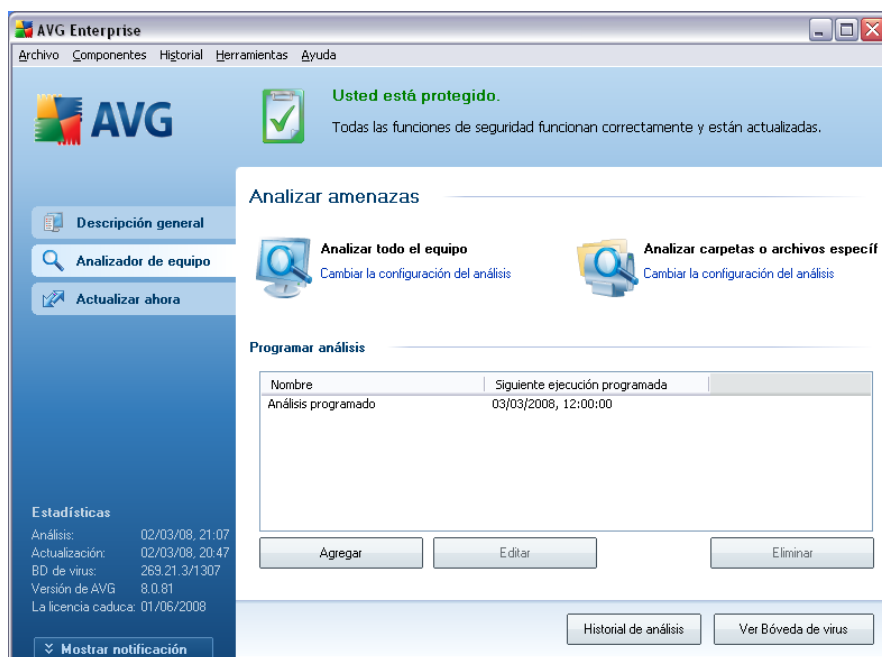
- **/HELP** Visualizar ayuda sobre este tema
- **/PRIORITY** Establecer prioridad de análisis/Baja, Automática, Alta/  
(consulte [Configuración avanzada/Análisis](#))
- **/SHUTDOWN** Apagado del equipo después de la finalización del análisis
- **/FORCESHUTDOWN** Forzar el apagado del equipo tras la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

## 12.5.Programación de análisis

Con **Anti-Virus AVG 8.5** 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**:



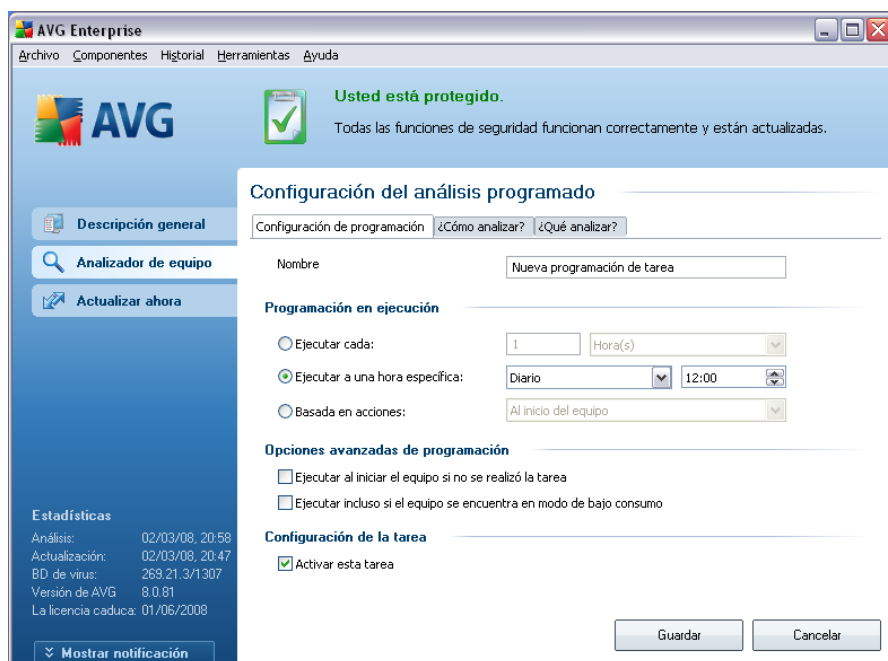
## Botones de control de programación de análisis

Dentro de la sección de edición puede encontrar 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.

### 12.5.1. Configuración de programación

Si desea programar un nuevo análisis y su ejecución periódica, utilice el diálogo **Configuración del análisis programado**. El diálogo está dividido en tres pestañas: **Configuración de programación**: consulte la imagen siguiente (la pestaña predeterminada a la que se le enviará automáticamente), [¿Cómo analizar?](#) y [¿Qué analizar?](#).



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

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

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

[carpetas seleccionados.](#)

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

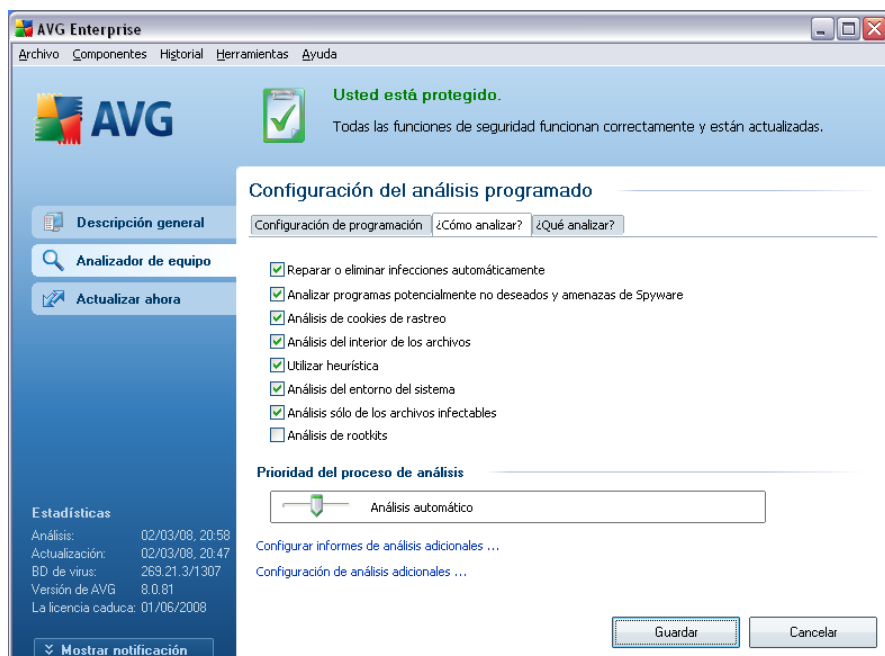
- **Ejecución de la programación:** especifique los intervalos de tiempo de la ejecución del análisis recién programada. El tiempo se puede definir con la ejecución repetida del análisis tras un período de tiempo determinado (**Ejecutar cada...**), estableciendo una fecha y una hora exactas (**Ejecutar en un momento específico...**) o estableciendo un evento al que debe estar asociada la ejecución de análisis (**Acción basada en el inicio del equipo**).
- **Opciones de programación avanzada:** esta sección permite definir en qué condiciones debe o no ejecutarse el análisis si el equipo se encuentra en modo de alimentación baja o totalmente apagado.

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

Hay dos botones de control en cada una de las tres pestañas del 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](#).

## 12.5.2. Cómo analizar



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

- **Reparar o eliminar infecciones automáticamente:** *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** (*activado, de manera predeterminada*): este parámetro controla la función [Anti-Virus](#) que permite [la detección, bloqueo y eliminación de archivos ejecutables de programas potencialmente no deseados](#) que se pueden ejecutar como spyware o adware ;
- **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, 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;
- **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**;
- **Analizar sólo archivos infectables** :(*desactivado, de manera predeterminada*): con esta opción activada, no se analizarán los archivos que no se pueden infectar. Por ejemplo, algunos archivos de sólo texto o algún otro tipo de archivo no ejecutable.

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.

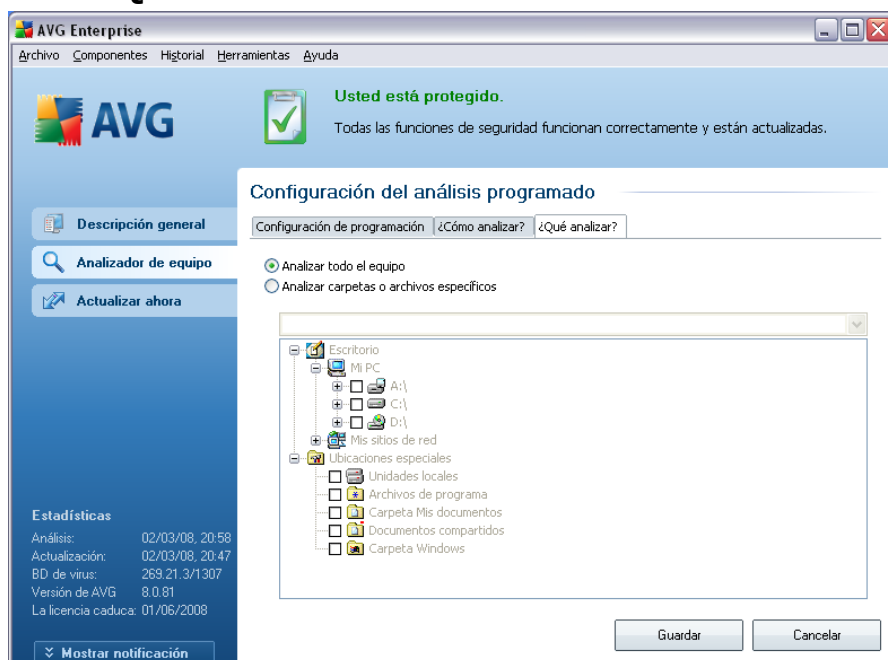
**Nota:** *de manera predeterminada, la configuración del análisis está programado para un rendimiento óptimo. A menos que se tenga una razón válida para cambiar la configuración del análisis, se recomienda encarecidamente que se mantenga la configuración predefinida. Sólo los usuarios experimentados 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 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](#).

### 12.5.3. Qué analizar



En la pestaña **Qué analizar** puede definir si desea programar el [análisis de todo el equipo](#) o el [análisis de archivos o carpetas específicos](#). Si selecciona analizar archivos o carpetas específicos, en la parte inferior de este diálogo se activará la estructura de



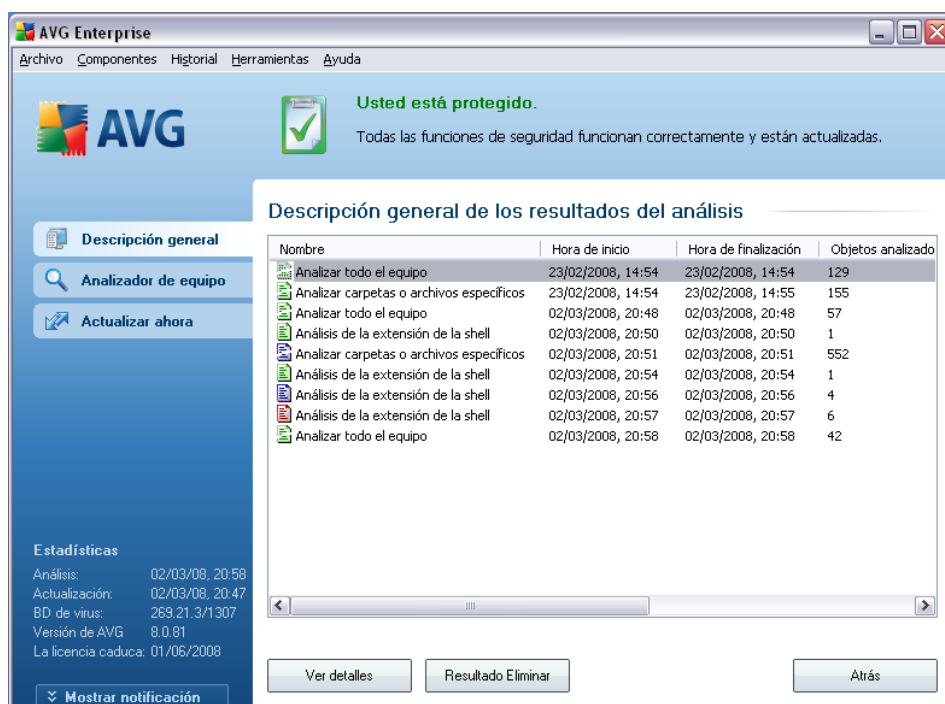
árbol visualizada y podrá especificar las carpetas que se analizarán.

### 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](#).

## 12.6.Descripción general de los resultados del análisis



Usted está protegido.  
Todas las funciones de seguridad funcionan correctamente y están actualizadas.

Descripción general de los resultados del análisis

Nombre	Hora de inicio	Hora de finalización	Objetos analizado
Analizar todo el equipo	23/02/2008, 14:54	23/02/2008, 14:54	129
Analizar carpetas o archivos específicos	23/02/2008, 14:54	23/02/2008, 14:55	155
Analizar todo el equipo	02/03/2008, 20:48	02/03/2008, 20:48	57
Análisis de la extensión de la shell	02/03/2008, 20:50	02/03/2008, 20:50	1
Analizar carpetas o archivos específicos	02/03/2008, 20:51	02/03/2008, 20:51	552
Análisis de la extensión de la shell	02/03/2008, 20:54	02/03/2008, 20:54	1
Análisis de la extensión de la shell	02/03/2008, 20:56	02/03/2008, 20:56	4
Análisis de la extensión de la shell	02/03/2008, 20:57	02/03/2008, 20:57	6
Analizar todo el equipo	02/03/2008, 20:58	02/03/2008, 20:58	42


Ver detalles      Resultado Eliminar      Atrás

Estadísticas  
 Análisis: 02/03/08, 20:58  
 Actualización: 02/03/08, 20:47  
 BD de virus: 269.21.3/1307  
 Versión de AVG: 8.0.81  
 La licencia caduca: 01/06/2008


Mostrar notificación

El diálogo **Descripción general de los resultados del análisis** está disponible desde la [interfaz de análisis de AVG](#) a 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](#)

## 12.7. Detalles de los resultados del análisis

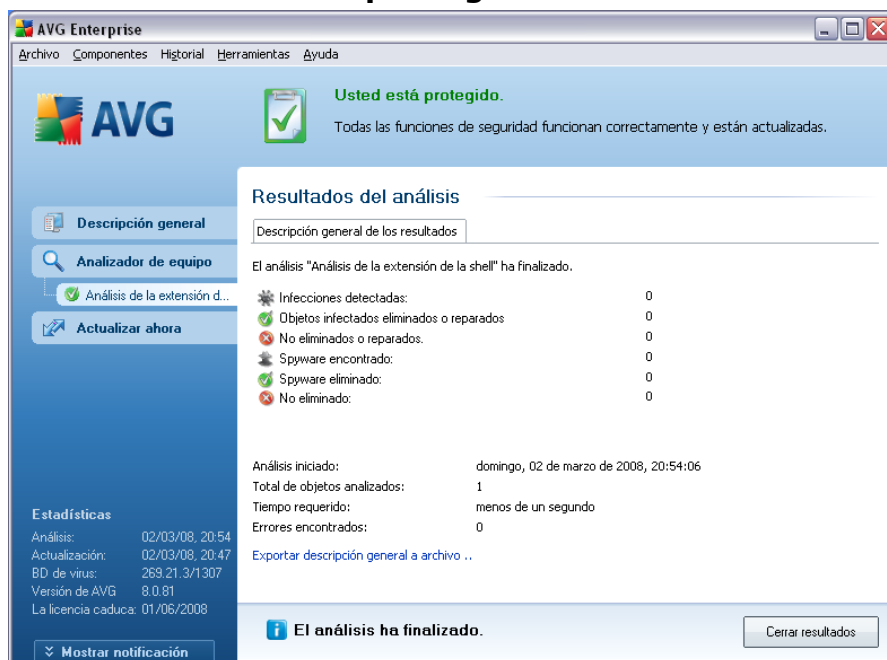
Si en el diálogo **Descripción general de los resultados del análisis** se selecciona un análisis específico, puede a continuación hacer clic en el botón **Ver detalles** para cambiar al diálogo **Resultados del análisis**, que proporciona datos detallados sobre el curso y resultado del análisis seleccionado.

El diálogo está dividido en varias pestañas:

- **Descripción general de los resultados**: esta pestaña se visualiza en todo momento y proporciona los datos estadísticos que describen el progreso del análisis.
- **Infecciones**: esta pestaña se visualiza sólo si durante el análisis se detectó una [infección de virus](#).
- **Spyware**: esta pestaña se visualiza sólo si durante el análisis se detectó un [spyware](#).
- **Advertencias**: esta pestaña se visualiza sólo si durante el análisis se detectaron algunos objetos que no se pudieron analizar.
- **Rootkits**: esta pestaña se visualiza sólo si durante el análisis se detectaron [rootkits](#).
- **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.

### 12.7.1. Pestaña Descripción general de los resultados



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

- [Infecciones de virus/spyware detectadas](#)
- [Infecciones de virus/spyware eliminadas](#)
- [Infecciones de virus/spyware](#) que no se han podido eliminar ni reparar

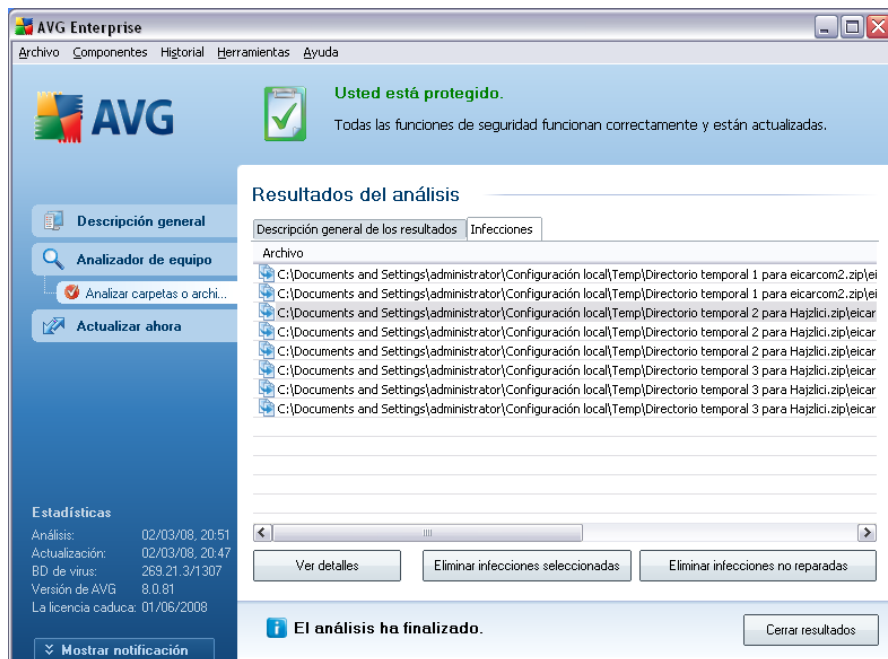
También encontrará información sobre la fecha y la hora exactas de la ejecución del análisis, el número total de objetos analizados, la duración del análisis y el número de errores que se han producido durante el análisis.

#### Botones de control

En este diálogo, solo hay un botón de control disponible. El botón **Cerrar resultados**

permite volver al diálogo [Descripción general de los resultados del análisis](#).

### 12.7.2. Pestaña Infecciones



La pestaña **Infecciones** sólo se muestra en el diálogo **Resultados del análisis** si durante el análisis se detecta [una infección de virus](#). La pestaña se divide en tres secciones que facilitan la información siguiente:

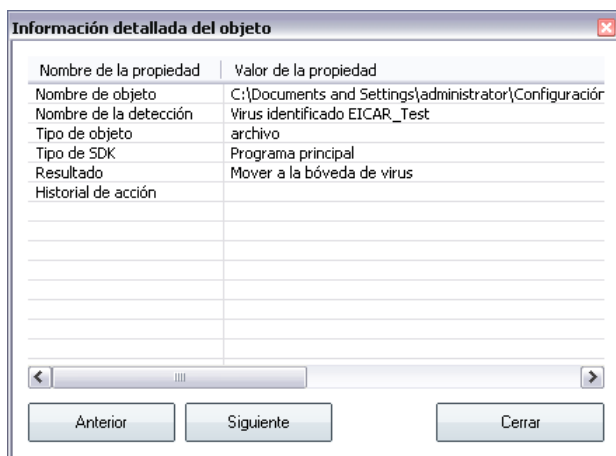
- **Archivo:** ruta completa de la ubicación original del objeto infectado.
- **Infecciones:** nombre del [virus](#) detectado (*para obtener detalles sobre virus específicos, consulte la [Enciclopedia de Virus](#) en línea*).
- **Resultado:** define el estado actual del objeto infectado detectado durante el análisis:
  - **Infectado:** el objeto infectado se ha detectado y se ha dejado en su ubicación original (por ejemplo, si tiene *desactivada la opción de reparación automática* en una configuración de análisis específica).
  - **Reparado:** el objeto infectado se ha reparado automáticamente y se ha dejado en su ubicación original.

- **Movido a la Bóveda de Virus:** el objeto infectado se ha movido a la [Bóveda de Virus](#) donde está en cuarentena.
- **Eliminado:** el objeto infectado se ha eliminado.
- **Agregado a excepciones de PPND:** el hallazgo se ha evaluado como una excepción y se ha agregado a la lista de excepciones de PPND ( configurada en el diálogo [Excepciones PPND](#) en configuración avanzada)
- **Archivo bloqueado, no analizado :** el objeto correspondiente está bloqueado, por lo que el programa AVG no puede analizarlo
- **Objeto potencialmente peligroso :** el objeto se ha detectado como potencialmente peligroso pero no infectado (*puede que, por ejemplo, contenga macros*); la información es sólo una advertencia
- **Para finalizar la acción, es necesario reiniciar el equipo:** el objeto infectado no se puede eliminar; para eliminarlo es preciso reiniciar el equipo.

## Botones de control

Hay tres botones de control disponibles en este diálogo:

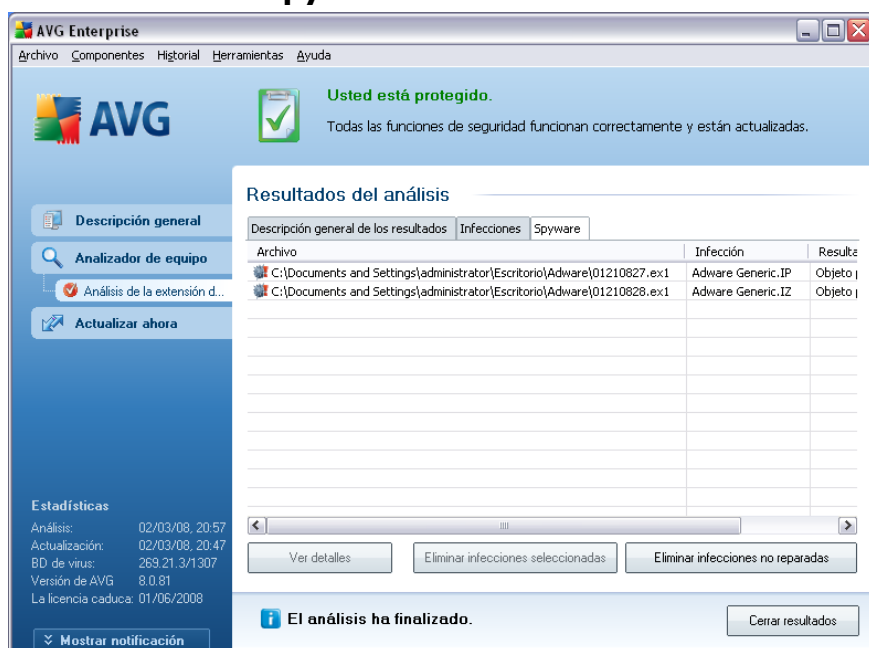
- **Ver detalles:** : el botón abre una nueva ventana de diálogo denominada **Información detallada de resultados del análisis:**



En este diálogo puede encontrar información sobre la ubicación del objeto infeccioso detectado (**Nombre de propiedad**). Mediante los botones **Anterior/Siguiente** puede ver información sobre hallazgos concretos. Utilice el botón **Cerrar** para cerrar este diálogo.

- **Eliminar las infecciones seleccionadas:** utilice este botón para mover el hallazgo seleccionado a la **Bóveda de Virus**.
- **Eliminar todas las infecciones sin reparar:** este botón elimina todos los hallazgos que no se pueden reparar o mover a la **Bóveda de Virus**.
- **Cerrar resultados:** termina la vista general de información detallada y permite volver al diálogo **Descripción general de los resultados del análisis**.

### 12.7.3.Pestaña Spyware



La pestaña **Spyware** solo se visualiza en el diálogo **Resultados del análisis** si se ha detectado **spyware** durante el análisis. La pestaña se divide en tres secciones que facilitan la información siguiente:

- **Archivo:** ruta completa de la ubicación original del objeto infectado.
- **Infecciones:** nombre del **spyware** detectado (*para obtener detalles sobre*

virus específicos, consulte la [Enciclopedia de Virus](#) en línea).

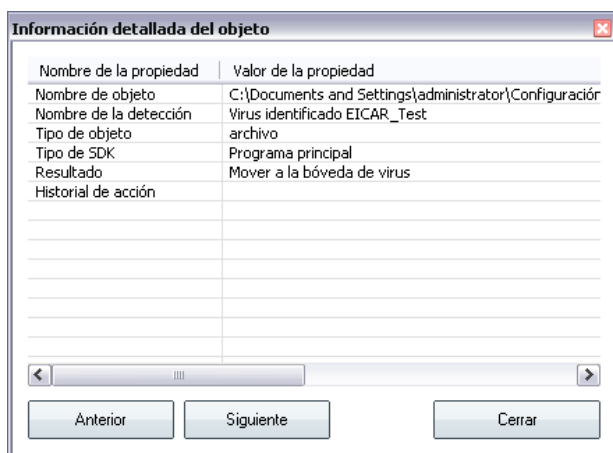
- **Resultado:** define el estado actual del objeto detectado durante el análisis:
  - **Infectado:** el objeto infectado se ha detectado y se ha dejado en su ubicación original (por ejemplo, si tiene [desactivada la opción de reparación automática](#) en una configuración de análisis específica).
  - **Reparado:** el objeto infectado se ha reparado automáticamente y se ha dejado en su ubicación original.
  - **Movido a la Bóveda de Virus:** el objeto infectado se ha movido a la [Bóveda de Virus](#) donde está en cuarentena.
  - **Eliminado:** el objeto infectado se ha eliminado.
  - **Agregado a excepciones de PPND:** el hallazgo se ha evaluado como una excepción y se ha agregado a la lista de excepciones de PPND (configurada en el diálogo [Excepciones PPND](#) de la configuración avanzada)
  - **Archivo bloqueado, no analizado:** el objeto correspondiente está bloqueado, por lo que el programa AVG no puede analizarlo.
  - **Objeto potencialmente peligroso:** el objeto se ha detectado como potencialmente peligroso pero no infectado (por ejemplo, puede contener macros); la información es solo una advertencia.
  - **Para finalizar la acción, es necesario reiniciar el equipo:** el objeto infectado no se puede eliminar; para eliminarlo es preciso reiniciar el equipo.

## Botones de control

Hay tres botones de control disponibles en este diálogo:

- **Ver detalles:** el botón abre una nueva ventana de diálogo denominada **Información detallada de resultados del análisis:**





En este diálogo puede encontrar información sobre la ubicación del objeto infeccioso detectado (**Nombre de propiedad**). Mediante los botones **Anterior/Siguiente** puede ver información sobre hallazgos concretos. Utilice el botón **Cerrar** para salir de este diálogo.

- **Eliminar las infecciones seleccionadas:** utilice este botón para mover el hallazgo seleccionado a la [Bóveda de Virus](#).
- **Eliminar todas las infecciones sin reparar:** este botón elimina todos los hallazgos que no se pueden reparar o mover a la [Bóveda de Virus](#).
- **Cerrar resultados:** termina la vista general de información detallada y permite volver al diálogo [Descripción general de los resultados del análisis](#).

#### 12.7.4. Pestaña Advertencias

La pestaña **Advertencias** muestra información sobre los objetos "sospechosos" (*normalmente archivos*) detectados durante el análisis. Una vez detectados por la [Protección residente](#), se bloquea el acceso a estos archivos. Son ejemplos típicos de este tipo de hallazgos los archivos ocultos, las cookies, las claves de registro sospechosas, los documentos o archivos protegidos mediante contraseñas, etc.

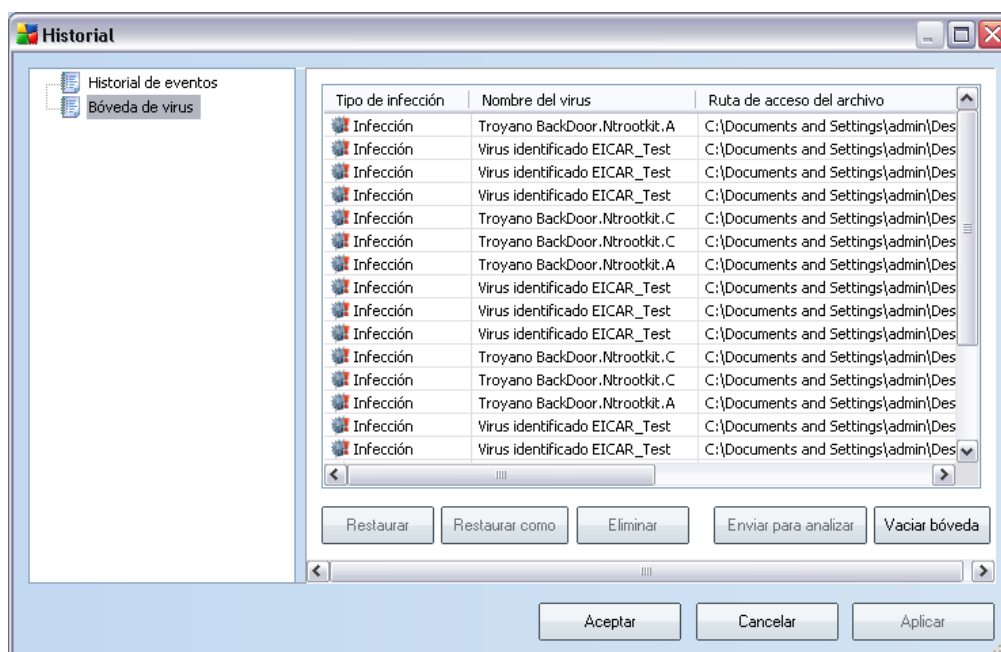
#### 12.7.5. Pestaña Rootkits

La pestaña **Rootkits** muestra la información acerca de los rootkits detectados durante el análisis. Su estructura es básicamente la misma que la de la [pestaña Infecciones](#) o la de la [pestaña Spyware](#).

### 12.7.6. Pestaña Información

La pestaña **Información** contiene datos sobre los "hallazgos" que no se pueden clasificar como infecciones, spyware, etc. No se pueden etiquetar positivamente como peligrosos pero, sin embargo, merecen su atención. Todos los datos de esta pestaña son meramente informativos.

### 12.8. Bóveda de virus



**Bóveda de Virus** es un entorno seguro para administrar los objetos sospechosos/ infectados que se han detectado durante los análisis de AVG. Una vez que se detecta un objeto infectado durante el análisis, y AVG no puede repararlo de inmediato, se le pide que decida qué hacer con el objeto sospechoso. La solución recomendada es mover el objeto a la **Bóveda de virus** para tratarlo allí.

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:

- **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 tenía 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.
- **Enviar a análisis:** envía el archivo sospechoso a los laboratorios de virus de AVG para proceder a su análisis exhaustivo.
- **Vaciar Bóveda de Virus** - elimina todo el contenido de la **Bóveda de Virus** permanentemente

## 13. Actualizaciones de AVG

### 13.1. Niveles de actualización

AVG permite seleccionar dos niveles de actualización:

- **Actualización de definiciones** contiene los cambios necesarios para la protección anti-virus, anti-spam y anti-malware fiable. 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.

### 13.2. Tipos de actualización

Puede distinguir dos tipos de actualización:

- **La actualización a pedido** es una actualización inmediata de AVG que se puede realizar en cualquier momento en que sea necesaria.
- **Actualización programada:** en AVG también se puede [predefinir un plan de actualización](#). La actualización planificada se realiza entonces de manera periódica de acuerdo con la configuración establecida. Siempre que haya nuevos archivos de actualización en la ubicación especificada, se descargan ya sea directamente de Internet, o desde el directorio de red. Cuando no hay actualizaciones más recientes disponibles, nada sucede.

### 13.3. Proceso de actualización

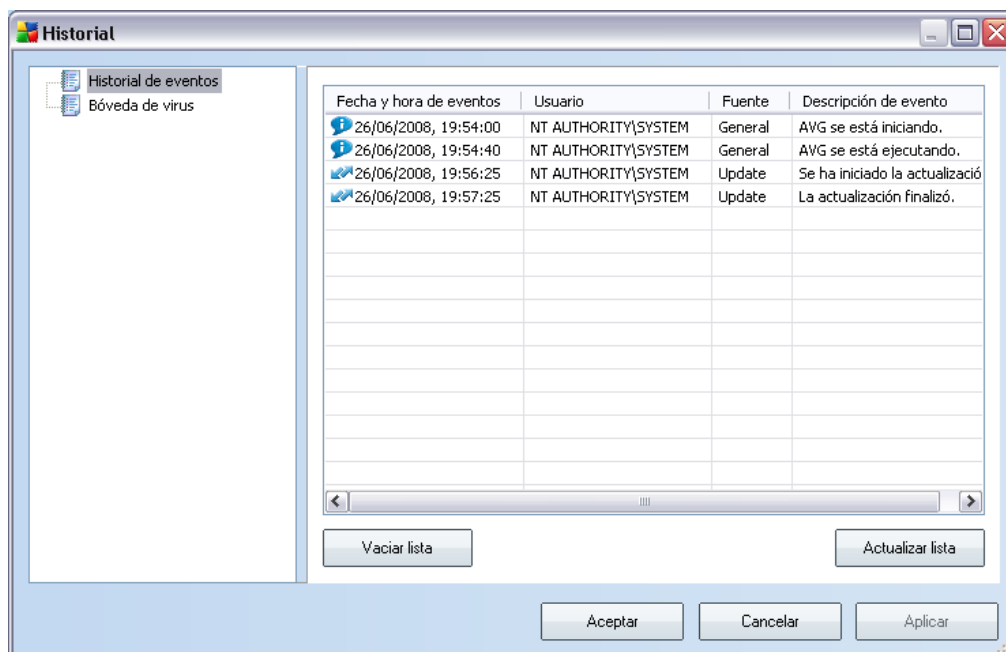
El proceso de actualización se puede iniciar inmediatamente cuando se necesite, mediante el vínculo rápido **Actualizar ahora** . Este vínculo está disponible en todo momento desde cualquier diálogo de la [Interfaz del usuario de AVG](#) . Sin embargo, es altamente recomendable llevar a cabo las actualizaciones regularmente como se establece en la programación de actualización editable dentro del componente [Administrador de actualizaciones](#)

Una vez que se inicia la actualización, AVG verificará primero si hay nuevos archivos de actualización disponibles. De ser así, AVG empieza su descarga e inicia el proceso de actualización por sí mismo. Durante el proceso de actualización, se le enviará a la

interfaz de **Actualización** en donde puede ver 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!*

## 14. Historial de eventos



Se puede tener acceso al cuadro de diálogo **Historial de eventos** desde el [menú del sistema](#) mediante el elemento **Historial/Registro de historial de eventos**. En este cuadro de diálogo, puede encontrar un resumen de los eventos importantes que se han producido durante el funcionamiento de **Anti-Virus AVG 8.5**. El **Historial de eventos** registra los siguientes tipos de eventos:

- Información sobre las actualizaciones de la aplicación AVG
- Comienzo, finalización o interrupción del análisis (incluidos los análisis realizados automáticamente)
- Eventos relacionados con la detección de virus (por [Protección residente](#) o durante el [análisis](#)), con la ubicación del evento incluida.
- Otros eventos importantes

### Botones de control

- **Lista vacía:** elimina todas las entradas de la lista de eventos.

- **Lista de actualizaciones:** actualiza todas las entradas de la lista de eventos.

## 15. Preguntas frecuentes y soporte técnico

Si tiene algún problema técnico o de otra índole con el AVG, consulte la sección **Preguntas frecuentes** del sitio web de AVG en [www.avg.com](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**.